aws

Guía de administración

Amazon Redshift

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Redshift: Guía de administración

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es Amazon Redshift? 1
¿Es la primera vez que usa Amazon Redshift? 1
Información general sobre las características de Amazon Redshift Serverless 2
Información general de los clústeres de Amazon Redshift aprovisionados 5
Administración de clústeres 5
Obtención de acceso a clústeres y seguridad 6
Supervisión de clústeres 8
Bases de datos 9
Comparación de Amazon Redshift Serverless con un almacén de datos aprovisionado de Amazon Redshift 10
Uso de las interfaces de administración de Amazon Redshift para clústeres aprovisionados 39
Trabajar con SDK de AWS 40
Firma de una solicitud HTTP 41
Configuración de la CLI de Amazon Redshift 46
Amazon Redshift sin servidor 48
¿Qué es Amazon Redshift sin servidor? 48
Consola de Amazon Redshift sin servidor 49
Consideraciones sobre el uso de Amazon Redshift sin servidor 53
Capacidad informática para Amazon Redshift Serverless 56
Descripción de la capacidad de Amazon Redshift Serverless 56
Escalado y optimización impulsados por la IA (versión preliminar) 57
Facturación para Amazon Redshift Serverless 59
Precios 59
Facturación de la capacidad de computación 59
Facturación del almacenamiento 64
Uso de la prueba gratuita de Amazon Redshift sin servidor 64
Notas sobre la facturación de uso 65
Conexión a Amazon Redshift sin servidor 67
Conexión a Amazon Redshift sin servidor 67
Conexión a Amazon Redshift sin servidor por medio de controladores JDBC 67
Conexión a Amazon Redshift sin servidor con la API de datos 69
Conexión con SSL a Amazon Redshift sin servidor 69
Conexión con Amazon Redshift sin servidor desde un punto de conexión de VPC administrado por Amazon Redshift 71

Conexión a Amazon Redshift sin servidor desde un punto de conexión de VPC de Redshift en otra cuenta o región ... 72
Configuración de las opciones de tráfico de red adecuadas para Amazon Redshift sin servidor ... 77
Definición de roles de base de datos para concederlos a los usuarios federados en Amazon Redshift sin servidor ... 77
Recursos adicionales ... 77
Definición de roles de base de datos para concederlos a los usuarios federados en Amazon Redshift sin servidor ... 77
Identity and access management en Amazon Redshift Serverless ... 81
Concesión de permisos a Amazon Redshift Serverless ... 81
Introducción a las credenciales de IAM para Amazon Redshift ... 83
Administración del acceso a objetos de base de datos de Amazon Redshift sin servidor con permisos de rol de base de datos ... 84
Migrar un clúster aprovisionado a Amazon Redshift Serverless ... 86
Creación de una instantánea del clúster aprovisionado ... 86
Conexión a Amazon Redshift sin servidor con un controlador ... 87
Uso del SDK de Amazon Redshift Serverless ... 90
Información general de los grupos de trabajo y espacios de nombres de Amazon Redshift sin servidor ... 90
Información general de los grupos de trabajo y espacios de nombres de Amazon Redshift sin servidor ... 90
Administración de Amazon Redshift sin servidor mediante la consola ... 93
Configuración de Amazon Redshift sin servidor por primera vez ... 93
Uso de los grupos de trabajo ... 94
Uso de espacios de nombres ... 99
Administración de los límites de uso, los límites de consulta y otras tareas administrativas ... 103
Monitoreo de consultas y cargas de trabajo con Amazon Redshift sin servidor ... 106
Supervisión de consultas y carga de trabajo con Amazon Redshift sin servidor ... 106
Registro de auditoría para Amazon Redshift sin servidor ... 111
Exportación de registros ... 111
Trabajo con instantáneas y puntos de recuperación ... 121
Instantáneas ... 122
Puntos de recuperación ... 125
Programación de instantáneas ... 126
Copia de las copias de seguridad en otra Región de AWS ... 129

Restauración de una tabla ... 130
Uso de la API de la AWS Command Line Interface y de Amazon Redshift sin servidor ... 131
Uso compartido de datos en Amazon Redshift sin servidor ... 134
Uso compartido de datos en Amazon Redshift sin servidor ... 134
Información general de recursos de etiquetado ... 136
Clústeres aprovisionados de Amazon Redshift ... 139
Información general de Amazon Redshift ... 139
Clústeres y nodos ... 140
Usar EC2-VPC al crear el clúster ... 146
EC2-VPC ... 147
EC2-Classic ... 147
Lance un clúster ... 148
Alarma predeterminada de espacio en disco ... 148
Estado del clúster ... 149
Consideraciones para el uso de clústeres aprovisionados de Amazon Redshift ... 152
Consideraciones sobre regiones y zonas de disponibilidad ... 152
Mantenimiento de clústeres ... 152
Administración de los límites de uso ... 159
Características de red compatibles con los nodos RA3 ... 161
Tipos de nodos ... 162
Operaciones de clúster ... 174
Cambio de tamaño de clústeres ... 174
Pausa y reanudación de clústeres ... 192
Cambio de nombre de los clústeres ... 194
Cierre y eliminación de clústeres ... 195
Reubicación del clúster ... 196
Instantáneas y copias de seguridad ... 202
Configuración de la implementación multi-AZ ... 232
Configuración de la implementación multi-AZ ... 233
Administración de la implementación multi-AZ ... 236
Fallo en la implementación multi-AZ ... 244
Monitoreo de consultas para multi-AZ ... 246
Administración de clústeres a través de la consola ... 249
Creación de un clúster ... 250
Crear un clúster de vista previa ... 253
Modificación de un clúster ... 254

Eliminación de un clúster ... 256
Reinicio de un clúster ... 256
Redimensionamiento de un clúster ... 257
Actualizar la versión de lanzamiento de un clúster ... 258
Obtención de información acerca de la configuración del clúster ... 258
Obtención de información general acerca del estado del clúster ... 259
Crear una instantánea de un clúster ... 259
Crear o editar una alarma de espacio en disco ... 259
Uso de los datos de rendimiento del clúster ... 260
Administración de clústeres mediante la AWS CLI y la API de Amazon Redshift ... 260
Administración de clústeres en una VPC ... 261
Información general ... 261
Creación de un clúster en una VPC ... 264
Administración de grupos de seguridad de VPC para un clúster ... 265
Configuración de las opciones de comunicación del grupo de seguridad para un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor ... 267
Cómo funciona Amazon Redshift con el uso compartido de VPC para los recursos de AWS ... 270
Grupos de subredes del clúster ... 272
Historial de versiones del clúster ... 274
Uso de integraciones sin ETL ... 276
Consideraciones ... 278
Introducción a las integraciones sin ETL ... 280
Creación y configuración de un almacenamiento de datos de Amazon Redshift de destino ... 281
Activación de la distinción entre mayúsculas y minúsculas ... 283
Configuración de la autorización en Amazon Redshift ... 286
Siguientes pasos ... 290
Creación de bases de datos de destino ... 290
Creación de bases de datos de destino en Amazon Redshift ... 290
Adición de datos al origen ... 292
Consulta y creación de vistas materializadas con datos replicados ... 292
Consulta de datos replicados en Amazon Redshift ... 292
Creación de vistas materializadas con datos replicados ... 293
Administración de integraciones sin ETL ... 295
Uso compartido de datos en Amazon Redshift ... 297
Métricas para integraciones sin ETL ... 298

Solución de problemas de integración sin ETL ... 300
Consulta a una base de datos ... 311
Consulta de una base de datos mediante el editor de consultas v2 de Amazon Redshift ... 312
Configuración de su Cuenta de AWS ... 313
Trabajo con el editor de consultas v2 ... 321
Interacción con el SQL generativo del editor de consultas v2 (versión preliminar) ... 339
Descarga de datos en una base de datos ... 347
Creación y ejecución de consultas ... 357
Creación y ejecución de cuadernos ... 363
Consulta de AWS Glue Data Catalog ... 367
Consulta de un lago de datos ... 370
Uso de recursos compartidos de datos ... 373
Programación de una consulta ... 376
Visualización de resultados ... 387
Colaboración y uso compartido en equipo ... 393
Consulta de una base de datos mediante el editor de consultas ... 395
Consideraciones ... 396
Habilitar el acceso ... 397
Conexión con el editor de consultas ... 399
Uso del editor de consultas de ... 400
Programación de una consulta ... 401
Conexión a un almacenamiento de datos mediante herramientas de cliente SQL ... 406
Recomendaciones para conectarse con las herramientas cliente ... 407
Configuración de conexiones en Amazon Redshift ... 408
Configuración de las opciones de seguridad para las conexiones ... 586
Conexión desde herramientas y código cliente ... 595
Conexión con SQL Workbench/J ... 645
Conexión a un almacenamiento de datos mediante programación ... 646
Puede conectarse a Amazon Redshift con un perfil de autenticación. ... 646
Solución de problemas de conexión en Amazon Redshift ... 649
Uso de la API de datos ... 658
Uso de la API de datos ... 658
Consideraciones que deben tenerse en cuenta al llamar a la API de datos ... 659
Ejecución de instrucciones SQL con un token de idempotencia ... 665
Autorización del acceso ... 667
Llamadas a la API de datos ... 674

Solución de problemas de la API de datos 699
Programación de operaciones de la API de datos con Amazon EventBridge 700
Monitoreo de la API de datos 704
Grupos de parámetros 707
Información general 707
Acerca de los grupos de parámetros 707
Valores de parámetros predeterminados 708
Configuración de los valores de parámetros mediante la AWS CLI 710
Configuración de la administración de cargas de trabajo 712
Propiedades dinámicas y estáticas de WLM 712
Propiedades del parámetro wlm_json_configuration 712
Configuración del parámetro wlm_json_configuration mediante la AWS CLI 720
Administración de grupos de parámetros mediante la consola 728
Creación de un grupo de parámetros 729
Modificación de un grupo de parámetros 729
Creación o modificación de una regla de monitoreo de consultas mediante la consola 733
Eliminación de un grupo de parámetros 734
Asociación de un grupo de parámetros con un clúster 735
Administración de grupos de parámetros mediante la AWS CLI y la API de Amazon Redshift .. 735
Integración a un socio de AWS 736
Integración a un socio de AWS usando la consola de Amazon Redshift 736
Carga de datos con socios de AWS 738
Adquisición de nodos reservados 739
Información general 739
Consideraciones sobre ofertas de nodos reservados 740
Comparación del precio entre ofertas de nodos reservados 740
Cómo funcionan los nodos reservados 742
Nodos reservados y facturación unificada 743
Ejemplos de nodos reservados 743
Adquisición de una oferta de nodo reservado con la consola 745
Actualizar nodos reservados con AWS CLI 746
Adquisición de una oferta de nodo reservado mediante la AWS CLI y la API de Amazon Redshift 747
Seguridad 749
Protección de datos 751
Cifrado de datos 752

Tokenización de datos ... 771
Privacidad del tráfico entre redes ... 771
Administración de identidades y accesos ... 772
Autenticación con identidades ... 773
Control de acceso ... 776
Información general sobre la administración del acceso ... 776
Uso de políticas basadas en identidades (políticas de IAM) ... 784
Federación de proveedores de identidades (IdP) nativos para Amazon Redshift ... 842
Conexión de Redshift con IAM Identity Center para ofrecer a los usuarios una experiencia de inicio de sesión único ... 847
Uso de roles vinculados a servicios ... 863
Uso de la autenticación de IAM para generar credenciales de usuario de base de datos ... 869
Autorización a Amazon Redshift para obtener acceso a servicios de AWS ... 930
Administración de las contraseñas de administrador de Amazon Redshift mediante AWS Secrets Manager ... 966
Permisos necesarios para la integración de AWS Secrets Manager ... 967
Rotación del secreto de la contraseña de administrador ... 968
Recuperación del nombre de recurso de Amazon (ARN) del secreto en Amazon Redshift ... 968
Creación de un secreto para las credenciales de conexión a la base de datos ... 969
Consideraciones sobre el uso de AWS Secrets Manager con Amazon Redshift ... 970
Registro y monitoreo ... 971
Registro de auditoría de bases de datos ... 972
Registro con CloudTrail ... 985
Validación de conformidad ... 997
Resiliencia ... 998
Seguridad de infraestructuras ... 999
Aislamiento de red ... 771
Grupos de seguridad ... 1001
Conexión mediante un punto de enlace de la VPC de interfaz ... 1001
Configuración y análisis de vulnerabilidades ... 1008
Tareas de red ... 1009
Uso de un nombre de dominio personalizado para las conexiones de cliente ... 1009
Seguridad de un nombre de dominio personalizado ... 1010
Configuración de un nombre de dominio personalizado ... 1010
Uso de puntos de enlace de la VPC administrados por Redshift ... 1020
Consideraciones ... 1021

Administración de puntos de conexión mediante la consola de Redshift 1022
Administración mediante la AWS CLI 1024
Administración mediante las operaciones de la API de Amazon Redshift 1025
Administración mediante AWS CloudFormation 1025
Enhanced VPC Routing 1025
Uso de los puntos de enlace de la VPC 1027
Enhanced VPC Routing 1028
Redshift Spectrum y enrutamiento de VPC mejorado 1030
Monitoreo del rendimiento del clúster 1035
Información general 1035
Datos de rendimiento 1036
Métricas de Amazon Redshift 1037
Dimensiones de métricas de Amazon Redshift 1048
Datos de rendimiento de cargas y consultas de Amazon Redshift 1051
Uso de los datos de rendimiento 1052
Visualización de datos de rendimiento del clúster 1053
Visualización de datos del historial de consultas 1062
Visualización de datos de rendimiento de la base de datos 1066
Visualización de datos de escalado de simultaneidad y simultaneidad de cargas de trabajo 1069
Visualización de consultas y cargas 1072
Visualización de métricas de clúster durante las operaciones de carga 1076
Análisis del rendimiento de las cargas de trabajo 1077
Administración de alarmas 1080
Uso de métricas de rendimiento en la consola de CloudWatch 1081
Eventos 1083
Información general de eventos de clúster 1083
Uso de Amazon Simple Notification Service 1084
Suscripción a notificaciones de eventos de clúster de Amazon Redshift 1085
Visualización de eventos de clúster mediante la consola 1087
Visualización de eventos de clúster mediante la AWS CLI y la API de Amazon Redshift 1087
Administración de las notificaciones de eventos de clúster 1088
Administración de las notificaciones de eventos de clúster con la consola de Amazon Redshift 1088
Administración de notificaciones de eventos de clúster con la AWS CLI y la API de Amazon Redshift 1088

Notificaciones de eventos de Amazon Redshift 1089
Categorías y mensajes de eventos de Amazon Redshift 1089
Notificaciones de eventos de Amazon Redshift sin servidor con Amazon EventBridge 1113
Notificaciones de eventos de integración sin ETL con Amazon EventBridge 1121
Cuotas y límites 1131
Cuotas para objetos de Amazon Redshift 1131
Cuotas de objetos de Amazon Redshift Serverless 1140
Cuotas para la API de datos de Amazon Redshift 1142
Cuotas para objetos del editor de consultas v2 1145
Cuotas y límites de objetos de Amazon Redshift Spectrum 1147
Restricciones en la nomenclatura 1149
Etiquetado 1153
Información general del proceso de etiquetado 1153
Requisitos de etiquetado 1154
Administración de etiquetas de recursos mediante la consola 1155
Administración de etiquetas mediante la API de Amazon Redshift 1155
Versiones de clúster 1157
Revisión 180 1157
Nuevas características 1158
Parche 179 1159
Nuevas características 1160
Revisión 178 1161
Nuevas características 1162
Revisión 177 1164
Nuevas características 1165
Parche 176 1166
Nuevas características 1167
Parche 175 1168
Nuevas características 1169
Revisión 174 1169
Nuevas características para esta versión 1169
Nuevas características para esta versión 1169
Nuevas características para esta versión 1169
Nuevas características para esta versión 1169
Nuevas características para esta versión 1169
Nuevas características para esta versión 1169

Nuevas características para esta versión ... 1169
Parche 173 ... 1171
Nuevas características para esta versión ... 1171
Nuevas características para esta versión ... 1171
Nuevas características para esta versión ... 1171
Nuevas características para esta versión ... 1171
Nuevas características para esta versión ... 1171
Nuevas características para esta versión ... 1171
Nuevas características para esta versión ... 1171
Nuevas características de esta versión ... 1171
Nuevas características de esta versión ... 1171
Nuevas características de esta versión ... 1171
Parche 172 ... 1172
Nuevas características ... 1173
Parche 171 ... 1173
Nuevas características ... 1174
Parche 170 ... 1174
Nuevas características ... 1174
Parche 169 ... 1174
Nuevas características ... 1175
Parche 168 ... 1175
Nuevas características ... 1175
Ejemplos de código ... 1176
Acciones ... 1178
Crear un clúster ... 1179
Creación de una tabla ... 1183
Eliminar un clúster ... 1184
Descripción de una instrucción de consulta ... 1188
Describir clústers ... 1189
Obtención del resultado de la instrucción ... 1195
Inserción de datos en una tabla ... 1196
Modificar un clúster ... 1198
Consultar una tabla ... 1202
Escenarios ... 1203
Introducción a Amazon Redshift ... 1203
Ejemplos de servicios cruzados ... 1217

Crear una aplicación web para realizar un seguimiento de los datos de Amazon Redshift . 1217
Historial del documento 1219

¿Qué es Amazon Redshift?

Le damos la bienvenida a la Guía de administración de Amazon Redshift. Amazon Redshift es un servicio de almacenamiento de datos administrado a escala de petabytes en la nube . Amazon Redshift sin servidor le permite acceder a los datos y analizarlos sin todas las configuraciones de un almacenamiento de datos aprovisionado. Los recursos se aprovisionan automáticamente y la capacidad del almacenamiento de datos se escala de forma inteligente para ofrecer un rendimiento rápido incluso para las cargas de trabajo más exigentes e impredecibles. No incurrirá en gastos cuando el almacenamiento de datos esté inactivo, por lo que solo pagará por lo que utilice. Puede cargar datos y comenzar a realizar consultas de inmediato en el editor de consultas de Amazon Redshift v2 o en su herramienta de inteligencia empresarial (BI) favorita. Disfrute de la mejor relación precio-rendimiento y de las conocidas características de SQL en un entorno sin administración y fácil de utilizar.

Independientemente del tamaño del conjunto de datos, Amazon Redshift ofrece un rendimiento de consultas rápido con las mismas herramientas basadas en SQL y aplicaciones de inteligencia empresarial que usted usa en la actualidad.

¿Es la primera vez que usa Amazon Redshift?

Si es la primera vez que utiliza Amazon Redshift, le recomendamos que comience leyendo las siguientes secciones:

- Aspectos resaltados y precios del servicio: en esta página de detalles del producto, se proporciona una propuesta de valor, aspectos resaltados del servicio y precios de Amazon Redshift.
- Introducción a Amazon Redshift sin servidor: este tema le guía por el proceso de configuración de un almacenamiento de datos sin servidor, la creación de recursos y la consulta de datos de muestra.
- Guía para desarrolladores de bases de datos de Amazon Redshift: si es un desarrollador de bases de datos, en esta guía, se explica cómo diseñar, crear, consultar y mantener las bases de datos que componen el almacenamiento de datos.

Si prefiere administrar sus recursos de Amazon Redshift manualmente, puede crear clústeres aprovisionados para sus necesidades de consulta de datos. Para obtener más información, consulte Clústeres de Amazon Redshift.

Como desarrollador de aplicaciones, puede usar la API de Amazon Redshift o las bibliotecas de los kits de desarrollo de software (SDK) de AWS para administrar los clústeres mediante programación. Si usa la API de Amazon Redshift, debe autenticar todas las solicitudes HTTP o HTTPS enviadas a la API firmándolas. Para obtener más información acerca de la firma de solicitudes, visite Firma de una solicitud HTTP.

Para obtener más información acerca de la API, la CLI y los SDK, visite los siguientes enlaces:

- Referencia de la API de Amazon Redshift sin servidor
- Referencia de la API de Amazon Redshift
- Referencia de la API de datos de Amazon Redshift
- Referencia de los comandos de la AWS CLI
- Referencias sobre los SDK de Herramientas para Amazon Web Services.

Información general sobre las características de Amazon Redshift Serverless

La mayoría de las características que son compatibles con un aalmacén de datos aprovisionado de Amazon Redshift también lo son con Amazon Redshift Serverless. A continuación se muestran algunas de sus capacidades clave.

Característica	Descripción
Instantáneas	Puede restaurar una instantánea de Amazon Redshift Serverless o de un almacén de datos aprovisionado en Amazon Redshift Serverless. Para obtener más información, consulte Trabajo con instantáneas y puntos de recuperación.
Puntos de recuperación	Amazon Redshift Serverless crea automáticamente un punto de recuperación cada 30 minutos. Estos puntos de recuperación se conservan durante 24 horas. Puede utilizarlos para restaurar después de escrituras o eliminaciones involunta rias. Cuando se restaura desde un punto de recuperación, todos los datos de la base de datos de Amazon Redshift Serverless lo hacen desde un punto anterior. También puede crear una instantánea a partir de un punto de recuperac ión si necesita conservar uno de ellos durante un periodo más prolongado. Para obtener más información, consulte Trabajo con instantáneas y puntos de recuperación.

Característica	Descripción
Capacidad base de RPU	Puede establecer una capacidad base en unidades de procesamiento de Redshift (RPU). Una RPU proporciona 16 GB de memoria. Esta configuración le permite controlar el equilibrio entre los recursos en uso y el costo de la carga de trabajo. Puede aumentar este valor para incrementar los recursos disponibles y mejorar el rendimiento de las consultas o reducir el valor para limitar el gasto. El valor predeterminado es 128 RPU. También puede establecer límites de uso, como las RPU utilizadas por día, para controlar los costes. Para obtener más información, consulte Facturación para Amazon Redshift Serverless.
Límites de uso del intercambio de datos	Puede limitar la cantidad de datos transferidos de una región productora a una región consumidora con la consola o la API. Estos costos de transferencia de datos varían según Región de AWS y se miden en terabytes. Para obtener más información acerca del uso compartido de datos, consulte Introducción al uso compartido de datos con la colsola en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Funciones definidas por el usuario (UDF)	Puede ejecutar funciones definidas por el usuario (UDF) en Amazon Redshift Serverless. Para obtener más información, consulte Creación de funciones definidas por el usuario en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Procedimientos almacenados	Puede ejecutar procedimientos almacenados en Amazon Redshift Serverless. Para obtener más información, consulte Creación de procedimientos almacenados en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Vistas materializadas	Puede crear vistas materializadas en Amazon Redshift Serverless. Para obtener más información, consulte Creación de vistas materializadas en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Funciones espaciales	Puede ejecutar funciones espaciales en Amazon Redshift Serverless. Para obtener más información, consulte Consulta de datos espaciales en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Característica	Descripción
Consultas federadas	Puede ejecutar consultas que unan datos con las bases de datos de Aurora y Amazon RDS desde Amazon Redshift Serverless. Para obtener más informaci ón, consulte Consulta de datos con consultas federadas en la Guía para desarroll adores de bases de datos de Amazon Redshift.
Consultas de lago de datos	Puede ejecutar consultas para unir datos del lago de datos de Amazon S3 con Amazon Redshift Serverless. Para obtener más información, visite Consulta de un lago de datos en la Guía de administración de Amazon Redshift.
HyperLogLog	Puede ejecutar funciones de HyperLogLog en Amazon Redshift Serverless. Para obtener más información, consulte Uso de bocetos de HyperLogLog en la Guía para desarrolladores de bases de datos Amazon Redshift.
Consulta de datos entre distintas bases de datos	Puede consultar datos entre bases de datos con Amazon Redshift Serverless. Para obtener más información, consulte Consulta de datos entre distintas bases de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Uso compartido de datos	Puede acceder a los recursos compartidos de datos en almacenes de datos aprovisionados con Amazon Redshift Serverless. Para obtener más informaci ón, consulte Compartir datos entre clústeres en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Consulta de datos semiestru cturados	Puede capturar y almacenar datos semiestructurados con el tipo de datos SUPER con Amazon Redshift Serverless. Para obtener más información, consulte Captura y consulta de datos semiestructurados en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Etiquetado de recursos	Puede utilizar la AWS CLI o la API de Amazon Redshift Serverless para etiquetar recursos con metadatos relacionados con el recurso. Para obtener más informaci ón, consulte Etiquetado de los recursos.
Machine learning	Puede utilizar machine learning de Amazon Redshift con Amazon Redshift Serverless. Para obtener más información, consulte Uso de machine learning en la Guía para desarrolladores de bases de datos Amazon Redshift.

Característica	Descripción
Comandos y funciones SQL	Salvo algunas excepciones (como `REBOOT_CLUSTER`), puede utilizar comandos y funciones SQL de Amazon Redshift con Amazon Redshift Serverless. Para obtener más información, consulte la Referencia de la SQL en la Guía para desarrolladores de bases de datos de Amazon Redshift..
Recursos de CloudFormation	Con las plantillas de CloudFormation, puede implementar y actualizar los recursos de Amazon Redshift Serverless. Esta integración significa que puede dedicar menos tiempo a administrar recursos y centrarse en las aplicaciones. Para obtener más información sobre los recursos de CloudFormation en Amazon Redshift Serverless, consulte Amazon Redshift Serverless resource type reference (Referencia del tipo de recursos de Amazon Redshift Serverless).
Recursos de CloudTrail	Amazon Redshift sin servidor se integra con AWS CloudTrail para proporcionar un registro de las acciones realizadas en Amazon Redshift sin servidor. CloudTrail captura todas las llamadas a la API de Amazon Redshift Serverless como eventos. Para obtener más información, consulte CloudTrail para Amazon Redshift Serverless.

Información general de los clústeres de Amazon Redshift aprovisionados

El servicio Amazon Redshift administra todo el trabajo de configuración, operación y escalado del almacenamiento de datos. Entre estas tareas, se incluyen el aprovisionamiento de capacidad, la supervisión y la creación de copias de seguridad del clúster, además de la aplicación de parches y actualizaciones al motor de Amazon Redshift.

El siguiente vídeo muestra cómo crear un clúster y consultar datos mediante el editor de consultas v2 de Amazon Redshift.

Administración de clústeres

Un clúster de Amazon Redshift es un conjunto de nodos que consiste en un nodo principal y uno o más nodos informáticos. El tipo y la cantidad de nodos de computación que necesita dependen del tamaño de los datos, la cantidad de consultas que ejecutará y el rendimiento de tiempo de ejecución de consultas que necesite.

Creación y administración de clústeres

Según sus necesidades de data warehouse, puede comenzar con un clúster pequeño, de nodo único, y escalar con facilidad a un clúster más grande de nodos múltiples, a medida que cambien sus requisitos. Puede agregar o eliminar nodos de computación al clúster sin que se interrumpa el servicio. Para obtener más información, consulte Clústeres aprovisionados de Amazon Redshift.

Reserva de nodos de computación

Si desea que el clúster se siga ejecutando durante un año o más, puede ahorrar dinero si reserva los nodos de computación por un periodo de uno o tres años. La reserva de nodos de computación le ofrece ahorros significativos en comparación con las tasas por hora que se pagan al aprovisionar nodos de computación bajo demanda. Para obtener más información, consulte Adquisición de nodos reservados de Amazon Redshift.

Creación de instantáneas de un clúster

Las snapshots son backups de un momento determinado de un clúster. Existen dos tipos de instantáneas: automatizadas y manuales. Amazon Redshift guarda estas instantáneas internamente en Amazon Simple Storage Service (Amazon S3) con una conexión de capa de conexión segura (SSL) cifrada. Si tiene que restaurar datos a partir de una instantánea, Amazon Redshift crea un nuevo clúster e importa los datos de la instantánea que usted especifique. Para obtener más información acerca de las instantáneas, consulte Instantáneas y copias de seguridad de Amazon Redshift.

Obtención de acceso a clústeres y seguridad

Hay varias características relacionadas con el acceso a los clústeres y la seguridad en Amazon Redshift. Estas características lo ayudan a controlar la obtención de acceso a su clúster, definir reglas de conectividad y cifrar datos y conexiones. Estas características se suman a las relacionadas con el acceso a la base de datos y la seguridad en Amazon Redshift. Para obtener más información acerca de la seguridad de bases de datos, consulte Administración de la seguridad de bases de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Cuentas de AWS y credenciales de IAM

De forma predeterminada, solo la cuenta de AWS que crea el clúster de Amazon Redshift puede acceder a él. El clúster se encuentra bloqueado de manera tal que nadie más obtenga acceso. En su cuenta de AWS, utiliza el servicio AWS Identity and Access Management (IAM) para crear

cuentas de usuario y administrar los permisos de esas cuentas para controlar las operaciones del clúster. Para obtener más información, consulte Seguridad en Amazon Redshift. Para obtener más información sobre cómo administrar las identidades de IAM, incluida la orientación y las prácticas recomendadas para los roles de IAM, consulte Administración de identidades y accesos en Amazon Redshift.

Grupos de seguridad

De forma predeterminada, nadie podrá acceder a cualquier clúster que cree. Las credenciales de IAM solo controlan el acceso a los recursos relacionados con la API de Amazon Redshift: la consola de Amazon Redshift, la interfaz de línea de comandos (CLI), la API y el SDK. Para habilitar el acceso al clúster desde herramientas de cliente SQL mediante JDBC u ODBC, se usan grupos de seguridad:

- Si utiliza la plataforma EC2-VPC para su clúster de Amazon Redshift, debe usar grupos de seguridad de la VPC. Le recomendamos que lance el clúster en una plataforma EC2-VPC.

  No se puede mover un clúster a una VPC después de haberse lanzado con EC2-Classic. No obstante, puede restaurar una instantánea de EC2-Classic en un clúster EC2-VPC a través de la consola de Amazon Redshift. Para obtener más información, consulte Restauración de un clúster desde una instantánea.
- Si utiliza la plataforma EC2-Classic en su clúster de Amazon Redshift, debe usar grupos de seguridad de Amazon Redshift.

En cualquiera de los casos, se agregan reglas al grupo de seguridad para otorgar acceso de entrada explícito a un rango específico de direcciones IP/CIDR o a un grupo de seguridad de Amazon Elastic Compute Cloud (Amazon EC2), si el cliente SQL se ejecuta en una instancia de Amazon EC2. Para obtener más información, consulte Grupos de seguridad del clúster de Amazon Redshift.

Además de las reglas de acceso de entrada, crea usuarios de base de datos para brindar credenciales que se autentique para la base de datos dentro del mismo clúster. Para obtener más información, consulte Bases de datos en este tema.

Cifrado

Al aprovisionar el clúster, tiene la opción de cifrarlo para obtener seguridad adicional. Cuando se habilita el cifrado, Amazon Redshift almacena todos los datos en las tablas creadas por el usuario en un formato cifrado. Puede usar AWS Key Management Service (AWS KMS) para administrar las claves de cifrado de Amazon Redshift.

El cifrado es una propiedad inmutable del clúster. La única forma de cambiar de un clúster cifrado a uno no cifrado es descargar los datos y volverlos a cargar en un clúster nuevo. El cifrado se aplica al clúster y a todos los backups. Cuando los datos se restauran desde una snapshot cifrada, el nuevo clúster también se cifra.

Para obtener más información acerca del cifrado, las claves y los módulos de seguridad de hardware, consulte Cifrado de la base de datos de Amazon Redshift.

Conexiones SSL

Puede usar un Secure Sockets Layer (SSL, Cifrado de capa de conexión segura) para cifrar la conexión entre el cliente SQL y el clúster. Para obtener más información, consulte Configuración de las opciones de seguridad para las conexiones.

Supervisión de clústeres

Hay varias características relacionadas con la supervisión en Amazon Redshift. Puede utilizar el registro de auditoría de base de datos para generar registros de actividad, configurar eventos y suscripciones a notificaciones para realizar un seguimiento de información de interés. Utilice las métricas de Amazon Redshift y Amazon CloudWatch para obtener más información sobre el estado y el rendimiento de sus clústeres y bases de datos.

Registro de auditoría de bases de datos

Puede usar la característica de registro de auditoría de bases de datos para realizar un seguimiento de información relacionada con los intentos de autentificación, las conexiones, las desconexiones, los cambios en las definiciones de usuario de la base de datos y las consultas ejecutadas en esta última. Esta información es útil en términos de seguridad y solución de problemas en Amazon Redshift. Los registros se almacenan en buckets de Amazon S3. Para obtener más información, consulte Registro de auditoría de bases de datos.

Eventos y notificaciones

Amazon Redshift realiza un seguimiento de los eventos y retiene información sobre ellos durante varias semanas en su cuenta de AWS. Amazon Redshift brinda información sobre cada evento, como la fecha en la que se produjo, una descripción de él, su fuente (por ejemplo, un clúster, un grupo de parámetros o una instantánea) y el ID de la fuente. Puede crear suscripciones de notificaciones de eventos de Amazon Redshift que especifiquen un conjunto de filtros de eventos. Cuando se produce un evento que coincide con los criterios de filtro, Amazon Redshift usa Amazon

Simple Notification Service para informarle de que se ha producido el evento. Para obtener más información acerca de eventos y notificaciones, consulte Eventos de Amazon Redshift.

Rendimiento

Amazon Redshift proporciona métricas y datos de rendimiento para que pueda realizar un seguimiento del estado y el rendimiento de sus clústeres y bases de datos. Amazon Redshift utiliza las métricas de Amazon CloudWatch para supervisar los aspectos físicos del clúster, como la utilización de la CPU, la latencia y el rendimiento. Amazon Redshift también proporciona datos de rendimiento de la carga y la consulta para ayudarlo a supervisar la actividad de la base de datos en el clúster. Para obtener más información acerca de las métricas y la supervisión del rendimiento, consulte Monitoreo del rendimiento de clústeres de Amazon Redshift.

Bases de datos

Cuando aprovisiona un clúster, Amazon Redshift crea una base de datos. Esta es la base de datos que utiliza para cargar datos y ejecutar consultas en sus datos. Puede crear bases de datos adicionales según necesidad mediante la ejecución de un comando SQL. Para obtener más información acerca de la creación de bases de datos adicionales, consulte Paso 1: Creación de una base de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Al aprovisionar un clúster, especifica un usuario administrador que tiene acceso a todas las bases de datos creadas dentro del clúster. Ese usuario administrador es un superusuario, el único con acceso inicial a la base de datos, aunque este usuario puede crear usuarios y superusuarios adicionales. Para obtener más información, consulte Superusuarios y Usuarios en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Amazon Redshift usa grupos de parámetros, como estilo de presentación de la fecha y precisión de un coma flotante, para definir el comportamiento de todas las bases de datos en un clúster. Si no especifica un grupo de parámetros cuando aprovisiona el clúster, Amazon Redshift le asocia un grupo de parámetros predeterminado. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift.

Para obtener más información sobre las bases de datos de Amazon Redshift, consulte la Guía para desarrolladores de bases de datos de Amazon Redshift.

Comparación de Amazon Redshift Serverless con un almacén de datos aprovisionado de Amazon Redshift

Para Amazon Redshift Serverless, algunos conceptos y características son diferentes de su característica correspondiente para un almacén de datos aprovisionado de Amazon Redshift. Por ejemplo, una comparación que contrasta es que Amazon Redshift Serverless no tiene el concepto de clúster o nodo. En la siguiente tabla se describen las características y el comportamiento de Amazon Redshift Serverless y se explica en qué se diferencian de la característica equivalente en un almacén de datos aprovisionado.

Característica	Descripción	Sin servidor	Aprovisionado
Grupo de trabajo y espacio de nombres	Para aislar cargas de trabajo y administrar distintos recursos en Amazon Redshift Serverless, puede crear espacios de nombres y grupos de trabajo para administrar los recursos de almacenamiento e	Un espacio de nombres es una recopilación de objetos de base de datos y usuarios. El grupo de trabajo es una recopilación de recursos informáticos. Para obtener más información, consulte	Un clúster aprovisionado es un conjunto de nodos de procesamiento y un nodo principal, que se administran directamente. Para obtener más información, consulte Clústeres aprovisionados de Amazon Redshift.

Característica	Descripción	Sin servidor	Aprovisionado
	informáticos de forma independiente.	Amazon Redshift sin servidor para entender el diseño de Amazon Redshift Serverless.	

Característica	Descripción	Sin servidor	Aprovisionado
Tipos de nodos	Cuando trabaja con Amazon Redshift Serverless, no elige tipos de nodos ni especifica el recuento de nodos como lo hace con un clúster de Amazon Redshift aprovisionado.	Amazon Redshift Serverless aprovisiona y administra automáticamente la capacidad por usted. Si lo desea, puede especificar la capacidad del almacenamiento de datos base para seleccionar el equilibrio de precio/rendimiento adecuado para las cargas de trabajo. También puede especific	Crea un clúster con tipos de nodos que cumplen con sus especificaciones de coste y rendimiento. Para obtener más información, consulte Clústeres aprovisionados de Amazon Redshift.

Característica	Descripción	Sin servidor	Aprovisionado
		ar horas máximas de RPU para establecer controles de costos y asegurarse que los costos sean predecibles. Para obtener más información, consulte Descripción de la capacidad de Amazon Redshift Serverless.	

Característica	Descripción	Sin servidor	Aprovisionado
Administración de la carga de trabajo y escalado de simultaneidad	Amazon Redshift puede escalarse para períodos de carga pesada. Amazon Redshift Serverless también se puede escalar para cumplir con períodos intermitentes de alta carga.	Amazon Redshift Serverless administra automáticamente los recursos de forma eficiente y escala, en función de las cargas de trabajo, dentro de los umbrales de los controles de costos. Para obtener más información, consulte Facturación de la capacidad de computación.	Con un almacén de datos aprovisionado, el escalado de simultaneidad se habilita en el clúster para manejar periodos de carga elevada. Para obtener más información, consulte Escalado de simultaneidad.

Característica	Descripción	Sin servidor	Aprovisionado
Puerto	El número de puerto que use para conectarse.	Con Amazon Redshift sin servidor, puede cambiar a otro puerto del intervalo de puertos 5431-5455 u 8191-8215. Para obtener más información, consulte Conexión a Amazon Redshift sin servidor.	Con un almacén de datos aprovisionado, puede elegir cualquier puerto para conectarse.

Característica	Descripción	Sin servidor	Aprovisionado
Cambiar tamaño	Agregue o elimine recursos de computación para obtener un buen rendimiento para la carga de trabajo.	El cambio de tamaño no se aplica en Amazon Redshift Serverless. Sin embargo, puede cambiar la capacidad de RPU del almacenamiento de datos base en función de los requisitos de precio y rendimiento. Para obtener más información, consulte Descripción de la capacidad de Amazon Redshift Serverless.	Con un clúster aprovisionado, se realiza un cambio de tamaño de clúster para agregar o eliminar nodos. Para obtener más información, consulte Información general sobre la administración de los clústeres de Amazon Redshift.

Característica	Descripción	Sin servidor	Aprovisionado
Interrupción temporal y reanudación	Para ahorrar costes, puede pausar un clúster aprovisionado cuando no tenga cargas de trabajo que ejecutar.	Con Amazon Redshift Serverless, se paga solo cuando se ejecutan consultas, por lo que no es necesario pausar ni reanudar. Para obtener más información, consulte Facturación de la capacidad de computación.	Se pausa y reanuda el clúster manualmente, basándose en una evaluación de la carga de trabajo en varios momentos. Para obtener más información, consulte Información general sobre la administración de los clústeres de Amazon Redshift.

Característica	Descripción	Sin servidor	Aprovisionado
Consulta de datos externos con consultas de Spectrum	Puede consultar datos en buckets de Amazon S3, en diversos formatos, como JSON.	La facturación se acumula cuando los recursos de computación procesan las cargas de trabajo. Asimismo, la facturación se acumula cuando se consultan los datos de Redshift Spectrum externos, como cualquier otra transacción. Para obtener más información, consulte Facturación de la	Con un almacén de datos aprovisionado, la capacidad de Amazon Redshift Spectrum existe en servidores independientes que se consultan desde el clúster de Amazon Redshift. Para obtener más información, consulte Consulta de datos externos mediante Amazon Redshift Spectrum

Característica	Descripción	Sin servidor	Aprovisionado
		capacidad de computación.	

Característica	Descripción	Sin servidor	Aprovisionado
Facturación de recursos de computación	Cómo se acumula la facturación de Amazon Redshift frente a Amazon Redshift Serverless.	Con Amazon Redshift Serverless, paga por las cargas de trabajo que ejecuta, en horas de RPU por segundo, con un cargo mínimo de 60 segundos Esto incluye consultas que acceden a datos en formatos de archivo abiertos en Amazon S3. Para obtener más información, consulte Facturaci	Con un clúster aprovisionado, la facturación se produce por segundos cuando el clúster no está en pausa.

Característica	Descripción	Sin servidor	Aprovisionado
		ón de la capacidad de computación.	
Periodo de mantenimiento	Cómo funciona el mantenimiento de los servidores.	No existe un periodo de mantenimiento con Amazon Redshift Serverless. Las actualizaciones se gestionan sin problemas. Para obtener más información, consulte ¿Qué es Amazon Redshift Serverless?.	Con un clúster aprovisionado, se especifica un periodo de mantenimiento cuando se aplican revisiones. (Normalmente, se elige un momento recurrente cuando el uso es bajo).

Característica	Descripción	Sin servidor	Aprovisionado
Cifrado	Puede habilitar el cifrado de bases de datos.	Amazon Redshift Serverless siempre está cifrado con AWS KMS, con claves administradas por AWS o por el cliente.	Los datos de un almacén de datos aprovisionado pueden estar cifrados con AWS KMS (con claves administradas por AWS o por el cliente) o sin cifrar. Consulte Cifrado de la base de datos de Amazon Redshift.
Facturación de almacenamiento	Cómo funciona la facturación del almacenamiento.	Para Amazon Redshift Serverless La tasa se calcula según GB por mes. Consulte Facturación de la capacidad de computación.	El almacenamiento se factura aparte de los recursos informáticos para un clúster aprovisionado con nodos RA3.

Característica	Descripción	Sin servidor	Aprovisionado
Administración de usuarios	Cómo se administran los usuarios.	Tanto para un almacén de datos aprovisionado como para Amazon Redshift Serverless, los usuarios son usuarios de IAM o de Redshift. Para obtener más información, consulte Identity and access management en Amazon Redshift Serverless. Para obtener más	

Característica	Descripción	Sin servidor	Aprovisionado
		información sobre cómo administrar las identidades de IAM, incluidas las prácticas recomendadas para los roles de IAM, consulte Administración de identidades y accesos en Amazon Redshift.	

Característica	Descripción	Sin servidor	Aprovisionado
Herramientas y compatibilidad de JDBC y ODBC	Cómo funcionan las conexiones con los clientes.	Tanto los almacenes de datos aprovisionados como Amazon Redshift Serverless son compatibles con cualquier herramienta o aplicación cliente compatible con JDBC u ODBC. Para obtener más información acerca de los controladores, consulte Configuración de conexiones en la	

Característica	Descripción	Sin servidor	Aprovisionado
		Guía de administración de Amazon Redshift. Para obtener más información acerca de cómo conectarse a Amazon Redshift Serverless, consulte Configuración de conexiones.	

Característica	Descripción	Sin servidor	Aprovisionado
Requisito de credenciales en el inicio de sesión	Cómo se gestionan las credenciales.	Para Amazon Redshift Serverless, no tiene que ingresar credenciales en cada instancia. Para obtener más información, consulte Conexión a Amazon Redshift sin servidor.	El acceso a Amazon Redshift requiere credenciales de inicio de sesión de un usuario asociado a un rol de IAM. El rol de IAM tiene asociados permisos específicos para un almacenamiento de datos aprovisionado. Una vez autenticado, el usuario puede conectarse directamente a la base de datos, a la consola de Redshift y al editor de consultas v2.

Característica	Descripción	Sin servidor	Aprovisionado
Data API (API de datos)	Puede acceder a los datos de los servicios web y otras aplicaciones.	Amazon Redshift Serverless es compatible con la API de datos de Amazon Redshift. Con Amazon Redshift Serverless se utiliza el parámetro `workgroup-name` en lugar del parámetro `cluster-identity`. Para obtener más información sobre la llamada a la API de datos, consulte Uso de la API de	

Característica	Descripción	Sin servidor	Aprovisionado
		datos de Amazon Red	
Instantáneas	Proporciona recuperación a un momento dado.	Amazon Redshift Serverless admite instantáneas y puntos de recuperación. Para obtener más información sobre las instantáneas y los puntos de recuperación de un espacio de nombres, consulte Trabajo con instantáneas y puntos de recuperación.	Los clústeres aprovisionados admiten instantáneas. Para obtener más información, consulte Administración de instantáneas a través de la consola.

Característica	Descripción	Sin servidor	Aprovisionado
Uso compartido de datos	Proporciona la capacidad de compartir datos entre bases de datos de la misma cuenta o de cuentas diferentes.	Amazon Redshift sin servidor admite las mismas características de uso compartido de datos que un almacenamiento de datos aprovisionado. También admite el uso compartido de datos entre Amazon Redshift sin servidor y un almacenamiento de datos aprovisionado, una herramienta o una	Los clústeres aprovisionados admiten el uso compartido de datos entre bases de datos, cuentas, regiones y . Para obtener más información, consulte Compartir datos entre clústeres en Amazon Redshift.

Característica	Descripción	Sin servidor	Aprovisionado
		aplicación cliente.	
Pistas	Proporciona un programa para las actualizaciones de software.	Amazon Redshift Serverless no tiene el concepto de pista. El servicio se encarga de gestionar las versiones y las actualizaciones. Para obtener más información sobre el diselo de Amazon Redshift Serverless. consulte Trabajo con instantáneas y puntos de recuperación.	Los clústeres aprovisionados admiten el cambio entre las pistas actuales y las posteriores.

Característica	Descripción	Sin servidor	Aprovisionado
Tablas y vistas de sistema	Proporciona una forma de supervisar los recursos y los metadatos del sistema.	Amazon Redshift Serverless admite nuevas tablas y vistas del sistema. Para obtener más información acerca de las tablas de sistema, consulte Vistas de supervisión. Para obtener información sobre cómo migrar sus consultas de utilizar las antiguas tablas y vistas del sistema aprovisio	Los almacenes de datos aprovisionados admiten el conjunto existente de tablas y vistas para la supervisión y otras tareas que requieren metadatos del sistema.

Característica	Descripción	Sin servidor	Aprovisionado
		nadas a las nuevas vistas, consulte Migración a las vistas de monitorización SYS.	
Grupos de parámetros	Este es un grupo de parámetros que se aplican a todas las bases de datos creadas en un clúster. Estos parámetros establecen la configuración de la base de datos, como el tiempo de espera de consulta y el estilo de fecha.	Amazon Redshift Serverless no tiene el concepto de grupo de parámetros.	Los almacenes de datos aprovisionados admiten grupos de parámetros. Para obtener más información sobre los grupos de parámetros para un clúster aprovisionado, consulte Grupos de parámetros de Amazon Redshift.

Característica	Descripción	Sin servidor	Aprovisionado
Supervisión de consultas	Proporciona una vista basada en el tiempo de las consultas ejecutadas.	El monitoreo de las consultas en Amazon Redshift Serverless requiere que los usuarios se conecten a la base de datos para utilizar las tablas del sistema. Así, la supervisión de las consultas y las tablas del sistema están sincronizadas. Las consultas de las tablas del sistema en Amazon Redshift Serverless utilizan	La supercisión de consultas en clústeres aprovisionados no muestra todos los datos de las tablas del sistema.

Característica	Descripción	Sin servidor	Aprovisionado
		el usuario de la base de datos asignado al usuario de IAM para utilizar el monitoreo de las consultas. Para obtener más información acerca de cómo supervisar consultas, consulteSupervisión de consultas y carga de trabajo con Amazon Redshift Serverless.	

Característica	Descripción	Sin servidor	Aprovisionado
Registro de auditoría	Proporciona información acerca de las conexiones y las actividades de usuario en la base de datos.	Con Amazon Redshift Serverless, CloudWatch es un destino para los registros de auditoría. Amazon Redshift Serverless no admite la entrega de registros de auditoría basada en Amazon S3. Para obtener más información, consulte Registro de auditoría para Amazon	Para un clúster aprovisionado, la entrega de registros de auditoría basada en Amazon S3 ha sido la norma. Ahora, la entrega de registros de auditoría a CloudWatch se amplía para cubrir también los almacenes de datos aprovisionados.

Característica	Descripción	Sin servidor	Aprovisionado
		Redshift Serverless.	

Característica	Descripción	Sin servidor	Aprovisionado
Notificaciones de eventos	Amazon EventBridge es un servicio conductor de eventos sin servidor que se puede utilizar para conectar las aplicaciones con datos de eventos de varios orígenes.	Amazon Redshift Serverless utiliza Amazon EventBridge para administrar las notificaciones de eventos y mantenerle actualizado sobre los cambios en el almacenamiento de datos. Para obtener más información, consulte Notificaciones de eventos de Amazon Redshift sin servidor con Amazon	Para un clúster aprovisionado, adminisrte las notificaciones de eventos utilizando la consola de Amazon Redshift para crear suscripciones de eventos. Para obtener más información, consulte Administración de las notificaciones de eventos de clúster .

Característica	Descripción	Sin servidor	Aprovisionado
		EventBridge.	

Uso de las interfaces de administración de Amazon Redshift para clústeres aprovisionados

> **Note**
>
> Este tema se centra en las interfaces de administración de Amazon Redshift para clústeres aprovisionados. Existen interfaces de administración similares para Amazon Redshift sin servidor y la API de datos de Amazon Redshift.

Amazon Redshift admite diversas interfaces de administración que puede utilizar para crear, administrar y eliminar clústeres de Amazon Redshift: los AWS SDK, la AWS Command Line Interface (AWS CLI) y la API de administración de Amazon Redshift.

API de Amazon Redshift: puede llamar a esta API de administración de Amazon Redshift mediante el envío de una solicitud. Las solicitudes son solicitudes HTTPS o HTTP que utilizan los verbos HTTP `GET` o `POST` con un parámetro de consulta denominado `Action`. Llamar a la API de Amazon Redshift es la forma más directa de obtener acceso al servicio Amazon Redshift. No obstante, esto requiere que la aplicación controle niveles de detalle de bajo nivel, tales como el control de errores y la generación del código hash para firmar la solicitud.

- Para obtener información acerca de la creación y la firma de una solicitud de API de Amazon Redshift, consulte Firma de una solicitud HTTP.
- Para obtener información sobre las acciones de la API de Amazon Redshift y los tipos de datos para Amazon Redshift, consulte la Referencia de la API de Amazon Redshift.

AWS SDK: puede utilizar los AWS SDK para realizar operaciones relacionadas con clústeres de Amazon Redshift. Varias de las bibliotecas de SDK envuelven la API de Amazon Redshift subyacente. Los SDK integran la funcionalidad de la API en el lenguaje de programación específico y administran varios de los detalles de bajo nivel, como el cálculo de firmas, el control de reintentos

de solicitud y el control de errores. Llamar las funciones envolventes de las bibliotecas de SDK puede simplificar de manera significativa el proceso de escritura de una aplicación para administrar un clúster de Amazon Redshift.

- Los AWS SDK para Java, .NET, PHP, Python, Ruby y Node.js admiten el servicio Amazon Redshift. Las funciones envolventes para Amazon Redshift se documentan en el manual de referencia de cada SDK. Para obtener una lista de los AWS SDK y los enlaces a la documentación, consulte Herramientas para Amazon Web Services.
- En esta guía, se proporcionan ejemplos de cómo trabajar con Amazon Redshift mediante el SDK para Java. Para ver ejemplos de código del SDK de AWS más generales, consulte Ejemplos de código de Amazon Redshift usando SDK de AWS.

AWS CLI: la CLI proporciona un conjunto de herramientas de línea de comandos que puede utilizar para administrar servicios de AWS desde equipos Windows, Mac y Linux. La AWS CLI incluye comandos basados en las acciones de la API de Amazon Redshift.

- Para obtener información acerca de la instalación y la configuración de la CLI de Amazon Redshift, consulte Configuración de la CLI de Amazon Redshift.
- Para obtener material de referencia sobre los comandos de la CLI de Amazon Redshift, consulte Amazon Redshift en la Referencia de la AWS CLI.

Uso de este servicio con un SDK de AWS

Los kits de desarrollo de software (SDK) de AWS se encuentran disponibles en muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK for C++	Ejemplos de código de AWS SDK for C++
AWS SDK for Go	Ejemplos de código de AWS SDK for Go
AWS SDK for Java	Ejemplos de código de AWS SDK for Java
AWS SDK for JavaScript	Ejemplos de código de AWS SDK for JavaScript

Documentación de SDK	Ejemplos de código
AWS SDK para Kotlin	Ejemplos de código de AWS SDK para Kotlin
AWS SDK for .NET	Ejemplos de código de AWS SDK for .NET
AWS SDK for PHP	Ejemplos de código de AWS SDK for PHP
AWS SDK for Python (Boto3)	Ejemplos de código de AWS SDK for Python (Boto3)
AWS SDK for Ruby	Ejemplos de código de AWS SDK for Ruby
AWS SDK para Rust	Ejemplos de código de AWS SDK para Rust
AWS SDK para SAP ABAP	Ejemplos de código de AWS SDK para SAP ABAP
AWS SDK para Swift	Ejemplos de código de AWS SDK para Swift

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código mediante el enlace de Proporcionar comentarios que se encuentra en la parte inferior de esta página.

Firma de una solicitud HTTP

Amazon Redshift requiere que cada solicitud que envía a la API de administración se autentique con una firma. En este tema, se explica cómo firmar solicitudes.

Si utiliza uno de los kits de desarrollo de software (SDK) de AWS o la AWS Command Line Interface, la firma de solicitudes se realiza de forma automática, por lo que puede omitir esta sección. Para obtener más información acerca del uso de AWS SDK, consulte Uso de las interfaces de administración de Amazon Redshift para clústeres aprovisionados. Para obtener más información acerca del uso de la interfaz de línea de comandos de Amazon Redshift, visite la referencia de la línea de comandos de Amazon Redshift.

Para firmar una solicitud, se calcula una firma digital mediante una función hash criptográfica. Un hash criptográfico es una función que devuelve un valor hash único que se basa en la entrada. La entrada a la función hash incluye el texto de su solicitud y su clave de acceso secreta que puede obtener de las credenciales temporales. La función hash devuelve un valor hash que se incluye en la solicitud como la firma. La firma forma parte del encabezado de la `Authorization` de la solicitud.

> **Note**
>
> Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.
> Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	De
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Utilice credenciales a largo plazo para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • En el caso de la AWS CLI, consulte Configuración de la AWS CLI para usar AWS IAM Identity Center en la Guía del usuario de AWS Command Line Interface. • En el caso de los AWS SDK, las herramientas y las API de AWS, consulte Autenticación de IAM Identity Center en la Guía de referencia de AWS SDK y herramientas.
IAM	Utilice credenciales a largo plazo para firmar las	Siga las instrucciones de Uso de credenciales

¿Qué usuario necesita acceso programático?	Para	De
	solicitudes programáticas a la AWS CLI, los AWS SDK o las API de AWS.	temporales con recursos de AWS de la Guía del Usuario de IAM.
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para ver los SDK y las herramientas de AWS, consulte Autenticar mediante credenciales a largo plazo en la Guía de referencia de SDK y herramientas de AWS. • Para las API de AWS, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

Después de recibir su solicitud, Amazon Redshift recalcula la firma con la misma función hash y los datos que ingresó para firmar la solicitud. Si la firma resultante coincide con la firma de la solicitud, Amazon Redshift procesa la solicitud; de lo contrario, esta se rechaza.

Amazon Redshift admite la autenticación mediante AWS Signature Version 4. El proceso para calcular una firma se compone de tres tareas. Estas se ilustran en el siguiente ejemplo.

- Tarea 1: Crear una solicitud canónica

Reorganice la solicitud HTTP en forma canónica. Es preciso utilizar una forma canónica porque Amazon Redshift usa la misma forma canónica para calcular la firma que compara con la que ha enviado.

- Tarea 2: Crear una cadena para firmar

  Crear una cadena que se utilizará como uno de los valores de entrada de la función hash criptográfica. La cadena, denominada cadena para firmar, es una concatenación del nombre del algoritmo hash, la fecha de la solicitud, una cadena de ámbito de credenciales y la solicitud en formato canónico de la tarea anterior. La cadena del ámbito de credenciales es una concatenación de fecha, región e información del servicio.

- Tarea 3: Calcular una firma

  Calcule una firma para la solicitud utilizando una función hash criptográfica que acepte dos cadenas de entrada: la cadena para firmar y una clave derivada. La clave derivada se calcula a partir de la clave de acceso secreta, utilizando el ámbito de credencial para crear una serie de códigos de autenticación de mensajes basados en hash (HMAC-SHA256).

Ejemplo de cálculo de firma

En el siguiente ejemplo, se presentan los detalles de la creación de una firma de una solicitud CreateCluster. Puede utilizar el ejemplo como referencia para comprobar su propio método de cálculo de firmas. Otros cálculos de referencia se incluyen en la sección de ejemplos de firmas de solicitudes de la Guía del usuario de IAM.

Puede utilizar una solicitud GET o POST para enviar solicitudes a Amazon Redshift. La diferencia entre las dos solicitudes es que con la solicitud GET los parámetros se envían como parámetros de cadena de consulta. Con la solicitud POST, las firmas se incluyen en el cuerpo de la solicitud. En el ejemplo a continuación, se presenta una solicitud POST.

El ejemplo supone lo siguiente:

- La marca temporal de la solicitud es `Fri, 07 Dec 2012 00:00:00 GMT`.
- El punto de enlace es la región EE. UU. Este (Norte de Virginia), `us-east-1`.

La sintaxis general de la solicitud es la siguiente:

```
https://redshift.us-east-1.amazonaws.com/
```

```
   ?Action=CreateCluster
   &ClusterIdentifier=examplecluster
   &MasterUsername=masteruser
   &MasterUserPassword=12345678Aa
   &NumberOfNode=2
   &NodeType=ds2.xlarge
   &Version=2012-12-01
   &x-amz-algorithm=AWS4-HMAC-SHA256
   &x-amz-credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/redshift/aws4_request
   &x-amz-date=20121207T000000Z
   &x-amz-signedheaders=content-type;host;x-amz-date
```

La forma canónica de la solicitud calculada en Tarea 1: Crear una solicitud canónica es la siguiente:

```
POST
/

content-type:application/x-www-form-urlencoded; charset=utf-8
host:redshift.us-east-1.amazonaws.com
x-amz-date:20121207T000000Z

content-type;host;x-amz-date
55141b5d2aff6042ccd9d2af808fdf95ac78255e25b823d2dbd720226de1625d
```

La última línea de la solicitud canónica es el hash del cuerpo de la solicitud. La tercera línea de la solicitud canónica se encuentra vacía porque no hay parámetros de consulta para esta API.

La cadena para firmar de Tarea 2: Crear una cadena para firmar es la siguiente:

```
AWS4-HMAC-SHA256
20121207T000000Z
20121207/us-east-1/redshift/aws4_request
06b6bef4f4f060a5558b60c627cc6c5b5b5a959b9902b5ac2187be80cbac0714
```

La primera línea de la cadena para firmar es el algoritmo, la segunda es la marca temporal, la tercera es el ámbito de credenciales y la última es el hash de la solicitud canónica de Tarea 1: Crear una solicitud canónica. El nombre del servicio que se va a utilizar en el ámbito de credenciales es `redshift`.

En Tarea 3: Calcular una firma, la clave derivada puede representarse como sigue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20121207"),"us-
east-1"),"redshift"),"aws4_request")
```

La clave derivada se calcula como series de funciones hash. Desde la instrucción HMAC interna en la fórmula anterior, debe concatenar la frase **AWS4** con su clave de acceso secreta y utilizarla como la clave para aplicar la función hash en los datos “us-east-1”. El resultado de esta hash se convierte en la clave para la siguiente función hash.

Tras calcular la clave derivada, se usa en una función hash que acepte dos cadenas de entrada: la cadena para firmar y la clave derivada. Por ejemplo, si usa la clave de acceso secreta `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` y la cadena para firmar provistas anteriormente, la firma calculada es la siguiente:

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

El último paso consiste en construir el encabezado `Authorization`. Para la clave de acceso de demostración `AKIAIOSFODNN7EXAMPLE`, el encabezado (al que se han agregado saltos de línea para que resulte más legible) es el siguiente:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/
redshift/aws4_request,
SignedHeaders=content-type;host;x-amz-date,
Signature=9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

Configuración de la CLI de Amazon Redshift

En esta sección, se explica cómo configurar y ejecutar las herramientas de línea de comandos de AWS CLI para administrar Amazon Redshift. Las herramientas de línea de comandos de Amazon Redshift se ejecutan en la AWS Command Line Interface (AWS CLI), que, a su vez, utiliza Python (https://www.python.org/). La AWS CLI se puede ejecutar en cualquier sistema operativo que admita Python.

Instrucciones de instalación

Para comenzar a utilizar las herramientas de línea de comandos de Amazon Redshift, primero configura la AWS CLI y, luego, agrega los archivos de configuración que definen las opciones de la CLI de Amazon Redshift.

Si ya instaló y configuró la AWS CLI para otro producto de AWS, puede omitir este procedimiento.

Para instalar AWS Command Line Interface

1. Vaya a Install or update to the latest version of the AWS CLI y, a continuación, siga las instrucciones para instalar la AWS CLI.

   Para acceder a la CLI, necesita un ID de clave de acceso y una clave de acceso secreta. Cuando sea posible, utilice credenciales temporales en lugar de claves de acceso. Las credenciales temporales incluyen un ID de clave de acceso y una clave de acceso secreta, pero, además, incluyen un token de seguridad que indica cuándo caducan las credenciales. Para obtener más información, consulte Uso de credenciales temporales con AWS en la Guía del usuario de IAM.
2. Cree un archivo que contenga la información de configuración, como las claves de acceso, la región predeterminada y el formato de salida de comandos. Luego, establezca la variable de entorno `AWS_CONFIG_FILE` para que haga referencia a ese archivo. Para obtener instrucciones detalladas, visite Configuración de la interfaz de línea de comandos de AWS en la Guía del usuario de AWS Command Line Interface.
3. Ejecute un comando de prueba para confirmar que la AWS CLI está funcionando. Por ejemplo, el siguiente comando debe mostrar información de ayuda para la AWS CLI:

   ```
   aws help
   ```

   El siguiente comando debe mostrar información de ayuda para Amazon Redshift:

   ```
   aws redshift help
   ```

Para obtener material de referencia sobre los comandos de la CLI de Amazon Redshift, consulte Amazon Redshift en la Referencia de la AWS CLI.

Amazon Redshift sin servidor

Amazon Redshift sin servidor le facilita la ejecución y escalabilidad de los análisis sin tener que aprovisionar ni administrar almacenamiento de datos. Con Amazon Redshift sin servidor, los analistas de datos, los desarrolladores y los científicos de datos ahora pueden utilizar Amazon Redshift para obtener información de los datos en cuestión de segundos cargando datos y consultando registros del almacenamiento de datos. Amazon Redshift aprovisiona y escala automáticamente la capacidad del almacenamiento de datos con objeto de ofrecer un rendimiento rápido para cargas de trabajo exigentes e impredecibles. Solo pagará por la capacidad que utilice. Puede beneficiarse de esta simplicidad sin cambiar sus aplicaciones de análisis e inteligencia empresarial existentes.

¿Qué es Amazon Redshift sin servidor?

Amazon Redshift sin servidor aprovisiona automáticamente la capacidad del almacenamiento de datos y escala de manera inteligente los recursos subyacentes. Amazon Redshift sin servidor ajusta la capacidad en segundos para ofrecer un alto rendimiento constante y operaciones simplificadas, incluso para las cargas de trabajo más exigentes e inestables.

Con Amazon Redshift sin servidor, se puede beneficiar de las siguientes características:

- Acceda a los datos y analícelos sin necesidad de configurar, ajustar ni administrar los clústeres aprovisionados de Amazon Redshift.
- Utilice las excepcionales capacidades SQL de Amazon Redshift, el rendimiento líder del sector y la integración de lago de datos con objeto de realizar consultas sin problemas en un almacenamiento de datos, un lago de datos y los orígenes de datos operativos.
- Ofrezca un alto rendimiento constante y operaciones simplificadas para las cargas de trabajo más exigentes e inestables con un escalado automático e inteligente.
- Utilice grupos de trabajo y espacios de nombres para organizar los recursos informáticos y los datos con controles de costos detallados.
- Pague solo cuando se utilice el almacenamiento de datos.

Con Amazon Redshift sin servidor, se utiliza una interfaz de consola para acceder a un almacenamiento de datos sin servidor o API para compilar aplicaciones. A través del almacenamiento de datos, se puede acceder al almacenamiento administrado de Amazon Redshift y al lago de datos de Amazon S3.

Este video le muestra cómo Amazon Redshift sin servidor facilita la ejecución y escalabilidad de los análisis sin tener que administrar infraestructura de almacenamiento de datos:

Consola de Amazon Redshift sin servidor

Para comenzar a utilizar la consola de Amazon Redshift sin servidor, vea el siguiente video: Introducción a Amazon Redshift sin servidor.

Panel sin servidor

En la página Serverless dashboard (Panel de Serverless), puede ver un resumen de sus recursos y gráficos de su uso.

- Namespace overview (Información general del espacio de nombres): en esta sección se muestra la cantidad de instantáneas y recursos compartidos de datos dentro del espacio de nombres.
- Workgroups (Grupos de trabajo): en esta sección se muestran todos los grupos de trabajo de Amazon Redshift sin servidor.
- Queries metrics (Métricas de consultas): en esta sección se muestra la actividad de las consultas efectuadas durante la última hora.
- RPU capacity used (Capacidad de RPU utilizada): en esta sección se muestra la capacidad utilizada durante la última hora.
- Free trial (Prueba gratuita): en esta sección se muestran los créditos de prueba gratuita que quedan en la cuenta de AWS. Esto cubre todo el uso de recursos y operaciones de Amazon Redshift sin servidor, incluidas instantáneas, almacenamiento, grupo de trabajo, etc., en la misma cuenta.
- Alarms (Alarmas): en esta sección se muestran las alarmas que configuró en Amazon Redshift sin servidor.

Copia de seguridad de datos

En la pestaña Data backup (Copia de seguridad de datos), puede trabajar con lo siguiente:

- Snapshots (Instantáneas): puede crear, eliminar y administrar instantáneas de los datos de Amazon Redshift sin servidor. El periodo de retención predeterminado es `indefinitely`, pero puede configurarlo para que sea cualquier valor entre 1 y 3653 días. Puede autorizar a Cuentas de AWS para restaurar espacios de nombres desde una instantánea.
- Recovery points (Puntos de recuperación): muestra los puntos de recuperación que se crean automáticamente de manera tal que pueda recuperarse de una escritura o eliminación involuntaria

en las últimas 24 horas. Para recuperar datos, puede restaurar un punto de recuperación en cualquier espacio de nombres disponible. Puede crear una instantánea a partir de un punto de recuperación si desea conservar uno de ellos durante un periodo más prolongado. El periodo de retención predeterminado es `indefinitely`, pero puede configurarlo para que sea cualquier valor entre 1 y 3653 días.

Acceso a los datos

En la pestaña Data access (Acceso a los datos), puede trabajar con lo siguiente:

- Configuraciones de Network and security (Red y seguridad): puede visualizar los valores relacionados con la VPC, los valores de cifrado de AWS KMS y los valores de registro de auditoría. Puede actualizar solo el registro de auditoría. Para obtener más información sobre la configuración de la red y la seguridad con la consola, consulte Administración de los límites de uso, los límites de consulta y otras tareas administrativas.
- AWS KMS key: se utiliza AWS KMS key para cifrar recursos en Amazon Redshift sin servidor.
- Permissions (Permisos): puede administrar los roles de IAM que Amazon Redshift sin servidor puede asumir cuando utiliza recursos en su nombre. Para obtener más información, consulte Identity and access management en Amazon Redshift Serverless.
- Redshift-managed VPC endpoints (Puntos de conexión de la VPC administrados por Redshift): puede acceder a la instancia de Amazon Redshift sin servidor desde otra VPC o subred. Para obtener más información, consulte Conexión a Amazon Redshift sin servidor desde otros puntos de conexión de la VPC.

Límites

En la pestaña Limits (Límites), puede trabajar con lo siguiente:

- Base capacity in Redshift processing units (RPUs) (Capacidad base en la configuración de las unidades de procesamiento de Redshift [RPU]): puede establecer la capacidad base utilizada para el procesamiento de la carga de trabajo. Para mejorar el rendimiento de las consultas, aumente el valor de la RPU.
- Usage limits (Límites de uso): los recursos informáticos máximos que la instancia de Amazon Redshift sin servidor puede utilizar en un periodo determinado antes de que se inicie una acción. Se limita la cantidad de recursos que Amazon Redshift sin servidor utiliza a la hora de ejecutar la carga de trabajo. El uso se mide en horas de unidades de procesamiento de Redshift (RPU). Una

hora de RPU es el número de RPU utilizadas en una hora. Se determina que ocurra una acción cuando se alcanza el límite que se ha establecido, tal y como se indica a continuación:

- enviar una alerta
- registrar una entrada en una tabla del sistema
- desactivar las consultas de los usuarios

Puede configurar hasta cuatro límites.

- Query limits (Límites de consulta): puede agregar un límite para supervisar el rendimiento y los límites. Para obtener más información sobre los límites de supervisión de consultas, consulte Reglas de supervisión de consultas de WLM.

Para obtener más información, consulte Descripción de la capacidad de Amazon Redshift Serverless.

Recursos compartidos de datos

En la pestaña Datashares (Recursos compartidos de datos), puede trabajar con lo siguiente:

- Datashares created in my namespace (Recursos compartidos de datos creados en la configuración de mi espacio de nombres): puede crear un recurso compartido de datos y compartirlo con otros espacios de nombres y Cuentas de AWS.
- Datashares from other namespaces and Cuentas de AWS (Recursos compartidos de datos de otros espacios de nombres y): puede crear una base de datos a partir de un recurso compartido de datos desde otro espacio de nombres y Cuentas de AWS.

Para obtener más información sobre el uso compartido de datos, consulte Uso compartido de datos en Amazon Redshift sin servidor.

Monitoreo de consultas y bases de datos

En la página Query and database monitoring (Supervisión de consultas y bases de datos), puede visualizar los gráficos del historial de consultas y del rendimiento de la base de datos.

En la pestaña Query history (Historial de consultas), puede ver los siguientes gráficos (puede elegir entre Query list [Lista de consultas] y Resource metrics [Métricas de recursos]):

- Query runtime (Tiempo de ejecución de consultas): este gráfico muestra las consultas que se ejecutan en el mismo periodo. Elija una barra del gráfico para obtener más detalles sobre la ejecución de la consulta.

- Queries and loads (Consultas y cargas): en esta sección se enumeran las consultas y las cargas según el ID de la consulta.
- RPU capacity used (Capacidad de RPU utilizada): este gráfico muestra la capacidad global en unidades de procesamiento de Redshift (RPU).
- Database connections (Conexiones de bases de datos): este gráfico muestra la cantidad de conexiones activas a la base de datos.

Rendimiento de la base de datos

En la pestaña Database performance (Rendimiento de la base de datos), puede consultar los siguientes gráficos:

- Queries completed per second (Consultas completadas por segundo): este gráfico muestra el número medio de consultas completadas por segundo.
- Queries duration (Duración de la consulta): este gráfico muestra el tiempo medio que se tarda en completar una consulta.
- Database connections (Conexiones de bases de datos): este gráfico muestra la cantidad de conexiones activas a la base de datos.
- Running queries (Consultas en curso): este gráfico muestra la cantidad total de consultas en curso en un momento dado.
- Queued queries (Consultas en cola): este gráfico muestra la cantidad total de consultas en cola en un momento dado.
- Query run time breakdown (Desglose del tiempo de ejecución de consultas): este gráfico muestra el tiempo total de ejecución de las consultas según el tipo que sea.

Monitoreo de recursos

En la página Supervisión de recursos, puede consultar los gráficos de los recursos consumidos. Puede filtrar los datos en función de diferentes facetas.

- Metric filter (Filtro de métricas): puede utilizar filtros de métricas para seleccionar filtros para un grupo de trabajo específico, así como elegir el intervalo de tiempo.
- RPU capacity used (Capacidad de RPU utilizada): este gráfico muestra la capacidad global en unidades de procesamiento de Redshift (RPU).
- Uso de computación: este gráfico muestra el uso de horas de RPU por período para el rango de tiempo seleccionado. Para intervalos de tiempo inferiores a 6 horas, las horas de RPU se muestran

con la hora exacta. Para intervalos de tiempo de 6 horas o más, las horas de RPU se muestran como promedios.

En la página Datashares (Recursos compartidos de datos), puede administrar recursos compartidos de datos In my account (En mi cuenta) y From other accounts (Desde otras cuentas). Para obtener más información sobre el uso compartido de datos, consulte Uso compartido de datos en Amazon Redshift sin servidor.

Consideraciones sobre el uso de Amazon Redshift sin servidor

Para obtener una lista de las Regiones de AWS donde Amazon Redshift sin servidor está disponible, consulte los puntos de conexión enumerados para la API de Redshift sin servidor en la Referencia general de Amazon Web Services.

Algunos recursos que utiliza Amazon Redshift sin servidor están sujetos a cuotas. Para obtener más información, consulte Cuotas de objetos de Amazon Redshift Serverless.

Cuando se DECLARA un cursor, las especificaciones de tamaño del conjunto de resultados para Amazon Redshift sin servidor se especifican en DECLARE.

Periodo de mantenimiento: no hay ningún periodo de mantenimiento con Amazon Redshift sin servidor. Las actualizaciones de la versión del software se aplican de forma automática. No hay interrupción para la conexión existente o la ejecución de consultas cuando Amazon Redshift cambia de versión. Las nuevas conexiones siempre se conectarán y funcionarán con Amazon Redshift sin servidor al instante.

ID de zonas de disponibilidad: cuando configure la instancia de Amazon Redshift sin servidor, Additional considerations (Consideraciones adicionales) y asegúrese de que los ID de subred proporcionados en Subnet (Subred) contienen al menos tres de los ID de zonas de disponibilidad admitidos. Para ver la asignación de subred al ID de zona de disponibilidad, diíjase a la consola de la VPC y elija Subnets (Subredes) para la lista de ID de subred con sus correspondientes ID de zona de disponibilidad. Compruebe que su subred está asignada a un ID de zona de disponibilidad compatible. Para crear una subred, consulte Crear una subred en la VPC en la Guía del usuario de Amazon VPC.

Tres subredes: debe tener al menos tres subredes y deben estar distribuidas en tres zonas de disponibilidad. Por ejemplo, es posible que utilice tres subredes que se asignan a las zonas de disponibilidad us-east-1a, us-east-1b y us-east-1c. Una excepción a esto es la es la región Oeste de EE. UU. (Norte de California). Requiere tres subredes, de la misma manera que las demás regiones,

pero estas solo deben abarcar dos zonas de disponibilidad. Una condición es que una de las zonas de disponibilidad abarcadas contenga dos de las subredes.

Requisitos de dirección IP gratuita: debe tener direcciones IP gratuitas disponibles cuando cree un grupo de trabajo de Amazon Redshift sin servidor. El número mínimo de direcciones IP aumenta a medida que se incrementa el número de unidades de procesamiento Redshift (RPU) del grupo de trabajo. En concreto, cada subred de la VPC de su grupo de trabajo requiere un número mínimo de direcciones IP. Para obtener más información sobre la asignación de direcciones IP, consulte Direccionamiento IP en la Guía del usuario de Amazon VPC.

El número mínimo de direcciones IP libres necesarias al crear un grupo de trabajo es el siguiente:

Número de direcciones IP libres necesarias para cada subred

Unidades de procesamiento Redshift (RPU)	Direcciones IP libres necesarias	Tamaño de CIDR mínimo
8	9	/27
16	15	/27
32	13	/27
64	21	/27
128	37	/26
256	69	/25
512	133	/24

También necesitará direcciones IP libres cuando actualice su grupo de trabajo para utilizar más RPU. El número de direcciones IP libres necesarias al actualizar las subredes de un grupo de trabajo es el siguiente:

Número de direcciones IP libres necesarias para actualizar una subred

Unidades de procesamiento Redshift (RPU)	Unidades de procesamiento Redshift (RPU) actualizadas	Direcciones IP libres necesarias
8	16	10

Unidades de procesamiento Redshift (RPU)	Unidades de procesamiento Redshift (RPU) actualizadas	Direcciones IP libres necesarias
16	32	13
32	64	16
64	128	28
128	256	52
256	512	100

Espacio de almacenamiento después de la migración: al migrar clústeres aprovisionados de Amazon Redshift pequeños a Amazon Redshift sin servidor, es posible que aparezca un aumento en la asignación de espacio de almacenamiento después de la migración. Esto es el resultado de la asignación optimizada del espacio de almacenamiento, lo que produce un espacio de almacenamiento preasignado. Este espacio se utiliza durante un periodo de tiempo a medida que los datos crecen en Amazon Redshift sin servidor.

Recurso compartido de datos entre clústeres aprovisionados de Amazon Redshift sin servidor y Amazon Redshift: cuando se comparten datos donde Amazon Redshift sin servidor es el productor y un clúster aprovisionado es el consumidor, el clúster aprovisionado debe tener una versión de clúster posterior a 1.0.38214. Si se utiliza una versión de clúster anterior a esta, se produce un error al ejecutar una consulta. Puede consultar la versión de clúster en la consola de Amazon Redshift en la pestaña Maintenance (Mantenimiento). También puede ejecutar `SELECT version();`.

Tiempo máximo de ejecución de la consulta: tiempo de ejecución transcurrido para una consulta, en segundos. El tiempo de ejecución no incluye el tiempo de espera empleado en una cola. Si una consulta supera el tiempo de ejecución establecido, Amazon Redshift sin servidor la detiene. Los valores válidos son de 0 a 86 399.

Migración para tablas con claves de clasificación intercaladas: al migrar clústeres aprovisionados de Amazon Redshift a Amazon Redshift sin servidor, Redshift convierte tablas con claves de clasificación intercaladas y DISTSTYLE KEY en claves de clasificación compuestas. El DISTSTYLE no cambia. Para obtener más información sobre los estilos de distribución, consulte Uso de estilos de distribución de datos en la guía para desarrolladores de Amazon Redshift. Para obtener más información sobre claves de clasificación, consulte Trabajo con claves de clasificación.

Uso compartido de la VPC: puede crear grupos de trabajo de Amazon Redshift sin servidor en una VPC compartida. Si lo hace, le recomendamos que no elimine el recurso compartido, ya que puede provocar que el grupo de trabajo deje de estar disponible.

Capacidad informática para Amazon Redshift Serverless

Descripción de la capacidad de Amazon Redshift Serverless

RPU

Amazon Redshift Serverless mide la capacidad del almacenamiento de datos en unidades de procesamiento de Redshift (RPU). Las RPU son recursos que se utilizan para gestionar cargas de trabajo.

Capacidad base

Esta configuración especifica la capacidad base del almacenamiento de datos que Amazon Redshift utiliza para atender las consultas. La capacidad base se especifica en las RPU. Puede establecer una capacidad base en unidades de procesamiento de Redshift (RPU). Una RPU proporciona 16 GB de memoria. Configurar una capacidad base más alta mejora el rendimiento de las consultas, especialmente para los trabajos de procesamiento de datos que consumen muchos recursos. La capacidad base predeterminada para Amazon Redshift Serverless es de 128 RPU. Puede ajustar la configuración Capacidad base de 8 a 512 RPU en unidades de 8 (8,16,24...512) con la consola de AWS, la operación de la API `UpdateWorkgroup` o la operación `update-workgroup` en la AWS CLI.

Con una capacidad mínima de 8 RPU, ahora tiene más flexibilidad para ejecutar cargas de trabajo más simples o más complejas en función de los requisitos de rendimiento. Las capacidades de RPU base de 8, 16 y 24 RPU están destinadas a cargas de trabajo que requieren menos de 128 TB de datos. Si sus requisitos de datos son superiores a 128 TB, debe utilizar un mínimo de 32 RPU. Para las cargas de trabajo que tienen tablas con columnas de números grandes y simultaneidad más alta, recomendamos usar 32 o más RPU.

Consideraciones y limitaciones de la capacidad de Amazon Redshift sin servidor

A continuación se presentan las consideraciones y limitaciones de la capacidad de Amazon Redshift sin servidor.

- Las configuraciones de 8 o 16 RPU admiten una capacidad de almacenamiento administrado por Redshift de hasta 128 TB. Si utiliza más de 128 TB de almacenamiento administrado, no podrá reducir a menos de 32 RPU.
- La edición de la capacidad base del grupo de trabajo puede cancelar algunas de las consultas que se están ejecutando en el grupo de trabajo.

Escalado y optimización impulsados por la IA (versión preliminar)

Esta es la documentación de la versión preliminar del escalado y la optimización impulsados por la IA en Amazon Redshift sin servidor. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

Esta versión preliminar está disponible en las siguientes Regiones de AWS:

- Este de EE. UU. (Ohio) (us-east-2)
- Este de EE. UU. (Norte de Virginia) (us-east-1)
- EE. UU. Oeste (Norte de California) (us-west-1)
- Asia-Pacífico (Tokio) (ap-northeast-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Estocolmo) (eu-north-1)

Puede crear un grupo de trabajo de versión preliminar para probar nuevas características de Amazon Redshift sin servidor. No puede utilizar estas características en producción ni trasladar su grupo de trabajo a otro grupo de trabajo. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS. Para obtener instrucciones sobre cómo crear un grupo de trabajo de versión preliminar, consulte Crear un grupo de trabajo de vista previa.

También puede establecer un objetivo de precio y rendimiento para su grupo de trabajo, de modo que Redshift pueda realizar automáticamente optimizaciones impulsadas por la IA de sus recursos. De esta forma, puede cumplir sus objetivos de precio y rendimiento y, al mismo tiempo, optimizar los costos. Esta optimización automática de la relación entre precio y rendimiento resulta especialmente

útil si no sabe qué capacidad base debe configurar para sus cargas de trabajo o si algunas partes de la carga de trabajo podrían beneficiarse de una mayor asignación de recursos.

Por ejemplo, si su organización suele ejecutar cargas de trabajo que solo requieren 32 RPU, pero de repente introduce una consulta más compleja, es posible que no sepa cuál es la cantidad adecuada de capacidad base. Si se establece una capacidad base mayor, se obtiene una mejor relación de precio y rendimiento, pero también se incurre en costos más altos, por lo que es posible que el costo no se ajuste a sus expectativas. Mediante el escalado y la optimización de recursos impulsados por la IA, Amazon Redshift sin servidor ajusta automáticamente las RPU para cumplir sus objetivos de precio y rendimiento y, al mismo tiempo, mantiene los costos optimizados para su organización. Esta optimización automática es útil independientemente del tamaño de la carga de trabajo. La optimización automática puede ayudarle a cumplir los objetivos de relación entre precio y rendimiento de su organización si tiene un número de consultas complejas.

Los objetivos de precio y rendimiento son una configuración específica de cada grupo de trabajo. Los diferentes grupos de trabajo pueden tener diferentes objetivos de precio y rendimiento.

Para mantener la previsibilidad de los costos, establezca un límite de capacidad máxima que Amazon Redshift sin servidor pueda asignar a sus cargas de trabajo.

Para configurar los objetivos de precio y rendimiento, utilice la consola de AWS. De forma predeterminada, el objetivo de precio y rendimiento está activado al crear un nuevo grupo de trabajo y se establece en Equilibrado. Para establecer un objetivo de precio y rendimiento diferente o especificar una capacidad base para su grupo de trabajo, utilice una configuración personalizada al crear un grupo de trabajo. Para obtener más información sobre la creación de un grupo de trabajo, consulte Creación de un grupo de trabajo con un espacio de nombres.

Para editar el objetivo de precio y rendimiento de su grupo de trabajo:

1. En la consola de Amazon Redshift sin servidor, elija Configuración del espacio de nombres.
2. Elija el grupo de trabajo para el que desea editar el objetivo de precio y rendimiento. Seleccione la pestaña Rendimiento y, a continuación, Editar.
3. Elija Objetivo de precio y rendimiento y ajuste el control deslizante de acuerdo con el objetivo que desee establecer para su grupo de trabajo.
4. Elija Guardar cambios.

Para actualizar la cantidad máxima de RPU que Amazon Redshift sin servidor puede asignar a su carga de trabajo, vaya a la pestaña Límites de la configuración del grupo de trabajo.

Para obtener más información sobre las optimizaciones y el escalado de recursos impulsadas por la IA, vea el siguiente video.

Facturación para Amazon Redshift Serverless

Precios

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

Facturación de la capacidad de computación

Capacidad base y su efecto en la facturación

Cuando se ejecutan las consultas, se le factura en función de la capacidad utilizada en una duración determinada, en horas de RPU por segundo. Cuando no se ejecuta ninguna consulta, no se le factura por capacidad informática. También se le cobra el almacenamiento administrado de Redshift (RMS), según la cantidad de datos almacenados.

Cuando cree su grupo de trabajo, tendrá la opción de establecer la Capacidad base de computación. Para satisfacer los requisitos de precio/rendimiento de su carga de trabajo en el nivel de grupo de trabajo, ajuste la capacidad base más alta o más baja para un grupo de trabajo existente. Seleccione el grupo de trabajo en Configuración de grupos de trabajo y elija la pestaña Límites para modificar la capacidad base mediante la consola.

A medida que aumenta el número de consultas, Amazon Redshift sin servidor se escala automáticamente para proporcionar un rendimiento uniforme.

Límite máximo de uso de horas de la RPU

Para mantener los costos predecibles para Amazon Redshift Serverless, puede configurar el valor de Maximum RPU hours (Horas máximas de RPU) que se necesita por día, por semana o por mes. Puede configurarlo desde la consola o la API. Si se alcanza un límite, puede especificar que se escriba una entrada de registro en una tabla del sistema, que se reciba una alerta o que se desactiven las consultas de los usuarios. La configuración de las horas máximas de RPU ayuda a mantener el costo bajo control. La configuración de horas máximas de RPU se aplica al grupo de trabajo tanto para consultas que acceden a los datos del almacenamiento de datos como para consultas que acceden a datos externos, como en una tabla externa en Amazon S3.

A continuación, se muestra un ejemplo:

Supongamos que establece un límite de 100 horas por semana. Para definirlo en la consola, debe hacer lo siguiente:

1. Elija su grupo de trabajo y, a continuación, Administrar los límites de uso en la pestaña Límites.
2. Agregue un límite de uso, elija la frecuencia Semanalmente, una duración de 100 horas y configure la acción para Desactivar las consultas de usuario.

En este ejemplo, si alcanza el límite de 100 horas de RPU durante una semana, las consultas se desactivan.

Establecer un número de horas máximas de RPU para el grupo de trabajo no limita el rendimiento ni los recursos de computación del grupo de trabajo. Puede ajustar la configuración en cualquier momento sin que afecte al procesamiento de las consultas. El objetivo de establecer un número máximo de horas de RPU es ayudarle a cumplir los requisitos de precio y rendimiento. Para obtener más información sobre la facturación de la infraestructura sin servidor, consulte los precios de Amazon Redshift.

Otra forma de mantener predecible el costo de Amazon Redshift sin servidor es utilizar la Detección de anomalías de costos de AWS para reducir las sorpresas en la facturación y proporcionar más control.

> **Note**
>
> La calculadora de precios de Amazon Redshift es útil para realizar una estimación de precios. Introduzca los recursos de computación que necesita y le ofrecerá una vista previa del costo.

Establecimiento de la capacidad máxima para controlar los costos de los recursos de computación

La configuración de capacidad máxima sirve como límite máximo de la RPU hasta el que puede escalar Amazon Redshift sin servidor. Ayuda a controlar el costo de los recursos de computación. De manera similar a la forma en que la capacidad base establece una cantidad mínima de recursos de computación disponibles, la capacidad máxima establece un límite en el uso de la RPU. De esta forma, ayuda a que sus gastos cumplan con lo previsto. La capacidad máxima se aplica específicamente a cada grupo de trabajo y limita el uso de la computación en todo momento.

Diferencias entre la capacidad máxima y los límites de uso por hora de la RPU

El objetivo tanto de los límites máximos por hora de la RPU como de la configuración de capacidad máxima es controlar los costos. Sin embargo, lo logran a través de diferentes medios. Los puntos siguientes explican la diferencia:

- Capacidad máxima: esta configuración establece el recuento más alto de las RPU que Amazon Redshift sin servidor utiliza para escalar Cuando se requiere un escalado de computación automático, tener un valor más alto para la capacidad máxima puede mejorar el rendimiento de las consultas. Cuando se alcanza el límite de capacidad máxima, el grupo de trabajo no escala verticalmente los recursos.
- Límite máximo de uso por horas de la RPU: a diferencia de la capacidad máxima, esta configuración no establece un límite máximo de capacidad. Sin embargo, lleva a cabo otras acciones para ayudarle a limitar los costos. Estas incluyen añadir una entrada a un registro, enviarle una notificación o impedir que se ejecuten las consultas, si así lo desea.

Puede usar la capacidad máxima de forma exclusiva o puede complementarla con acciones que se ajusten a los límites máximos de uso por horas de la RPU.

Un caso práctico de capacidad máxima

Cada grupo de trabajo puede tener una configuración de capacidad máxima diferente para ayudarle a cumplir los requisitos presupuestarios. En los siguientes ejemplos se ilustra cómo funciona:

- Tiene un grupo de trabajo con la capacidad base establecida en 256 RPU. Tiene cargas de trabajo estables de poco más de 256 RPU durante la mayor parte del mes.
- La capacidad máxima se establece en 512 RPU.

Supongamos que durante un período de tres días hay un elevado uso inesperado para generar informes estadísticos ad-hoc. En este caso, tiene configurada la capacidad máxima para evitar costos de computación superiores a los de 512 RPU. Al hacerlo, puede asegurarse de que la capacidad de computación no supere este límite superior.

Notas de uso sobre la capacidad máxima

Estas notas pueden ayudarle a configurar la capacidad máxima de forma adecuada:

- Cada grupo de trabajo de Amazon Redshift sin servidor puede tener una configuración de capacidad máxima diferente.

- Si tiene un período de uso de recursos muy elevado y la capacidad máxima se establece en un nivel de RPU bajo, esto puede retrasar el procesamiento de la carga de trabajo y provocar una experiencia de usuario que no sea óptima.
- La configuración de la capacidad máxima no interfiere con la ejecución de las consultas, incluso en momentos de elevado uso de la RPU. No funciona como un límite de uso, que puede impedir que se ejecuten las consultas. Solo limita los recursos de computación disponibles para el grupo de trabajo. Puede ver la capacidad utilizada durante un periodo de tiempo en el panel de Amazon Redshift sin servidor. Para obtener más información sobre la visualización de los datos de resumen, consulte Comprobación de los datos de resumen de Amazon Redshift sin servidor mediante el panel.
- La configuración de capacidad máxima se establece en 5632 RPU.

Cómo configurar la capacidad máxima

Puede configurar la capacidad máxima en la consola. Para un grupo de trabajo existente, puede cambiar la configuración en Configuración de grupos de trabajo. También puede utilizar la CLI para configurarlo mediante un comando como en el siguiente ejemplo:

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity
 512
```

Esto establece la configuración de capacidad máxima para el grupo de trabajo con el nombre correspondiente. Después de configurarlo, puede comprobar el valor en la consola para verificarlo. También puede comprobar el valor en la CLI ejecutando el comando `get-workgroup`.

Puede desactivar la configuración de capacidad máxima estableciéndola en `-1`, como a continuación:

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity -1
```

Monitoreo del uso y el costo de Amazon Redshift sin servidor

Hay varias formas de estimar el uso y la facturación de Amazon Redshift Serverless. Las vistas del sistema pueden ser útiles porque los metadatos del sistema, incluidos los datos de consulta y uso, son oportunos y no hay que configurar nada para consultarlos. CloudWatch también puede ser útil para el monitoreo del uso de la instancia de Amazon Redshift Serverless y tiene características adicionales para proporcionar información y configurar acciones.

Visualización del uso mediante la consulta de una vista del sistema

Consulte la tabla del sistema SYS_SERVERLESS_USAGE para realizar un seguimiento del uso y obtener los cargos por consultas:

```
select trunc(start_time) "Day",
(sum(charged_seconds)/3600::double
precision) * <Price for 1 RPU> as cost_incurred
from sys_serverless_usage
group by 1
order by 1
```

Esta consulta proporciona el costo por día incurrido para Amazon Redshift sin servidor, basado en el uso.

Notas de uso para determinar el uso y el costo

- Pagará por las cargas de trabajo que ejecuta en horas de RPU por segundo, con un cargo mínimo de 60 segundos.
- En los registros de la tabla del sistema sys_serverless_usage se muestran los costos incurridos en intervalos de tiempo de un minuto. Es importante comprender las siguientes columnas:

  La columna charged_seconds:

  - Proporciona los segundos de la unidad de computación (RPU) que se han cargado durante el intervalo de tiempo. Los resultados incluyen cualquier cargo mínimo en Amazon Redshift sin servidor.
  - Dispone de información sobre el uso de los recursos de computación una vez finalizadas las transacciones. Así, el valor de esta columna puede ser 0 si las transacciones no han finalizado.

  La columna compute_seconds:

  - Proporciona información sobre el uso de computación en tiempo real. Esto no incluye ningún cargo mínimo en Amazon Redshift sin servidor. Por lo tanto, puede diferir en cierta medida de los segundos facturados durante el intervalo.
  - Muestra la información de uso durante cada transacción (aunque esta no haya finalizado), por lo que los datos proporcionados son en tiempo real.
- Hay situaciones en las que compute_seconds es 0 pero charged_seconds es mayor que 0 o viceversa. Este es un comportamiento normal debido a la forma en que se graban los datos en

la vista del sistema. Para obtener una representación más precisa de los detalles del uso sin servidor, recomendamos agregar los datos en SYS_SERVERLESS_USAGE.

Para obtener más información sobre la supervisión de tablas y vistas, consulte Supervisión de consultas y cargas de trabajo con Amazon Redshift sin servidor.

Visualización del uso con CloudWatch

Puede utilizar las métricas disponibles en CloudWatch para hacer un seguimiento del uso. Las métricas generadas para CloudWatch son `ComputeSeconds`, que indica el total de segundos de RPU utilizados en el minuto actual, y `ComputeCapacity`, que indica la capacidad total de computación para ese minuto. Las métricas de uso también se pueden encontrar en la consola de Redshift en Redshift Serverless dashboard (Panel de Redshift Serverless). Para obtener más información sobre CloudWatch, consulte ¿Qué es Amazon CloudWatch?

Facturación del almacenamiento

La capacidad de almacenamiento principal se factura como Redshift Managed Storage (RMS). El almacenamiento se factura por GB al mes. La facturación del almacenamiento es independiente de la facturación de la capacidad recursos de computación. El almacenamiento que se utiliza para las instantáneas de los usuarios se factura con las tarifas estándar de facturación de las copias de seguridad, en función del nivel de uso.

Los costos de transferencia de datos y de machine learning (ML) se aplican por separado, al igual que los clústeres aprovisionados. La replicación de instantáneas y el uso compartido de datos entre regiones de AWS se facturan según las tarifas de transferencia indicadas en la página de precios. Para obtener más información, consulte Precios de Amazon Redshift.

Visualización del uso de facturación con CloudWatch

La métrica `SnapshotStorage`, que realiza un seguimiento del uso del almacenamiento de instantáneas, se genera y envía a CloudWatch. Para obtener más información sobre CloudWatch, consulte ¿Qué es Amazon CloudWatch?

Uso de la prueba gratuita de Amazon Redshift sin servidor

Amazon Redshift Serverless ofrece una prueba gratuita. Si participa en la prueba gratuita, puede ver el saldo de crédito de prueba gratuita en la consola de Redshift y comprobar el uso de la prueba gratuita en la vista del sistema SYS_SERVERLESS_USAGE. Tenga en cuenta que los detalles de

facturación para el uso de prueba gratuita no aparecen en la consola de facturación. Solo puede ver el uso en la consola de facturación una vez finalizada la prueba gratuita. Para obtener más información sobre la prueba gratuita de Amazon Redshift sin servidor, consulte Prueba gratuita de Amazon Redshift sin servidor.

Notas sobre la facturación de uso

- Registro del uso: una consulta o transacción solo se mide y registra después de que la transacción se complete, se revierta o se detenga. Por ejemplo, si una transacción se ejecuta durante dos días, el uso de RPU se registra después de que se complete. Puede supervisar el uso en curso en tiempo real si consulta `sys_serverless_usage`. El registro de las transacciones puede reflejarse como una variación del uso de RPU y afectar a los costos para horas específicas y para el uso diario.
- Escritura de transacciones explícitas: es importante, como práctica recomendada, finalizar las transacciones. Si no finaliza ni revierte una transacción abierta, Amazon Redshift Serverless sigue utilizando las RPU. Por ejemplo, si escribe un `BEGIN TRAN` explícito, es importante que estén las instrucciones `COMMIT` y `ROLLBACK` correspondientes.
- Consultas canceladas: si ejecuta una consulta y la cancela antes de que termine, se le sigue facturando el tiempo que se ha ejecutado la consulta.
- Escalado: la instancia de Amazon Redshift Serverless puede iniciar el escalado para manejar periodos de mayor carga, con el fin de mantener un rendimiento constante. La facturación de Amazon Redshift Serverless incluye tanto la capacidad base de computación como la capacidad escalada a la misma tasa de RPU.
- Reducir verticalmente: Amazon Redshift Serverless escala verticalmente desde su capacidad de RPU base para gestionar periodos de mayor carga. En algunos casos, la capacidad de RPU puede permanecer en una configuración superior durante un periodo después de que la carga de la consulta disminuya. Le recomendamos que establezca un máximo de horas de RPU en la consola para protegerse de costes inesperados.
- Tablas del sistema: cuando se consulta una tabla del sistema, se factura el tiempo de consulta.
- Redshift Spectrum: cuando se tiene Amazon Redshift Serverless y se realizan consultas, no se cobra por separado por las consultas del lago de datos. Para las consultas de datos almacenados en Amazon S3, el cargo es el mismo, por tiempo de transacción, que en las consultas de datos locales.
- Consultas federadas: las consultas federadas se cobran en términos de RPU utilizadas durante un intervalo de tiempo específico, de la misma manera que las consultas en el almacenamiento de datos o el lago de datos.

- Almacenamiento: el almacenamiento se factura por separado, por GB al mes.
- Cargo mínimo: el cargo mínimo es de 60 segundos de uso de recursos, contabilizado por segundos.
- Facturación de instantáneas: la facturación de instantáneas no cambia. Se cobra según el almacenamiento, facturado a una tasa de GB al mes. Puede restaurar su almacenamiento de datos a puntos específicos de las últimas 24 horas con una precisión de 30 minutos, de forma gratuita. Para obtener más información, consulte Precios de Amazon Redshift.

Prácticas recomendadas de Amazon Redshift Serverless para mantener la previsibilidad de la facturación

A continuación, se describen las prácticas recomendadas y las configuraciones integradas que leoayudarán a mantener la coherencia de la facturación.

- Asegúrese de finalizar cada transacción. Cuando usa `BEGIN` para iniciar una transacción, también es importante `END`.
- Use el control de errores de las prácticas recomendadas para responder correctamente a los errores y finalizar cada transacción. Minimizar las transacciones abiertas ayuda a evitar el uso innecesario de RPU.
- Use `SESSION TIMEOUT` para finalizar las transacciones abiertas y las sesiones inactivas. Hace que se agote el tiempo de espera de cualquier sesión inactiva durante más de 3600 segundos (1 hora). Hace que se agote el tiempo de espera de cualquier transacción que se mantenga abierta e inactiva durante más de 21 600 segundos (6 horas). Esta configuración de tiempo de espera se puede cambiar explícitamente para un usuario específico, por ejemplo, cuando desea mantener abierta una sesión para una consulta de larga duración. En el tema CREATE USER (CREAR USUARIO), se muestra cómo ajustar `SESSION TIMEOUT` para un usuario.
  - En la mayoría de los casos, le recomendamos que no amplíe el valor `SESSION TIMEOUT`, a menos que tenga un caso de uso que lo requiera específicamente. Si la sesión permanece inactiva, con una transacción abierta, puede dar lugar a un caso en que se utilicen RPU hasta que se cierre la sesión. Esto dará lugar a costos innecesarios.
  - Amazon Redshift sin servidor tiene un tiempo máximo de 86 399 segundos (24 horas) para una consulta en ejecución. El periodo máximo de inactividad de una transacción abierta es de seis horas antes de que Amazon Redshift sin servidor finalice la sesión asociada a la transacción. Para obtener más información, consulte Cuotas de objetos de Amazon Redshift Serverless.

Conexión a Amazon Redshift sin servidor

Una vez que haya configurado la instancia de Amazon Redshift sin servidor, puede conectarse a ella mediante una variedad de métodos, que se describen a continuación. Si dispone de varios equipos o proyectos y desea administrar los costos por separado, puede utilizar distintas Cuentas de AWS.

Para obtener una lista de las Regiones de AWS donde Amazon Redshift sin servidor está disponible, consulte los puntos de conexión enumerados para la API de Redshift sin servidor en la Referencia general de Amazon Web Services.

Amazon Redshift sin servidor se conecta al entorno sin servidor en la Cuenta de AWS en la Región de AWS actual. Amazon Redshift sin servidor se ejecuta en una VPC en los intervalos de puertos 5431 a 5455 y 8191 a 8215. El valor predeterminado es 5439. Actualmente, solo puede cambiar los puertos con la operación `UpdateWorkgroup` de la API y la operación `update-workgroup` de la AWS CLI.

Conexión a Amazon Redshift sin servidor

Se puede conectar a una base de datos (denominada `dev`) en Amazon Redshift sin servidor con la siguiente sintaxis.

```
workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:port/dev
```

Por ejemplo, la siguiente cadena de conexión especifica la región us-east-1.

```
default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev
```

Conexión a Amazon Redshift sin servidor por medio de controladores JDBC

Puede utilizar uno de los siguientes métodos para conectarse a Amazon Redshift sin servidor con el cliente SQL que prefiera mediante el controlador JDBC versión 2 proporcionado por Amazon Redshift.

Para conectarse con credenciales de inicio de sesión para la autenticación de la base de datos mediante el controlador JDBC versión 2.1.x o posterior, utilice la siguiente sintaxis. El número de puerto es opcional; si no se incluye, Amazon Redshift sin servidor tiene por defecto el número de puerto 5439. Puede cambiar a otro puerto del intervalo de puertos 5431-5455 u 8191-8215. Para cambiar el puerto predeterminado de un punto de conexión sin servidor, utilice la AWS CLI y la API de Amazon Redshift.

```
jdbc:redshift://workgroup-name.account-number.aws-region.redshift-
serverless.amazonaws.com:5439/dev
```

Por ejemplo, la siguiente cadena de conexión especifica el grupo de trabajo predeterminado, el ID de la cuenta 123456789012 y la región us-east-2.

```
jdbc:redshift://default.123456789012.us-east-2.redshift-serverless.amazonaws.com:5439/
dev
```

Para conectar con IAM a través del controlador JDBC versión 2.1.x o posterior, utilice la siguiente sintaxis. El número de puerto es opcional; si no se incluye, Amazon Redshift sin servidor tiene por defecto el número de puerto 5439. Puede cambiar a otro puerto del intervalo de puertos 5431-5455 u 8191-8215. Para cambiar el puerto predeterminado de un punto de conexión sin servidor, utilice la AWS CLI y la API de Amazon Redshift.

```
jdbc:redshift:iam://workgroup-name.account-number.aws-region.redshift-
serverless.amazonaws.com:5439/dev
```

Por ejemplo, la siguiente cadena de conexión especifica el grupo de trabajo predeterminado, el ID de la cuenta 123456789012 y la región us-east-2.

```
jdbc:redshift:iam://default.123456789012.us-east-2.redshift-
serverless.amazonaws.com:5439/dev
```

Para ODBC, utilice la siguiente sintaxis.

```
Driver={Amazon Redshift (x64)}; Server=workgroup-name.account-number.aws-
region.redshift-serverless.amazonaws.com; Database=dev
```

Si utiliza una versión del controlador JDBC anterior a 2.1.0.9 y se conecta con IAM, deberá utilizar la siguiente sintaxis.

```
jdbc:redshift:iam://redshift-serverless-<name>:aws-region/database-name
```

Por ejemplo, la siguiente cadena de conexión especifica el grupo de trabajo predeterminado y la us-east-1 de Región de AWS.

```
jdbc:redshift:iam://redshift-serverless-default:us-east-1/dev
```

Para obtener más información sobre los controladores, consulte Configuración de conexiones en Amazon Redshift.

Búsqueda de la cadena de conexión JDBC y ODBC

Para conectarse al grupo de trabajo con la herramienta de cliente SQL, debe tener la cadena de conexión JDBC u ODBC. Puede encontrar la cadena de conexión en la consola de Amazon Redshift sin servidor en la página de detalles de un grupo de trabajo.

Para encontrar la cadena de conexión de un grupo de trabajo

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En menú de navegación, elija Redshift sin servidor.
3. En el menú de navegación, elija Configuración de grupos de trabajo y, a continuación, el nombre del grupo de trabajo de la lista para abrir sus detalles.
4. Las cadenas de conexión de la URL de JDBC y la URL de ODBC están disponibles, junto con detalles adicionales, en la sección Información general. Cada cadena se basa en la región de AWS en la que se ejecuta el grupo de trabajo. Elija el icono situado junto a cadena de conexión adecuada para copiarla.

Conexión a Amazon Redshift sin servidor con la API de datos

También puede utilizar la API de datos de Amazon Redshift para conectarse a Amazon Redshift sin servidor. Use el parámetro `workgroup-name` en lugar del parámetro `cluster-identifier` en las llamadas a la AWS CLI.

Consulte Uso de la API de datos de Amazon Redshift para obtener más información acerca de la API de datos. Para ver el código de ejemplo que llama a la API de datos en Python y otros ejemplos, consulte Introducción a la API de datos de Redshift y busque en las carpetas `quick-start` y `use-cases` en GitHub.

Conexión con SSL a Amazon Redshift sin servidor

Configuración de una conexión segura con Amazon Redshift sin servidor

Para admitir las conexiones SSL, Redshift Serverless crea e instala un certificado SSL emitido por AWS Certificate Manager (ACM) para cada grupo de trabajo. La mayoría de los sistemas operativos,

navegadores web y clientes confían públicamente en los certificados ACM. No obstante, este cambio lo afectará en caso de que sus clientes o aplicaciones SQL se conectan a Redshift Serverless mediante SSL con el conjunto de opciones de conexión `sslmode` establecido como `require`, `verify-ca` o `verify-full`. Si su cliente necesita un certificado, Redshift Serverless proporciona un certificado de paquete de la siguiente manera:

- Descargue el paquete desde https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt.
  - El número de suma de comprobación MD5 esperado es 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - El número de suma de comprobación sha256 es 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  No utilice el paquete de certificados anterior que se encontraba en`https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.
- En la Región de AWS China, descargue el paquete desde https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt.
  - El número de suma de comprobación MD5 esperado es 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - El número de suma de comprobación sha256 es 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  No utilice los paquetes de certificados anteriores que se encontraban en `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` y `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`

> **Important**
>
> Redshift Serverless ha cambiado la forma en que se administran los certificados SSL. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los grupos de trabajo que usan SSL. Para obtener más información acerca de los certificados ACM para conexiones SSL, consulte Migración a certificados de ACM para las conexiones SSL.

De manera predeterminada, las bases de datos del grupo de trabajo aceptan una conexión, independientemente de que use una SSL o no.

Para crear un grupo de trabajo nuevo que solo acepte conexiones SSL, utilice el comando `create-workgroup` y defina el parámetro `require_ssl` como `true`. Para usar el ejemplo siguiente, sustituya *yourNamespaceName* por el nombre de su espacio de nombres y reemplace *yourWorkgroupName* por el nombre de su grupo de trabajo.

```
aws redshift-serverless create-workgroup \
--namespace-name yourNamespaceName \
--workgroup-name yourWorkgroupName \
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Para actualizar un grupo de trabajo existente de modo que solo acepte conexiones SSL, utilice el comando `update-workgroup` y defina el parámetro `require_ssl` como `true`. Tenga en cuenta que Redshift Serverless reiniciará el grupo de trabajo cuando actualice el parámetro `require_ssl`. Para usar el siguiente ejemplo, reemplace *yourWorkgroupName* por el nombre de su grupo de trabajo.

```
aws redshift-serverless update-workgroup \
--workgroup-name yourWorkgroupName \
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Amazon Redshift es compatible con el protocolo de acuerdo de clave de Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Con ECDHE, tanto el cliente como el servidor tienen un par de claves pública-privada de curva elíptica que se usa para establecer un código secreto compartido sobre un canal inseguro. No es necesario que configure nada en Amazon Redshift para habilitar ECDHE. Si se conecta desde una herramienta de cliente SQL que usa ECDHE para cifrar la comunicación entre el cliente y el servidor, Amazon Redshift usará la lista de cifrado proporcionada para realizar la conexión adecuada. Para obtener más información, consulte Elliptic Curve Diffie-Hellman en Wikipedia y Ciphers en el sitio web de OpenSSL.

Conexión con Amazon Redshift sin servidor desde un punto de conexión de VPC administrado por Amazon Redshift

Conexión a Amazon Redshift sin servidor desde otros puntos de conexión de la VPC

Para obtener información sobre cómo configurar un punto de conexión de VPC administrado para un grupo de trabajo de Amazon Redshift sin servidor, consulte Uso de puntos de conexión de la VPC administrados por Redshift.

Conexión a Amazon Redshift sin servidor desde un punto de conexión de VPC de Redshift en otra cuenta o región

Conexión a Amazon Redshift sin servidor entre puntos de conexión de VPC

Amazon Redshift sin servidor se aprovisiona en una VPC. Puede conceder acceso a una VPC de otra cuenta para acceder a Amazon Redshift sin servidor desde su cuenta. Es similar a una conexión desde un punto de conexión de VPC administrado, pero en este caso la conexión se origina, por ejemplo, desde un cliente de base de datos de otra cuenta. Puede realizar algunas operaciones:

- El propietario de una base de datos puede conceder acceso a una VPC que contenga Amazon Redshift sin servidor a otra cuenta de la misma región.
- El propietario de una base de datos puede revocar el acceso a Amazon Redshift sin servidor.

La principal ventaja del acceso entre cuentas es que permite una colaboración más sencilla entre las bases de datos. Los usuarios no tienen que estar aprovisionados en la cuenta que contiene la base de datos para acceder a ella, lo que reduce los pasos de configuración y ahorra tiempo.

Permisos necesarios para otorgarle acceso a una VPC en otra cuenta

Para conceder acceso o cambiar el acceso permitido, el otorgante debe tener una política de permisos asignada que incluya los siguientes permisos:

- redshift-serverless:PutResourcePolicy
- redshift-serverless:GetResourcePolicy
- redshift-serverless:DeleteResourcePolicy
- ec2:CreateVpcEndpoint
- ec2:ModifyVpcEndpoint

Es posible que necesite otros permisos que se especifican en la política administrada por AWS AmazonRedshiftFullAccess. Para obtener más información, consulte Concesión de permisos a Amazon Redshift Serverless.

El beneficiario debe tener una política de permisos asignada que incluya los siguientes permisos:

- redshift-serverless:ListWorkgroups
- redshift-serverless:CreateEndpointAccess

- redshift-serverless:UpdateEndpointAccess
- redshift-serverless:GetEndpointAccess
- redshift-serverless:ListEndpointAccess
- redshift-serverless:UpdateEndpointAccess

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Este es un ejemplo de política de recursos que se utiliza para configurar el acceso entre VPC:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountCrossVPCAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                   "123456789012",
                   "234567890123"
                ]
             },
            "Action": [
                "redshift-serverless:CreateEndpointAccess",
                "redshift-serverless:UpdateEndpointAccess",
                "redshift-serverless:DeleteEndpointAccess",
                "redshift-serverless:GetEndpointAccess"
            ],
            "Condition": {
                "ArnLike": {
                    "redshift-serverless:AuthorizedVpc": [
                        "arn:aws:ec2:us-east-1:123456789012:vpc/*",
                        "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-456",
                        "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-987"
                        ]
                    }
                }
            }
        }
    ]
```

```
}
```

Los procedimientos que se indican en esta sección suponen que el usuario que los realiza tiene asignados los permisos adecuados, por ejemplo, mediante un rol de IAM asignado que tiene los permisos enumerados. Los procedimientos también suponen que el grupo de trabajo tiene un rol de IAM asociado con los permisos de recursos adecuados.

Concesión de acceso de VPC a otras cuentas mediante la consola

Este procedimiento muestra los pasos para configurar el acceso a la base de datos si es el propietario de la base de datos y desea conceder el acceso a la misma.

Concesión del acceso desde la cuenta del propietario

1. En las propiedades del grupo de trabajo de Amazon Redshift sin servidor, en la pestaña Acceso a los datos hay una lista denominada Cuentas concedidas. Muestra las cuentas y las VPC a las que se les ha concedido acceso al grupo de trabajo. Busque la lista y elija Conceder acceso para añadir una cuenta a la lista.
2. Aparece una ventana en la que puede añadir la información del beneficiario. Indique el ID de la cuenta de AWS, que es el ID de 12 dígitos de la cuenta a la que quiere conceder acceso.
3. Conceda al beneficiario acceso a todas las VPC o a VPC específicas. Si concede acceso solo a VPC específicas, puedes añadir los ID introduciendo cada una de ellas y seleccionando Agregar VPC.
4. Cuando haya finalizado, seleccione Guardar los cambios.

Al guardar los cambios, la cuenta aparece en la lista Cuentas concedidas. La entrada muestra el ID de la cuenta y la lista de VPC a las que se ha concedido acceso.

El propietario de la base de datos también puede revocar el acceso a una cuenta. El propietario puede revocar el acceso en cualquier momento.

Revocación del acceso a una cuenta

1. Puede empezar desde la lista de cuentas concedidas. En primer lugar, seleccione una o varias cuentas.
2. Elija Revocar acceso.

Una vez concedido el acceso, el administrador de la base de datos del beneficiario puede comprobar la consola para determinar si tiene acceso.

Uso de la consola para confirmar que se le ha concedido el acceso para que pueda acceder a otra cuenta

1. En las propiedades del grupo de trabajo de Amazon Redshift sin servidor, en la pestaña Acceso a los datos hay una lista denominada Cuentas autorizadas. Muestra las cuentas a las que se puede acceder desde este grupo de trabajo. El beneficiario no puede usar la URL del punto de conexión del grupo de trabajo para acceder directamente al grupo de trabajo. Para acceder al grupo de trabajo, usted, como beneficiario, debe ir a la sección punto de conexión y elegir crear un punto de conexión.
2. A continuación, como beneficiario, debe proporcionar un nombre de punto de conexión y una VPC para acceder al grupo de trabajo.
3. Cuando el punto de conexión se haya creado correctamente, aparecerá en la sección puntos de conexión y tendrá una URL de punto de conexión. Puede utilizar esta URL de punto de conexión para acceder al grupo de trabajo.

Concesión de acceso a otras cuentas mediante los comandos de la CLI

La cuenta que concede el acceso debe conceder primero acceso a otra cuenta para poder conectarse mediante `put-resource-policy`. El propietario de la base de datos puede llamar a `put-resource-policy` para autorizar a otra cuenta a crear conexiones con el grupo de trabajo. Luego, la cuenta del beneficiario puede utilizar `create-endpoint-authorization` para crear conexiones con el grupo de trabajo a través de las VPC permitidas.

A continuación, se muestran las propiedades de `put-resource-policy` que puede llamar para permitir el acceso a una cuenta y una VPC específicas.

```
aws redshift-serverless put-resource-policy
--resource-arn <value>
--policy <value>
```

Tras llamar al comando, puede llamar a `get-resource-policy` y especificar el `resource-arn` para ver qué cuentas y VPC tienen permiso para acceder al recurso.

El beneficiario puede realizar la siguiente llamada. Muestra información sobre el acceso concedido. En concreto, devuelve una lista que contiene las VPC a las que se ha concedido acceso.

```
aws redshift-serverless list-workgroups
--owner-account <value>
```

El objetivo es que el beneficiario obtenga información de la cuenta del otorgante sobre las autorizaciones de los puntos de conexión. `owner-account` es la cuenta de uso compartido. Al ejecutar esta opción, devuelve las `CrossAccountVpcs` de cada grupo de trabajo, que es una lista de las VPC permitidas. A continuación se muestran todas las propiedades disponibles para un grupo de trabajo a modo de referencia:

```
Output: workgroup (Object)
workgroupId String,
workgroupArn String,
workgroupName String,
status: String,
namespaceName: String,
baseCapacity: Integer, (Not-applicable)
enhancedVpcRouting: Boolean,
configParameters: List,
securityGroupIds: List,
subnetIds: List,
endpoint: String,
publiclyAccessible: Boolean,
creationDate: Timestamp,
port: Integer,
CrossAccountVpcs: List
```

Note

Como recordatorio, la reubicación del clúster no es un requisito previo para configurar características de red de Redshift adicionales, como las que se utilizan para la recuperación de desastres u otros fines. Tampoco es necesario que lo active para habilitar lo siguiente:

- Conexión desde una VPC con varias cuentas o regiones a Redshift: puede conectarse desde una nube privada virtual (VPC) de AWS a otra que contenga una base de datos de Redshift, tal como se describe en esta sección.
- Configuración de un nombre de dominio personalizado: puede crear un nombre de dominio personalizado, también conocido como URL personalizada, para su clúster de Amazon Redshift o grupo de trabajo de Amazon Redshift sin servidor, a fin de que el nombre del

punto de conexión sea sencillo y más fácil de recordar. Para obtener más información, consulte Uso de un nombre de dominio personalizado para las conexiones de cliente.

Configuración de las opciones de tráfico de red adecuadas para Amazon Redshift sin servidor

Conectarse a Amazon Redshift sin servidor cuando sea de acceso público

Encontrará instrucciones para establecer la configuración del tráfico de red en Accesibilidad pública con configuración de grupo de seguridad predeterminada o personalizada. Aquí se incluye un caso de uso en el que el clúster es de acceso público.

Conectarse a Amazon Redshift sin servidor cuando no es de acceso público

Encontrará instrucciones para establecer la configuración del tráfico de red en Accesibilidad privada con configuración de grupo de seguridad predeterminada o personalizada. Aquí se incluye un caso de uso en el que el clúster no está disponible en Internet.

Definición de roles de base de datos para concederlos a los usuarios federados en Amazon Redshift sin servidor

Puede definir roles en su organización que determinen qué roles de base de datos conceder en Amazon Redshift sin servidor. Para obtener más información, consulte Definición de roles de base de datos para concederlos a los usuarios federados en Amazon Redshift sin servidor.

Recursos adicionales

Para obtener más información sobre las conexiones seguras a Amazon Redshift sin servidor, incluida la concesión de permisos, la autorización de acceso a servicios adicionales y la creación de roles de IAM, consulte Identity and access management en Amazon Redshift Serverless.

Definición de roles de base de datos para concederlos a los usuarios federados en Amazon Redshift sin servidor

Cuando forma parte de una organización, tiene un conjunto de roles asociados. Por ejemplo, tiene roles para su puesto de trabajo, como programador y administrador. Sus roles determinan a qué

aplicaciones y datos tiene acceso. La mayoría de las organizaciones utilizan un proveedor de identidades, como Microsoft Active Directory, para asignar roles a los usuarios y los grupos. El uso de roles para controlar el acceso a los recursos ha aumentado, porque las organizaciones no tienen que ocuparse tanto de administrar a los usuarios individuales.

Recientemente, se incorporó el control de acceso basado en roles en Amazon Redshift sin servidor. Con los roles de base de datos, puede proteger el acceso a datos y objetos, como esquemas o tablas, por ejemplo. O puede utilizar roles con el fin de definir un conjunto de permisos elevados, por ejemplo, para un monitor del sistema o un administrador de bases de datos. Pero después de conceder permisos de recursos a los roles de base de datos, hay un paso adicional, que consiste en conectar los roles de un usuario de la organización a los roles de base de datos. Puede asignar cada usuario a sus roles de base de datos en el momento del registro inicial mediante la ejecución de instrucciones SQL, pero supone mucho esfuerzo. Una forma más sencilla consiste en definir los roles de base de datos que se van a conceder y pasarlos a Amazon Redshift sin servidor. Tiene la ventaja de simplificar el proceso de inicio de sesión inicial.

Puede pasar roles a Amazon Redshift sin servidor mediante `GetCredentials`. Cuando un usuario inicia sesión por primera vez en una base de datos de Amazon Redshift sin servidor, se crea un usuario de base de datos asociado y se asigna a los roles de base de datos correspondientes. En este tema se detalla el mecanismo para pasar roles a Amazon Redshift sin servidor.

Pasar roles de base de datos tiene un par de casos de uso principales:

- Cuando un usuario inicia sesión a través de un proveedor de identidades de terceros, normalmente con la federación configurada, y pasa los roles mediante una etiqueta de sesión.
- Cuando un usuario inicia sesión a través de las credenciales de inicio de sesión de IAM y sus roles se pasan mediante una clave y un valor de etiqueta.

Para obtener más información sobre el control de acceso basado en roles, consulte Control de acceso basado en roles (RBAC).

Configuración de roles de base de datos

Para poder pasar roles a Amazon Redshift sin servidor, debe configurar los roles de base de datos en su base de datos y concederles los permisos adecuados en los recursos de base de datos. Por ejemplo, en un escenario sencillo, puede crear un rol de base de datos denominado ventas y concederle acceso para consultar tablas con datos de ventas. Para obtener más información sobre cómo crear roles de base de datos y conceder permisos, consulte CREATE ROLE y GRANT.

Casos prácticos para definir los roles de base de datos que se concederán a los usuarios federados

En estas secciones se describe un par de casos de uso en los que pasar roles de base de datos a Amazon Redshift sin servidor puede simplificar el acceso a los recursos de base de datos.

Inicio de sesión con un proveedor de identidades

En el primer caso de uso se supone que su organización dispone de identidades de usuario en un servicio de administración de identidades y accesos. Este servicio puede estar basado en la nube, por ejemplo, JumpCloud u Okta, o en las instalaciones, como Microsoft Active Directory. El objetivo es asignar automáticamente los roles de un usuario del proveedor de identidades a sus roles de base de datos cuando inicie sesión con un cliente como el Editor de consultas V2, por ejemplo, o con un cliente JDBC. Para configurar esto, debe llevar a cabo un par de tareas de configuración. Estos incluyen los siguientes:

1. Configure la integración federada con su proveedor de identidades (IdP) mediante una relación de confianza. Es un requisito previo. Al efectuar esta configuración, el proveedor de identidades se encarga de autenticar al usuario mediante una aserción SAML y de proporcionarle credenciales de inicio de sesión. Para obtener más información, consulte Integración de proveedores de soluciones SAML externos con AWS. También puede encontrar más información en Federar el acceso al Editor de consultas de Amazon Redshift V2 con los Servicios de federación de Active Directory (AD FS) o Federar el acceso de inicio de sesión único al Editor de consultas de Amazon Redshift v2 con Okta.
2. El usuario debe tener los siguientes permisos de política:
   - `GetCredentials`: proporciona credenciales de autorización temporal para iniciar sesión en Amazon Redshift sin servidor.
   - `sts:AssumeRoleWithSAML`: proporciona un mecanismo para vincular un almacén o directorio de identidades empresariales al acceso de AWS basado en rol.
   - `sts:TagSession`: permiso para la acción de sesión de etiqueta, en la entidad principal del proveedor de identidades.

   En este caso, `AssumeRoleWithSAML` devuelve un conjunto de credenciales de seguridad para los usuarios que se han autenticado mediante una respuesta autenticada mediante SAML. Esta operación proporciona un mecanismo para vincular un almacén o directorio de identidades al acceso de AWS basado en roles sin credenciales específicas de usuario. En el caso de los

usuarios con permiso para `AssumeRoleWithSAML`, el proveedor de identidades es responsable de administrar la aserción SAML que se utiliza para pasar la información de rol.

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

3. Configure la etiqueta `RedshiftDbRoles` con los valores de rol separados por dos puntos, con el formato rol1:rol2. Por ejemplo, `manager:engineer`. Pueden recuperarse de una implementación de etiquetas de sesión configurada en su proveedor de identidades. La solicitud de autenticación SAML pasa los roles mediante programación. Para obtener más información sobre cómo pasar etiquetas de sesión, consulte Transferencia de etiquetas de sesión en AWS STS.

   Si pasa un nombre de rol que no existe en la base de datos, se ignorará.

En este caso de uso, cuando un usuario inicia sesión mediante una identidad federada, sus roles se pasan en la solicitud de autorización a través de la clave y el valor de la etiqueta de sesión. Posteriormente, tras la autorización, `GetCredentials` pasa los roles a la base de datos. Tras una conexión correcta, se asignan los roles de base de datos y el usuario puede realizar las tareas de base de datos correspondientes a su rol. La parte esencial de la operación es que a la etiqueta de sesión `RedshiftDbRoles` se le asignan los roles en la solicitud de autorización inicial. Para obtener más información sobre cómo pasar etiquetas de sesión, consulte Traspaso de etiquetas de sesión mediante AssumeRoleWithSAML.

Inicio de sesión con credenciales de IAM

En el segundo caso de uso, se pueden pasar roles a un usuario y este puede acceder a una aplicación cliente de base de datos a través de las credenciales de IAM.

1. El usuario que inicie sesión en este caso debe tener asignados permisos de política para las siguientes acciones:
   - `tag:GetResources`: devuelve los recursos etiquetados asociados a las etiquetas especificadas.
   - `tag:GetTagKeys`: devuelve las claves de etiqueta actualmente en uso.

     Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

2. También se requieren permisos de permiso para acceder al servicio de base de datos, como Amazon Redshift sin servidor.
3. Para este caso de uso, configure los valores de las etiquetas para sus roles en AWS Identity and Access Management. Puede elegir editar las etiquetas y crear una clave de etiqueta denominada RedshiftDbRoles con una cadena de valores de etiqueta adjunta que contenga los roles. Por ejemplo, manager:engineer.

Cuando un usuario inicia sesión, su rol se agrega a la solicitud de autorización y se pasa a la base de datos. Se asigna a un rol de base de datos existente.

Recursos adicionales de

Como se mencionó en los casos de uso, puede configurar la relación de confianza entre su IdP y AWS. Para obtener más información, consulte Configuración de una relación de confianza para usuario autenticado y agregación de notificaciones en el proveedor de identidades SAML 2.0.

Identity and access management en Amazon Redshift Serverless

El acceso a Amazon Redshift requiere credenciales que AWS puede utilizar para autenticar las solicitudes. Estas credenciales deben tener permisos para obtener acceso a los recursos de AWS, como Amazon Redshift Serverless.

En las siguientes secciones, se proporcionan detalles acerca del uso de AWS Identity and Access Management (IAM) y Amazon Redshift para ayudar a proteger los recursos mediante el control de quién puede acceder a ellos. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Concesión de permisos a Amazon Redshift Serverless

Para obtener acceso a los servicios de AWS, Amazon Redshift Serverless requiere permisos.

Autorización a Amazon Redshift Serverless para obtener acceso a otros servicios de AWS en su nombre

Algunas características de Amazon Redshift requieren que este servicio acceda a otros servicios de AWS en su nombre. Para que la instancia de Amazon Redshift Serverless actúe en su nombre, proporciónele credenciales de seguridad. El método preferido para proporcionar credenciales de seguridad consiste en especificar un rol de AWS Identity and Access Management (IAM). También puede crear un rol de IAM a través de la consola de Amazon Redshift y configurarlo

como predeterminado. Para obtener más información, consulte Creación de un rol de IAM como predeterminado para Amazon Redshift.

Para obtener acceso a otros servicios de AWS, cree un rol de IAM con los permisos adecuados. También es necesario asociar el rol con Amazon Redshift Serverless. Además, especifique el nombre de recurso de Amazon (ARN) del rol cuando ejecute el comando de Amazon Redshift o especifique la palabra clave `default`.

Cuando modifique la relación de confianza para el rol de IAM en https://console.aws.amazon.com/iam/, asegúrese de que contiene `redshift-serverless.amazonaws.com` y `redshift.amazonaws.com` como nombres de servicio de entidades principales. Para obtener información general acerca de cómo administrar los roles de IAM para acceder a otros servicios de AWS en su nombre, consulte Autorización a Amazon Redshift para obtener acceso a otros servicios de AWS en su nombre.

Creación de un rol de IAM como predeterminado para Amazon Redshift

Cuando crea roles de IAM a través de la consola de Amazon Redshift, este servicio crea los roles mediante programación en su Cuenta de AWS. Además, Amazon Redshift les adjunta automáticamente políticas existentes administradas por AWS. Este enfoque significa que puede permanecer dentro de la consola de Amazon Redshift y no tiene que cambiar a la consola de IAM para crear roles.

El rol de IAM que crea a través de la consola para su clúster tiene la política administrada `AmazonRedshiftAllCommandsFullAccess` adjunta de forma automática. Este rol de IAM permite a Amazon Redshift copiar, descargar, consultar y analizar datos de los recursos de AWS de su cuenta de IAM. Los comandos relacionados incluyen COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL y CREATE LIBRARY. Para obtener más información acerca de cómo crear un rol de IAM como predeterminado para Amazon Redshift, consulte Creación de un rol de IAM como predeterminado para Amazon Redshift.

Para comenzar a crear un rol de IAM como predeterminado para Amazon Redshift, abra la AWS Management Console, elija la consola de Amazon Redshift y, a continuación, elija Redshift sin servidor en el menú Puede crear un grupo de trabajo nuevo desde el panel de control Sin servidor. Los pasos de creación permiten seleccionar un rol de IAM o configurar uno nuevo.

Cuando ya tenga un grupo de trabajo de Amazon Redshift sin servidor y desee configurar roles de IAM para él, abra la AWS Management Console. Elija la consola de Amazon Redshift y, a continuación, seleccione Redshift sin servidor. En la consola de Amazon Redshift sin servidor, elija

Configuración de espacio de nombres para un grupo de trabajo existente. En Seguridad y cifrado, puede editar los permisos.

Asignación de roles de IAM a un espacio de nombres

Cada rol de IAM es una identidad de AWS con políticas de permisos que determinan qué acciones puede realizar cada rol en AWS. La intención del rol es que cualquier persona que lo necesite lo pueda asumir. Además, cada espacio de nombres es un conjunto de objetos, como tablas, esquemas y usuarios. Cuando utiliza Amazon Redshift Serverless, puede asociar varios roles de IAM al espacio de nombres. Esto facilita la estructuración de los permisos de forma adecuada para una recopilación de objetos de base de datos, de modo que los roles puedan realizar acciones tanto en datos internos como externos. Por ejemplo, para que pueda ejecutar un comando `COPY` en una base de datos de Amazon Redshift para recuperar datos de Amazon S3 y rellenar una tabla de Redshift.

Puede asociar varios roles a un espacio de nombres mediante la consola, tal y como se describe anteriormente en esta sección. También puede utilizar el comando `CreateNamespace` de la API o el comando `create-namespace` de la CLI. Con el comando de la API o CLI puede asignar roles de IAM al espacio de nombres rellenando `IAMRoles` con uno o varios roles. En concreto, se agregan ARN para roles específicos a la recopilación.

Administración de roles de IAM asociados con el espacio de nombres

En AWS Management Console puede administrar políticas de permisos para roles en AWS Identity and Access Management. Puede administrar roles de IAM para el espacio de nombres, con la configuración disponible en Namespace configuration (Configuración de espacio de nombres). Para obtener más información acerca de los espacios de nombres y su uso en Amazon Redshift Serverless, consulte Información general de los grupos de trabajo y espacios de nombres de Amazon Redshift sin servidor.

Introducción a las credenciales de IAM para Amazon Redshift

Cuando inicie sesión en la consola de Amazon Redshift por primera vez y pruebe Amazon Redshift sin servidor, tendrá la posibilidad de acceder como usuario con un rol de IAM adjunto que tenga las políticas necesarias. Una vez que comience la creación de una instancia de Amazon Redshift sin servidor, Amazon Redshift registra el nombre de rol de IAM que haya utilizado al iniciar sesión. Puede utilizar las mismas credenciales para iniciar sesión en la consola de Amazon Redshift y en la consola de Amazon Redshift sin servidor.

Al crear la instancia de Amazon Redshift Serverless, puede crear una base de datos. Utilice el editor de consultas v2 para conectarse a la base de datos mediante la opción de credenciales temporales.

Si desea agregar un nuevo nombre de usuario administrador y una contraseña que se mantenga para la base de datos, elija Customize admin user credentials (Personalizar credenciales de usuario administrador) e ingrese un nuevo nombre de usuario administrador y una contraseña para este.

Para comenzar a utilizar Amazon Redshift sin servidor y crear un grupo de trabajo y un espacio de nombres en la consola por primera vez, utilice un rol de IAM con una política de permisos adjunta. Asegúrese de que este rol cuente con el permiso de administrador `arn:aws:iam::aws:policy/AdministratorAccess` o con el permiso pleno de Amazon Redshift `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess` que se adjunta a la política de IAM.

En los siguientes escenarios, se describe la forma en que Amazon Redshift Serverless emplea sus credenciales de IAM una vez que comienza a utilizar la consola de Amazon Redshift Serverless:

- Si elige Use default settings (Utilizar configuración predeterminada): Amazon Redshift Serverless traduce su identidad de IAM actual a un superusuario de base de datos. Puede utilizar la misma identidad de IAM con la consola de Amazon Redshift Serverless para realizar acciones de superusuario en la base de datos de Amazon Redshift Serverless.
- Si elige Customize settings (Personalizar configuración) sin especificar el Admin user name (Nombre de usuario administrador) ni la contraseña de Amazon Redshift Serverless, se utilizan las credenciales de IAM actuales como credenciales de usuario administrador predeterminadas.
- Si elige Customize settings (Personalizar configuración) y especifica Nombre de usuario administrador y contraseña Amazon Redshift Serverless: Amazon Redshift Serverless traduce su identidad de IAM actual en un superusuario de base de datos. Asimismo, Amazon Redshift Serverless crea otro par de nombre de usuario y contraseña de inicio de sesión a largo plazo también como superusuario. Puede utilizar su identidad de IAM actual o el par de nombre de usuario y contraseña creado para acceder a su base de datos como superusuario.

Administración del acceso a objetos de base de datos de Amazon Redshift sin servidor con permisos de rol de base de datos

En este procedimiento se muestra cómo conceder permiso para consultar una tabla mediante un rol de base de datos de Amazon Redshift. El rol se asigna mediante una etiqueta que se asocia a un usuario en IAM y se transmite a Amazon Redshift cuando inicia sesión. Es una explicación con ejemplos de los conceptos de Definición de roles de base de datos para conceder a usuarios federados en Amazon Redshift sin servidor. La ventaja de completar estos pasos es que puede asociar un usuario a un rol de base de datos y evitar establecer sus permisos para cada objeto de

base de datos. Simplifica la administración de la capacidad del usuario para consultar, modificar o agregar datos a las tablas y realizar otras acciones.

En el procedimiento se supone que ya ha configurado una base de datos de Amazon Redshift sin servidor y que tiene capacidad para conceder permisos en la base de datos. También se supone que tiene permisos para crear un usuario de IAM en la consola de AWS, para crear un rol de IAM y para asignar permisos de políticas.

1. Cree un usuario de IAM, mediante la consola de IAM. Más tarde, se conectará a la base de datos con este usuario.
2. Cree un rol de base de datos de Redshift, mediante el editor de consultas v2 u otro cliente SQL. Para obtener más información acerca de cómo crear roles de base de datos, consulte CREATE ROLE.

   ```
   CREATE ROLE urban_planning;
   ```

   Consulte la vista de sistema SVV_ROLES para comprobar que su rol se ha creado. También devuelve roles de sistema.

   ```
   SELECT * from SVV_ROLES;
   ```
3. Conceda al rol de base de datos que ha creado permiso para seleccionar en una tabla. (El usuario de IAM que haya creado acabará accediendo y seleccionando registros de la tabla mediante el rol de base de datos). El nombre de rol y el nombre de tabla en el siguiente ejemplo de código son muestras. Aquí se concede permiso para seleccionar de una tabla denominada `cities`.

   ```
   GRANT SELECT on TABLE cities to ROLE urban_planning;
   ```
4. Utilice la consola de AWS Identity and Access Management para crear un rol de IAM. Este rol concede permiso para utilizar el editor de consultas v2. Cree un nuevo rol de IAM y, para el tipo de entidad de confianza, elija Cuenta de AWS. A continuación, elija Esta cuenta. Conceda al rol los siguientes permisos de política:

   - `AmazonRedshiftReadOnlyAccess`
   - `tag:GetResources`
   - `tag:GetTagKeys`

- Todas las acciones para sqlworkbench, como `sqlworkbench:ListDatabases` y `sqlworkbench:UpdateConnection`.

5. En la consola de IAM, agregue una etiqueta con la Clave `RedshiftDbRoles` al usuario de IAM que creó anteriormente. El valor de la etiqueta debe coincidir con el rol de base de datos que creó en el primer paso. Es `urban_planning` en la muestra.

Una vez completados estos pasos, asigne el rol de IAM al usuario que ha creado en la consola de IAM. Cuando el usuario inicia sesión en la base de datos con el editor de consultas v2, su nombre de rol de base de datos que figura en la etiqueta se pasa a Amazon Redshift y se le asocia. De este modo, puede consultar las tablas adecuadas mediante el rol de base de datos. Para ilustrarlo, el usuario de esta muestra puede consultar la tabla `cities` a través del rol de base de datos `urban_planning`.

Migrar un clúster aprovisionado a Amazon Redshift Serverless

Para migrar de un clúster aprovisionado a Amazon Redshift Serverless, consulte los pasos que se indican a continuación.

Creación de una instantánea del clúster aprovisionado

Para transferir datos del clúster aprovisionado a Amazon Redshift Serverless, cree una instantánea del clúster aprovisionado y, a continuación, restaure la instantánea en Amazon Redshift Serverless. Amazon Redshift convierte automáticamente las claves intercaladas en claves compuestas al restaurar una instantánea de clúster aprovisionada en un espacio de nombres sin servidor.

> **Note**
>
> Antes de migrar los datos a un grupo de trabajo sin servidor, asegúrese de que las necesidades de clústeres aprovisionados sean compatibles con la cantidad de RPU que elija en Amazon Redshift sin servidor.

Para crear una instantánea del clúster aprovisionado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija Create snapshot (Crear instantánea).
3. Introduzca las propiedades de la definición de instantánea, luego seleccione Create snapshot (Crear instantánea). La instantánea puede tardar un poco en estar disponible.

Para restaurar una instantánea de clúster aprovisionada en un espacio de nombres sin servidor:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. Comience en la consola del clúster aprovisionado de Amazon Redshift y diríjase a las páginas Clusters (Clústeres), Snapshots (Instantáneas).
3. Elija la instantánea que desea utilizar.
4. Elija Restore snapshot (Restaurar instantánea), Restore to serverless namespace (Restaurar al espacio de nombres sin servidor).
5. Elija un espacio de nombres en el cual restaurar la instantánea.
6. Confirme que desea restaurar desde su instantánea. Esta acción reemplaza todas las bases de datos en su punto de conexión sin servidor por los datos de su clúster aprovisionado. Elija Restore (Restaurar).

Para obtener más información sobre las instantáneas del clúster aprovisionado, consulte Instantáneas de Amazon Redshift.

Conexión a Amazon Redshift sin servidor con un controlador

Para conectarse a Amazon Redshift Serverless con el cliente SQL de su preferencia, puede utilizar el controlador JDBC versión 2 proporcionado por Amazon Redshift. Le recomendamos conectarse mediante el controlador JDBC versión 2.1.x o posterior. El número de puerto es opcional. Si no lo incluye, Amazon Redshift Serverless utiliza el puerto número 5439 de forma predeterminada. Puede cambiar a otro puerto del intervalo de puertos 5431-5455 u 8191-8215. Para cambiar el puerto predeterminado de un punto de conexión sin servidor, utilice la AWS CLI y la API de Amazon Redshift.

Para encontrar el punto de conexión exacto que se debe utilizar para el controlador JDBC, ODBC o Python, consulte Configuración de grupos de trabajo en Amazon Redshift sin servidor. También puede utilizar la operación `GetWorkgroup` de la API de Amazon Redshift sin servidor o la operación

`get-workgroups` de la AWS CLI para devolver información sobre el grupo de trabajo y, a continuación, conectarse.

Conexión mediante autenticación basada en contraseña

Para conectarse mediante autenticación basada en contraseña, utilice la sintaxis a continuación.

```
jdbc:redshift://<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com:5439/?username=enter a username&password=enter a password
```

Para conectarse mediante el controlador Python de Amazon Redshift, utilice la siguiente sintaxis.

```
import redshift_connector
with redshift_connector.connect(
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>',
    user='enter a user',
    password='enter a password'
    # port value of 5439 is specified by default
) as conn:
    pass
```

Conexión mediante IAM

Si prefiere iniciar sesión con IAM, utilice el siguiente punto de conexión del controlador. Este punto de conexión del controlador le permite conectarse a una base de datos específica y utiliza la operación de la API `GetCredentials` de Amazon Redshift Serverless

```
jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com:5439/<database-name>
```

Este punto de conexión del controlador no admite la personalización `dbUser`, `dbGroup` y `auto-create`. De forma predeterminada, el controlador crea automáticamente usuarios de la base de datos al iniciar sesión y los asigna a grupos de acuerdo con los grupos que haya definido en IAM. Nota: Los nombres de grupos que especifique en IAM deben contener solo letras minúsculas, números, guion bajo (“_”), signo más (“+”), punto (“.”), símbolo arroba (@) o guion (“-”). De lo contrario, es posible que el controlador no se conecte `dbGroup`.

Asegúrese de que su identidad de AWS tenga la política de IAM correcta para la acción `RedshiftServerlessGetCredentials`. A continuación, se muestra una política de IAM de

ejemplo que concede los permisos correctos a una identidad de AWS para conectarse a Amazon Redshift Serverless. Para obtener más información sobre los permisos de IAM, consulte Agregar permisos de identidad de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": "redshift-serverless:GetCredentials",
            "Resource": "*"
        }
    ]
}
```

Conexión mediante IAM con dbUser y dbGroups

Si desea utilizar opciones de conexión dbUser y dbGroups personalizados, utilice el siguiente punto de conexión del controlador. Al igual que el otro punto de conexión del controlador de Amazon Redshift Serverless, esta sintaxis crea automáticamente usuarios de base de datos al iniciar sesión. Este punto de conexión del controlador utiliza la operación `GetCredentials` de la API de Amazon Redshift sin servidor. El recurso dbUser debe comenzar por una letra, solo debe contener caracteres alfanuméricos, guion bajo (“_”), signo más (“+”), punto (“.”), símbolo arroba (“@”) o guion (“-”), y debe tener menos de 128 caracteres. El recurso dbGroups solo puede contener letras en minúscula, números, guion bajo (“_”), signo más (“+”), punto (“.”), símbolo arroba (@) o guion.

```
jdbc:redshift:iam://redshift-serverless-<workgroup-name>:<aws-region>/<database-name>
```

Para conectarse mediante el controlador Python de Amazon Redshift, utilice la siguiente sintaxis.

```
import redshift_connector
with redshift_connector.connect(
    iam=True,
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>',
    db_user='enter a user',
    password='enter a password',
    db_groups='<db-groups>'
    # port value of 5439 is specified by default
```

```
) as conn:
    pass
```

Conexión mediante ODBC

Para conectarse a través de ODBC, utilice la siguiente sintaxis.

```
Driver={Amazon Redshift (x64)}; Server=<workgroup-name>.<account-number>.<aws-
region>.redshift-serverless.amazonaws.com; Database=dev
```

Uso del SDK de Amazon Redshift Serverless

Si escribió scripts de administración con el SDK de Amazon Redshift, debe utilizar el nuevo SDK de Amazon Redshift sin servidor para administrar Amazon Redshift sin servidor. Para obtener más información sobre las operaciones de la API disponibles, consulte la Guía de referencia de la API de Amazon Redshift Serverless.

Información general de los grupos de trabajo y espacios de nombres de Amazon Redshift sin servidor

Para aislar cargas de trabajo y administrar distintos recursos en Amazon Redshift sin servidor, puede crear espacios de nombres y grupos de trabajo y administrar los recursos de almacenamiento e informáticos de forma independiente.

Información general de los grupos de trabajo y espacios de nombres de Amazon Redshift sin servidor

El espacio de nombres es una recopilación de objetos de base de datos y usuarios. El espacio de nombres relacionado con el almacenamiento agrupa esquemas, tablas, usuarios o claves de AWS Key Management Service para cifrar datos. Las propiedades de almacenamiento incluyen el nombre de la base de datos y la contraseña del usuario administrador, los permisos y el cifrado y la seguridad. Otros recursos agrupados en espacios de nombres incluyen recursos compartidos de datos, puntos de recuperación y límites de uso. Puede configurar estas propiedades de almacenamiento mediante la consola de Amazon Redshift sin servidor, la AWS Command Line Interface o las API de Amazon Redshift sin servidor para el recurso específico.

El grupo de trabajo es una recopilación de recursos informáticos. El grupo de trabajo relacionado con la informática agrupa recursos informáticos como RPU, grupos de subredes de VPC y grupos

de seguridad. Las propiedades del grupo de trabajo incluyen la configuración de redes y seguridad. Otros recursos en grupos de trabajo incluyen límites de acceso y uso. Puede configurar estas propiedades informáticas mediante la consola de Amazon Redshift sin servidor, AWS Command Line Interface o las API de Amazon Redshift sin servidor.

Puede crear uno o varios espacios de nombres y grupos de trabajo. Cada espacio de nombres solo puede tener asociado un grupo de trabajo. De igual forma, cada grupo de trabajo solo puede tener asociado un espacio de nombres.

Introducción a Amazon Redshift sin servidor con la consola

La configuración de Amazon Redshift sin servidor implica seguir varios pasos de configuración. Cuando se siguen los pasos para configurar Amazon Redshift sin servidor, se crea un espacio de nombres y un grupo de trabajo y se asocian entre sí. Para empezar la configuración de Amazon Redshift sin servidor mediante la consola de Amazon Redshift sin servidor, puede elegir Get started with Amazon Redshift sin servidor (Introducción a Amazon Redshift sin servidor) para configurarlo y empezar a interactuar con él. Puede elegir un entorno con la configuración predeterminada, lo que permite una configuración más rápida o configurar explícitamente los ajustes según los requisitos de la organización. Durante este proceso, se especifica la configuración del grupo de trabajo y del espacio de nombres.

Después de configurar el entorno, Propiedades de grupo de trabajo y Propiedades de espacio de nombres le ayudan a familiarizarse con la configuración.

Administración de grupos de trabajo y espacios de nombres mediante la AWS Command Line Interface y la API de Amazon Redshift sin servidor

Aparte de utilizar la consola de AWS, también puede utilizar la AWS CLI o la API de Amazon Redshift sin servidor para interactuar con los grupos de trabajo y los espacios de nombres. En la siguiente tabla, se enumeran las operaciones de la API y la CLI que puede usar para administrar las instantáneas y los puntos de recuperación.

Operación de la API	Command de la CLI	Descripción
CreateNamespace	create-namespace	Crea un espacio de nombres. De forma predeterminada, Amazon Redshift sin servidor crea espacios de nombres

Operación de la API	Command de la CLI	Descripción
		con una clave de AWS Key Management Service predeterminada, pero puede especificar otra clave para cifrar los datos. También puede crear un espacio de nombres restaurando una instantánea. Para obtener más información, consulte Uso de instantáneas y puntos de recuperación.
UpdateNamespace	update-namespace	Actualiza un espacio de nombres.
GetNamespace	get-namespace	Obtiene información de un espacio de nombres.
ListNamepaces	list-namespaces	Obtiene información de una lista de espacios de nombres.
DeleteNamespace	delete-namespace	Elimina un espacio de nombres.
CreateWorkgroup	create-workgroup	Crea un grupo de trabajo. Al crear un grupo de trabajo, asegúrese de tener un espacio de nombres que pueda asociar al grupo de trabajo. Al crear el grupo de trabajo, puede especific ar cualquier recurso de computación, como subredes, grupos de seguridad o RPU.
UpdateWorkgroup	update-workgroup	Actualiza un grupo de trabajo.

Operación de la API	Command de la CLI	Descripción
GetWorkgroup	get-workgroup	Obtiene información de un grupo de trabajo.
ListWorkgroups	list-workgroups	Obtiene información de una lista de grupos de trabajo.
DeleteWorkGroup	delete-workgroup	Elimina un grupo de trabajo.

Administración de Amazon Redshift sin servidor mediante la consola

Para crear, editar y eliminar su almacenamiento de datos de Amazon Redshift sin servidor, utilice Serverless dashboard (Panel Sin servidor) de la consola de Amazon Redshift. El acceso a la configuración individual de la consola depende de su rol de IAM y de sus permisos.

Para obtener información sobre cómo configurar Amazon Redshift sin servidor, consulte Configuración de Amazon Redshift sin servidor por primera vez. Para obtener información sobre la creación y configuración de grupos de trabajo, consulte Uso de los grupos de trabajo. Para obtener información sobre la configuración de los espacios de nombres, consulte Uso de espacios de nombres.

Configuración de Amazon Redshift sin servidor por primera vez

La primera vez que seleccione Serverless dashboard (Panel Sin servidor), le guiará por los pasos para configurar Amazon Redshift sin servidor. En Get started with the serverless experience (Introducción a la experiencia sin servidor), puede configurar su almacenamiento de datos de Amazon Redshift sin servidor, utilizando un conjunto de datos de muestra. Amazon Redshift sin servidor carga automáticamente el conjunto de datos de muestra durante el proceso de creación. Una vez creado el almacenamiento de datos, podrá consultarlos inmediatamente. Para obtener más información sobre cómo configurar Amazon Redshift sin servidor por primera vez, consulte Configurar Amazon Redshift sin servidor por primera vez.

Uso de los grupos de trabajo

Para aislar las cargas de trabajo y administrar los recursos en Amazon Redshift sin servidor, puede crear grupos de trabajo y espacios de nombres. El grupo de trabajo relacionado con la computación agrupa recursos de computación como RPU y grupos de subredes de VPC. Si no ha creado un grupo de trabajo ni un espacio de nombres y busca instrucciones que muestren cómo comenzar a utilizar Amazon Redshift sin servidor, consulte Configuración de Amazon Redshift sin servidor por primera vez.

Creación de un grupo de trabajo con un espacio de nombres

En estos pasos se supone que ha completado la configuración inicial de Amazon Redshift sin servidor. Si no ha creado un grupo de trabajo ni un espacio de nombres y busca instrucciones que muestren cómo comenzar a utilizar Amazon Redshift sin servidor, consulte Configuración de Amazon Redshift sin servidor por primera vez.

Complete los siguientes pasos para crear un grupo de trabajo:

1. Elija Serverless dashboard (Panel Sin servidor). A continuación, elija Create workgroup (Crear grupo de trabajo).
2. Ingrese el nombre del grupo de trabajo.
3. Elija una Virtual private cloud (VPC) (Nube privada virtual [VPC]) para Amazon Redshift sin servidor. Esto asigna el grupo de trabajo a una red virtual específica del entorno de AWS. Para obtener más información acerca de VPC, consulte Información general sobre VPC y subredes.
4. Elija uno o varios VPC security groups (Grupos de seguridad de la VPC). Para obtener más información, consulte Control del tráfico hacia los recursos mediante grupos de seguridad.
5. En Subnet (Subred), especifique una o varias subredes para asociarlas a la base de datos. Estas subredes están contenidas en la VPC que eligió anteriormente y deben estar en tres zonas de disponibilidad distintas. Para obtener más información, consulte Consideraciones al usar Amazon Redshift sin servidor.
6. Seleccione la capacidad RPU base que se ajuste a sus necesidades.

Elección de un espacio de nombres

1. Elija Create a new namespace (Crear un nuevo espacio de nombres) e ingrese el nombre del espacio de nombres o Add to an existing namespace (Agregar a un espacio de nombres existente) y seleccione el espacio de nombres en la lista desplegable.

2. Para Database name and password (Contraseña y nombre de la base de datos), especifique el nombre de la primera base de datos. También puede especificar un administrador que no sea el administrador de la consola predeterminado, editando las Admin user credentials (Credenciales de usuario administrador).
3. Para Permissions (Permisos), se elige Associate IAM role (Asociar rol de IAM) para asociar roles de IAM específicos con el espacio de nombres y grupo de trabajo. Para obtener más información acerca de la asociación de roles de IAM con Amazon Redshift, consulte Identity and access management in Amazon Redshift (Administración de identidades y accesos en Amazon Redshift).
4. Puede personalizar la configuración de cifrado creando una nueva clave o eligiendo una clave distinta de la predeterminada. Para Audit logging (Registro de auditoría), elija los registros que se exportarán. Cada tipo de registro especifica metadatos diferentes. Elija Continue (Continuar) para revisar sus elecciones.

Revisar selecciones de grupos de trabajo

1. Revise la configuración en Review and create (Revisar y crear). Muestra la configuración que eligió en los pasos anteriores.
2. Elija Guardar.

Después de crear el grupo de trabajo, se agrega a la lista de Workgroups (Grupos de trabajo).

Crear un grupo de trabajo de vista previa

Para probar las nuevas características de Amazon Redshift sin servidor, cree un grupo de trabajo de Amazon Redshift sin servidor en Vista previa. No puede utilizar esas características en producción ni trasladar su grupo de trabajo de Preview (Versión preliminar) a un grupo de trabajo de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

Las siguientes características están disponibles actualmente en los grupos de trabajo de versión preliminar:

- Uso de integraciones sin ETL

Para crear un grupo de trabajo en Preview (Versión preliminar)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Panel sin servidor y Configuración de grupos de trabajo. Se enumeran los grupos de trabajo de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada grupo de trabajo en columnas.
3. Un banner en la página de configuración del grupo de trabajo presenta los grupos de trabajo de vista previa. Elija el botón Create preview workgroup (Crear grupo de trabajo de versión preliminar) para abrir la página de creación de grupos de trabajo.
4. Ingrese las propiedades de su grupo de trabajo. Le recomendamos que ingrese un nombre para el grupo de trabajo que indique que está en versión preliminar. Elija las opciones de su grupo de trabajo, incluidas las etiquetadas como -preview (-versión preliminar), para las características que desee probar. Continúe por las páginas para ingresar opciones para su grupo de trabajo y espacio de nombres. Para obtener información general acerca de la creación de grupos de trabajo, consulte the section called “Creación de un grupo de trabajo con un espacio de nombres”.
5. Elija Crear grupo de trabajo en vista previa para crear un grupo de trabajo de vista previa.
6. Cuando el grupo de trabajo de versión preliminar esté disponible, utilice su cliente SQL para cargar y consultar los datos.

Para obtener información sobre la versión preliminar en clústeres aprovisionados, consulte Crear un clúster de vista previa.

Visualización de las propiedades de un grupo de trabajo

En Amazon Redshift sin servidor, un grupo de trabajo es una recopilación de recursos disponibles para su uso. Cuando elige Amazon Redshift sin servidor, en la consola de AWS, puede elegir Workgroup configuration (Configuración del grupo de trabajo) del menú de navegación para ver una lista. Puede utilizar el cuadro Search (Búsqueda) para buscar grupos de trabajo que cumplan los criterios de búsqueda. Cada entrada de grupo de trabajo tiene algunas propiedades que se muestran:

- Workgroup (Grupo de trabajo): el nombre del grupo de trabajo. Puede seleccionarlo para ver y editar las propiedades del grupo de trabajo.
- Status (Estado): muestra si el grupo de trabajo está disponible.

- Namespace (Espacio de nombres): el espacio de nombres asociado al grupo de trabajo. Cada grupo de trabajo está asociado a un espacio de nombres.
- Creation date (Fecha de creación): la fecha en que se creó el grupo de trabajo.
- Etiquetas: etiquetas asociadas al grupo de trabajo.

Propiedades de grupo de trabajo

Puede mostrar grupos de trabajo eligiendo Workgroup configuration (Configuración de grupos de trabajo) en el menú de la izquierda. A continuación, puede elegir un grupo de trabajo de la lista. Varios paneles muestran las propiedades del grupo de trabajo. También puede realizar acciones. General information (Información general) muestra lo siguiente:

- Workgroup (Grupo de trabajo): el nombre del grupo de trabajo.
- Namespace (Espacio de nombres): el espacio de nombres asociado al grupo de trabajo. Puede elegirlo para ver sus propiedades. Un grupo de trabajo está asociado a un único espacio de nombres.
- Date created (Fecha de creación): cuándo se creó el grupo de trabajo.
- Status (Estado): indica si los recursos del grupo de trabajo están disponibles. Si están disponibles, puede conectar con un cliente en la instancia de Amazon Redshift sin servidor, para consultar datos o crear recursos de base de datos o conectarse con el editor de consultas v2.
- Endpoint (Punto de conexión): la URL.
- JDBC URL: la URL para establecer conexiones de cliente de JDBC. Puede utilizar esta URL para conectarse con un controlador JDBC para Amazon Redshift. Para obtener más información, consulte Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.
- ODBC URL (URL de ODBC): la URL para establecer conexiones de cliente de ODBC. Contiene propiedades, como la base de datos y el ID de usuario, y sus valores.
- Versión de grupo de trabajo y de parche: Amazon Redshift sin servidor publica periódicamente nuevas versiones y parches. Puede usar los números de versión del grupo de trabajo y del parche para realizar un seguimiento de las actualizaciones de software de su grupo de trabajo de Amazon Redshift sin servidor. Para obtener más información sobre los cambios y las características de parches específicos, consulte Versiones en clúster para Amazon Redshift.

La pestaña de Data access (Acceso a los datos) contiene varios paneles:

- Network and security (Redes y seguridad): puede ver las propiedades de la red, como el identificador de la Virtual private cloud (VPC) (Nube privada virtual [VPC]), la lista del VPC security group (Grupo de seguridad de la VPC), el Enhanced VPC routing (Enrutamiento de la VPC mejorado) y la configuración Publicly accessible (Accesible públicamente). Si elige Edit (Editar), puede cambiar esta configuración. Además, puede seleccionar Turn on enhanced VPC routing (Activar el enrutamiento de VPC mejorado), que enruta el tráfico de red entre la base de datos sin servidor y los repositorios de datos a través de una VPC, para mejorar la privacidad y la seguridad. También puede seleccionar Turn on Public Accessible (Activar acceso público), que hace que la base de datos sea accesible públicamente desde fuera de la VPC, lo que permite la conexión de instancias y dispositivos.
- Redshift managed VPC endpoints (Puntos de conexión de VPC administrada por Redshift): puede crear puntos de conexión de VPC administrados para acceder a Amazon Redshift sin servidor desde otra VPC.

La pestaña Limits (Límites) tiene ajustes para controlar la capacidad y los límites de uso de Amazon Redshift sin servidor. Contiene los siguientes paneles:

- Base capacity in Redshift processing units (RPUs) (Capacidad base en unidades de procesamiento de Redshift [RPU]): puede establecer la capacidad base de los recursos informáticos utilizada para el procesamiento de la carga de trabajo. Para obtener más información, consulte Descripción de la capacidad de Amazon Redshift Serverless.
- Límites de uso: puede configurar hasta cuatro límites para el número máximo de recursos de computación que la instancia de Amazon Redshift sin servidor puede utilizar en un período de tiempo y seleccionar las acciones que Amazon Redshift sin servidor debe realizar cuando alcance esos límites. Por ejemplo, puede configurar su grupo de trabajo para que tenga dos límites, uno de 500 horas de RPU y otro de 900 horas de RPU. Puede hacer que Amazon Redshift sin servidor le envíe una alerta cuando alcance el primer límite de 500 horas de RPU y, a continuación, desactivar las consultas de los usuarios cuando alcance el segundo límite de 900 horas. Estos límites ayudan a controlar los costos y que sean más predecibles.
- Query limits (Límites de consulta): puede configurar límites en las consultas, como la configuración de tiempo de espera. Estos límites le ayudan a optimizar los costos y el rendimiento.

La pestaña Pestañas incluye el panel Etiquetas, que muestra todas las etiquetas que ha creado para su grupo de trabajo. Para obtener más información acerca del etiquetado de recursos, consulte Información general de recursos de etiquetado.

Eliminación de un grupo de trabajo

Puede eliminar un grupo de trabajo con la consola. Antes de hacerlo, asegúrese de tener una copia de seguridad de los datos y las instantáneas instaladas. Los recursos eliminados como parte del grupo de trabajo en muchos casos no se pueden recuperar.

Realice los siguientes pasos:

1. Elija Amazon Redshift sin servidor (Amazon Redshift sin servidor), elija Workgroup configuration (Configuración de grupo de trabajo) y elija Delete Amazon Redshift sin servidor instance (Eliminar instancia de Amazon Redshift sin servidor).

2. Se abre un diálogo. Cuando elige eliminar el grupo de trabajo, se eliminan todos los límites de uso, se eliminan todos los puntos de conexión de VPC y se elimina el acceso a los puntos de conexión de VPC.

   Escriba eliminar y seleccione Delete (Eliminar) para confirmar.

Una vez completados los pasos, el estado del grupo de trabajo es Deleting (Eliminación) y un banner indica que el grupo de trabajo se está eliminando. Mientras el proceso de eliminación está en curso, algunas características en el Serverless dashboard (Panel sin servidor) están desactivadas. Pero puede configurar los clústeres aprovisionados en Provisioned clusters dashboard (Panel de clústeres aprovisionados).

Después de eliminar el grupo de trabajo, no aparece con el espacio de nombres. Puede elegir el botón Create workgroup (Crear grupo de trabajo) para crear uno nuevo.

Puede eliminar un grupo de trabajo existente y asociar un nuevo grupo de trabajo con una configuración diferente al mismo espacio de nombres. Al crear el nuevo grupo de trabajo, elija la capacidad base que funciona con el tamaño de los datos asociados al espacio de nombres.

Puede asociar un grupo de trabajo a un espacio de nombres que se creó con una clave administrada por el cliente (CMK). Para obtener más información sobre AWS KMS, consulte conceptos de AWS KMS.

Uso de espacios de nombres

En Amazon Redshift sin servidor, un espacio de nombres define un contenedor lógico para objetos de base de datos. Puede contener tablas, grupos de trabajo y otros recursos de bases de datos.

Si no ha creado un grupo de trabajo ni un espacio de nombres y busca instrucciones sobre cómo comenzar a utilizar Amazon Redshift sin servidor, consulte Configuración de Amazon Redshift sin servidor por primera vez.

Búsqueda de un espacio de nombres

En el menú de Amazon Redshift, puede elegir de la lista de Espacios de nombres para ver o editar las propiedades de un espacio de nombres. La información de la consola incluye el nombre del espacio de nombres, el nombre del administrador y otras propiedades.

La configuración y las propiedades de un espacio de nombres se encuentran en varias pestañas. Estos incluyen los siguientes:

- Workgroup (Grupo de trabajo): muestra los grupos de trabajo asociados al espacio de nombres.
- Data back up (Copia de seguridad de datos): puede configurar y crear instantáneas y configurar puntos de recuperación.
- Security and encryption (Seguridad y cifrado): puede administrar los permisos de rol de IAM y ver o editar la configuración de seguridad y cifrado. Estos incluyen el estado de la clave de cifrado y la configuración de registro de auditoría.
- Datashares (Recursos compartidos de datos): muestra recursos compartidos de datos.

Propiedades de espacio de nombres

En Amazon Redshift sin servidor, un espacio de nombres define un contenedor para objetos de base de datos. Puede elegir Namespace configuration (Configuración de espacio de nombres) de la lista de navegación, elija un espacio de nombres de la lista y edite su configuración.

La información general para el espacio de nombres incluye lo siguiente:

- Namespace (Espacio de nombres): el nombre.
- Namespace ID (ID de espacio de nombres): el identificador único.
- ARN: un identificador único que se utiliza para especificar el recurso en AWS. Contiene propiedades como la región y el servicio.
- Status (Estado): el estado, como Available (Disponible).
- Date created (Fecha de creación): la fecha en que se creó el espacio de nombres.
- Storage used (Almacenamiento utilizado): el espacio de almacenamiento utilizado por el espacio de nombres y todos sus objetos.

- Admin user name (Nombre de usuario administrador): la cuenta de administrador. Normalmente esta es la cuenta que se utiliza para crear el espacio de nombres.
- Database name (Nombre de base de datos): el nombre de la base de datos que contiene el espacio de nombres.
- Total table count (Recuento total de tablas): la cantidad de tablas que hay en todos los esquemas.

La configuración y las propiedades adicionales del espacio de nombres se encuentran en varias pestañas. Estos incluyen los siguientes:

- Workgroup (Grupo de trabajo): muestra el grupo de trabajo asociado al espacio de nombres.
- Data back up (Copia de seguridad de datos): en este panel, puede configurar y crear instantáneas y configurar puntos de recuperación.
- Security and encryption (Seguridad y cifrado): puede administrar los permisos de rol de IAM y ver o editar la configuración de seguridad y cifrado. Incluyen el estado de la clave de cifrado y la configuración para activar el registro de auditoría. Para obtener más información acerca del registro de auditoría de Amazon Redshift sin servidor, consulte Audit logging for Amazon Redshift sin servidor (Registro de auditoría para Amazon Redshift sin servidor).
- Datashares (Recursos compartidos de datos): muestra recursos compartidos de datos. Con el uso compartido de datos, puede proporcionar acceso a los datos sin necesidad de copiarlos o moverlos. Para obtener más información sobre el uso compartido de datos, consulte Uso compartido de datos en Amazon Redshift sin servidor.

Edición de la seguridad y el cifrado

Amazon Redshift sin servidor está protegido mediante cifrado KMS. Puede actualizar la configuración de cifrado a través de la consola:

1. Elija Namespace configuration (Configuración del espacio de nombres) en el menú principal de la consola, elija el espacio de nombres que desea editar y elija Edit (Editar) en la pestaña Security and encryption (Seguridad y cifrado). Aparecerá un cuadro de diálogo.
2. Puede seleccionar Personalizar la configuración de cifrado y, a continuación, Elegir una clave administrada por el cliente de AWS) para cambiar la clave utilizada para cifrar los recursos.
3. Para Audit logging (Registro de auditoría), elija los registros que se exportarán. Cada tipo de registro especifica metadatos diferentes.
4. Para completar la actualización de la configuración, elija Save changes (Guardar cambios).

Cambio de la clave de AWS KMS de un espacio de nombres

En Amazon Redshift, el cifrado protege los datos en reposo. Amazon Redshift sin servidor utiliza cifrado de claves de AWS KMS automáticamente para cifrar los recursos y las instantáneas de Amazon Redshift sin servidor. Como práctica recomendada, la mayoría de las organizaciones revisan el tipo de datos que almacenan y tienen planes de rotar las claves de cifrado según lo programado. La frecuencia de la rotación de las claves puede variar, en función de las políticas de seguridad de datos. Amazon Redshift sin servidor admite cambiar la clave de AWS KMS del espacio de nombres para que pueda cumplir con las políticas de seguridad de la organización.

Cuando cambie la clave de AWS KMS, los datos permanecen sin cambios.

Cambio de una clave de AWS KMS mediante la consola

En Amazon Redshift, el cifrado protege los datos en reposo. Amazon Redshift sin servidor utiliza cifrado de claves de AWS KMS automáticamente para cifrar Amazon Redshift sin servidor y las instantáneas. Como práctica recomendada, la mayoría de las organizaciones revisan el tipo de datos que almacenan y tienen planes de rotar las claves de cifrado según lo programado. La frecuencia de la rotación de las claves puede variar, en función de las políticas de seguridad de datos. Amazon Redshift sin servidor admite cambiar la clave de AWS KMS del espacio de nombres para que pueda cumplir con las políticas de seguridad de la organización.

Cuando cambie la clave de AWS KMS, los datos permanecen sin cambios.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Namespace configuration (Configuración de espacio de nombres). Elija el espacio de nombres de la lista.
3. Desde la pestaña Security and encryption (Seguridad y cifrado), elija Edit (Editar).
4. Elija Customize encryption settings (Personalizar configuración de cifrado) y, a continuación, elija una clave para el espacio de nombres. Como opción, puede crear una nueva clave.

Cambio de claves de cifrado de AWS KMS mediante la AWS CLI

Use `update-namespace` para cambiar la clave de AWS KMS para el espacio de nombres. A continuación, se muestra la sintaxis del comando:

```
aws redshift-serverless update-namespace
```

```
--namespace-name
[--kms-key-id <id-of-kms-key>]
// other parameters omitted here
```

Debe crear un espacio de nombres o el comando de la CLI produce un error.

El tiempo que tarda en cambiar la clave depende de la cantidad de datos de Amazon Redshift sin servidor. Esto suele tardar quince minutos por 8 TB de datos almacenados.

Limitaciones

No puede cambiar de una clave KMS administrada por el cliente a una clave de AWS KMS. En este caso, tiene que crear un nuevo espacio de nombres.

No puede realizar otras acciones mientras se cambia la clave.

Eliminación de un espacio de nombres

Si desea eliminar un espacio de nombres con un grupo de trabajo asociado, primero debe eliminar el grupo de trabajo.

En la consola de Amazon Redshift sin servidor, siga los pasos que se indican a continuación:

1. Elija Namespace configuration (Configuración de espacio de nombres) en el menú de la izquierda y, a continuación, elija el espacio de nombres que desee eliminar de la lista.
2. Elija Actions (Acciones) y, a continuación, elija Delete namespace (Eliminar espacio de nombres).
3. Se abre un cuadro de diálogo. Puede conservar los datos creando una instantánea manual antes de completar la operación de eliminación.

   Escriba eliminar y seleccione Delete (Eliminar) para confirmar.

Administración de los límites de uso, los límites de consulta y otras tareas administrativas

Puede establecer la configuración en la consola para controlar el uso y limitar el costo.

Administración de los límites de uso, incluido el establecimiento de límites de RPU

En la pestaña Limits (Límites) para un grupo de trabajo, puede agregar uno o varios límites de uso para controlar el máximo de RPU que utiliza en un periodo de tiempo determinado o para establecer un límite de uso compartido de datos.

1. Elija Manage usage limits (Administración de los límites de uso). La sección de límites aparece en la parte inferior del panel Uso de computación por período.
2. Configure un límite de uso en número de horas de RPU.
3. Elija una Frecuencia, que puede ser Diaria, Semanal o Mensual. Esto establece el periodo de tiempo del límite de uso. Elegir Daily (Diaria) en este caso, le proporciona un control más detallado.
4. Configure un límite de uso, en número de horas.
5. Configure la acción. Son lo que se muestra a continuación:

   - Log to system table (Registrar en la tabla del sistema): agregue un registro a una tabla del sistema, que puede consultar para determinar si se supera el límite.
   - Alert (Alerta): utiliza Amazon SNS para configurar suscripciones de notificaciones y enviar notificaciones si se incumple un límite. Puede elegir un tema de Amazon SNS existente o crear uno nuevo.
   - Turn off user queries (Desactivar las consultas de los usuarios): desactiva las consultas para detener el uso de Amazon Redshift sin servidor. También envía una notificación.

   Las dos primeras acciones son informativas, pero la última desactiva el procesamiento de consultas.
6. De forma opcional, puede establecer un Cross-Region data sharing usage limit (Límite de uso compartido de datos entre regiones), que limita la cantidad de datos transferidos de la región productora a la región de consumo que pueden consultar los consumidores. Para hacer esto, elija Add limit (Agregar límite) y siga los pasos.
7. Para guardar el límite, elija Guardar los cambios en la parte inferior de la página.
8. Configure hasta tres límites más según sea necesario.

Para obtener más información conceptual sobre las RPU y la facturación, consulte Facturación de Amazon Redshift sin servidor.

Administración de los límites de consultas

En la pestaña Limits (Límites) de un grupo de trabajo, puede agregar un límite para supervisar el rendimiento y los límites. Para obtener más información sobre los límites de supervisión de consultas, consulte Reglas de supervisión de consultas de WLM.

1. Elija Manage query limits (Administrar límites de consultas). Elija Add new limit (Agregar nuevo límite) en el cuadro de diálogo Manage query limits (Administrar límites de consulta).
2. Elija el tipo de límite que desea establecer e ingrese un valor para su límite correspondiente.
3. Elija Save changes (Guardar cambios) para guardar el límite.

Cuando cambie el límite de consultas y los parámetros de configuración, la base de datos se reiniciará.

Consultas de filtrado

Puede utilizar los filtros disponibles en el panel sin servidor. Para filtrar las consultas, realice los siguientes pasos.

1. A la izquierda del panel Query summary (Resumen de consultas), seleccione la lista desplegable para filtrar por consultas completadas, consultas con error o ambos tipos.
2. A la derecha del panel Query summary (Resumen de consultas), seleccione la lista desplegable para filtrar por consultas en ejecución, consultas en cola o ambos tipos.

Cambio de la contraseña de administrador

1. Elija Namespace configuration (Configuración del espacio de nombres). A continuación, elija Change admin password (Cambiar la contraseña de administrador). Aparecerá un cuadro de diálogo.
2. Puede especificar New admin username (Nuevo nombre de usuario administrador) y New admin user password (Nueva contraseña de usuario administrador).
3. Elija Guardar.

Comprobación de los datos de resumen de Amazon Redshift sin servidor mediante el panel

El panel de Amazon Redshift sin servidor contiene una colección de paneles que muestran de un vistazo métricas e información sobre su grupo de trabajo y espacio de nombres. Estos paneles incluyen lo siguiente:

- Resources summary (Resumen de recursos): muestra información de alto nivel sobre Amazon Redshift sin servidor, como el almacenamiento utilizado y otras métricas.
- Query summary (Resumen de consultas): muestra información sobre las consultas, incluidas las completadas y las que se están ejecutando. Elija View details (Ver detalles) para ir a una pantalla con filtros adicionales.
- RPU capacity used (Capacidad de RPU utilizada): muestra la capacidad global utilizada durante un periodo de tiempo determinado, como las diez horas anteriores, por ejemplo.
- Datashares (Recursos compartidos de datos): muestra el recuento de recursos compartidos de datos, que se utilizan para compartir datos entre, por ejemplo, las cuentas de AWS. Las métricas muestran qué recursos compartidos de datos requieren autorización y otra información.
- Uso total de computación: muestra el total de horas de RPU consumidas por el grupo de trabajo seleccionado en un intervalo de tiempo determinado, hasta los últimos 7 días.

Desde el panel puede profundizar rápidamente en estas métricas disponibles para comprobar un detalle relativo a Amazon Redshift sin servidor o revisar las consultas o hacer un seguimiento de los elementos de trabajo.

Monitoreo de consultas y cargas de trabajo con Amazon Redshift sin servidor

Supervisión de consultas y carga de trabajo con Amazon Redshift sin servidor

Puede monitorear las consultas y la carga de trabajo de Amazon Redshift sin servidor con las vistas del sistema que se proporcionan.

Concesión de acceso a consultas de supervisión

Un superusuario puede proporcionar acceso a los usuarios que no son superusuarios para que puedan realizar la supervisión de consultas para todos los usuarios. En primer lugar, debe agregar una política para un usuario o un rol con objeto de proporcionar acceso a la supervisión de consultas. A continuación, conceda permiso de supervisión de consultas al usuario o rol.

Para agregar la política de supervisión de consultas

1. Elija https://console.aws.amazon.com/iam/.
2. En Access management (Administración de acceso), seleccione Policies (Políticas).
3. Seleccione Crear política.
4. Elija la pestaña JSON (JSON) y pegue la siguiente definición de política:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
    "redshift-data:ExecuteStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListDatabases"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "redshift-serverless:GetCredentials",
"Resource": "*"
}
]
}
```

5. Elija Revisar política.
6. En Name (Nombre), especifique un nombre para la política, como `query-monitoring`.
7. Elija Crear política.

Después de crear la política, tendrá la posibilidad de acceder a los permisos adecuados.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para conceder permiso de supervisión de consultas a un usuario

Los usuarios con el permiso `sys:monitor` pueden ver todas las consultas. Además, los usuarios con el permiso `sys:operator` pueden cancelar consultas, analizar el historial de consultas y realizar operaciones de limpieza.

1. Ingrese el siguiente comando para proporcionar acceso de supervisión del sistema, donde user-name es el nombre del usuario para el que desea proporcionar acceso.

   ```
   grant role sys:monitor to "IAM:user-name";
   ```

2. (Opcional) Ingrese el siguiente comando para proporcionar acceso de operación del sistema, donde user-name es el nombre del usuario para el que desea proporcionar acceso.

   ```
   grant role sys:operator to "IAM:user-name";
   ```

Para conceder permiso de supervisión de consultas a un rol

Los usuarios con un rol que tengan el permiso `sys:monitor` pueden ver todas las consultas. Además, los usuarios con un rol que tengan el permiso `sys:operator` pueden cancelar consultas, analizar el historial de consultas y realizar operaciones de limpieza.

1. Ingrese el siguiente comando para proporcionar acceso de supervisión del sistema, donde role-name es el nombre del rol para el que desea proporcionar acceso.

```
grant role sys:monitor to "IAMR:role-name";
```

2. (Opcional) Ingrese el siguiente comando para proporcionar acceso de operación del sistema, donde role-name es el nombre del rol para el que desea proporcionar acceso.

```
grant role sys:operator to "IAMR:role-name";
```

Vistas de supervisión

Las vistas de supervisión son vistas del sistema en Amazon Redshift sin servidor que se utilizan para supervisar el uso de consulta y carga de trabajo. Estas vistas se encuentran en el esquema `pg_catalog`. Las vistas del sistema disponibles se han diseñado con el objetivo de proporcionar la información necesaria que permita monitorear Amazon Redshift sin servidor, lo que resulta mucho más sencillo de lo que se requiere en el caso de los clústeres aprovisionados. Las vistas del sistema SYS se han diseñado para que funcionen con Amazon Redshift sin servidor. Para mostrar la información que proporcionan estas vistas, ejecute las instrucciones SELECT de SQL.

Las vistas del sistema se definen para que sean compatibles con los siguientes objetivos de supervisión.

Supervisión de cargas de trabajo

Puede supervisar las actividades de consulta a lo largo del tiempo para lo siguiente:

- comprender los patrones de carga de trabajo, de modo que conozca lo que es normal (base de referencia) y lo que está dentro de los acuerdos de nivel de servicio de la empresa (SLA)
- identificar rápidamente cualquier desviación de la normalidad, que puede suponer un problema transitorio o que requiere medidas adicionales

Supervisión de la carga y descarga de datos

El movimiento de datos dentro y fuera de Amazon Redshift sin servidor constituye una función esencial. Se utilizan las funciones COPY y UNLOAD para cargar o descargar datos, y se debe supervisar de cerca el progreso en términos de bytes o filas transferidas y archivos completados con el fin de hacer un seguimiento del cumplimiento de los SLA de la empresa. Para ello, se suelen realizar consultas a las tablas del sistema con frecuencia (es decir, a cada minuto) para hacer un seguimiento del progreso y emitir alertas a efectos de investigación o acción correctiva si se detectan desviaciones significativas.

Diagnóstico de errores y problemas

En algunos casos, es necesario tomar medidas en caso de errores de consulta o de ejecución. Los desarrolladores cuentan con las tablas del sistema para diagnosticar automáticamente los problemas y determinar las soluciones adecuadas en cada caso.

Ajuste del rendimiento

Es posible que tenga que ajustar las consultas que no cumplen con los requisitos del SLA, ya sea desde el principio o que se han degradado con el tiempo. Para ajustarlas, debe disponer de los detalles del tiempo de ejecución, incluidos el plan de ejecución, las estadísticas, la duración y el consumo de recursos. Necesita datos de referencia de las consultas problemáticas para determinar la causa de tal desviación y orientarle sobre el modo de mejorar el rendimiento.

Supervisión de eventos de objetos del usuario

Es necesario monitorear las acciones y actividades en los objetos del usuario como la actualización de las vistas materializadas, el vacío y el análisis. En este caso, se incluyen los eventos administrados por el sistema, como la actualización automática de las vistas materializadas. Se desea monitorear el momento en que termina un evento si es iniciado por el usuario o la última ejecución correcta si es iniciado por el sistema.

Seguimiento del uso para la facturación

Puedes supervisar tus tendencias de uso a lo largo del tiempo para lo siguiente:

- informar sobre la planificación de presupuestos y las estimaciones de expansión de la empresa
- identificar posibles oportunidades de ahorro, como la eliminación de datos inactivos

Use las vistas del sistema SYS para monitorear Amazon Redshift sin servidor. Para obtener más información sobre las vistas de monitoreo de SYS, consulte Vistas de monitoreo de SYS.

Registro de auditoría para Amazon Redshift sin servidor

Exportación de registros

Puede configurar Amazon Redshift sin servidor para exportar datos de registro de conexión, usuario y actividad de usuario a un grupo de registros en Amazon CloudWatch Logs. Con Amazon CloudWatch Logs, puede realizar análisis en tiempo real de los datos de registro y utilizar CloudWatch para crear alarmas y ver métricas. Puede utilizar CloudWatch Logs para almacenar los registros en un almacenamiento de larga duración.

Puede crear alarmas de CloudWatch para realizar un seguimiento de sus métricas mediante la consola de Amazon Redshift. Para obtener más información sobre la creación de alarmas, consulte Administración de alarmas.

Para exportar los datos de registro generados a Registros de Amazon CloudWatch, los registros respectivos se deben seleccionar para su exportación en los ajustes de configuración de Amazon Redshift sin servidor, en la consola. Para ello, seleccione las opciones de Configuración de espacio de nombres, en Seguridad y cifrado.

Supervisión de eventos de registro en CloudWatch

Una vez seleccionados los registros de Redshift que se exportarán, puede supervisar los eventos en Amazon CloudWatch Logs. A continuación, se crea automáticamente un nuevo grupo de registro para Amazon Redshift sin servidor, en el que `log_type` representa el tipo de registro.

```
/aws/redshift/<namespace>/<log_type>
```

Cuando cree su primer grupo de trabajo y espacio de nombres, el nombre predeterminado será el del espacio de nombres. El nombre del grupo de registro varía en función de cómo llame al espacio de nombres.

Por ejemplo, si exporta el registro de conexiones, los datos de registro se almacenan en el siguiente grupo de registro.

```
/aws/redshift/default/connectionlog
```

Los eventos de registro se exportan a un grupo de registro mediante el flujo de registro sin servidor. El comportamiento depende de cuál de las siguientes condiciones es true (verdadera):

- Existe un grupo de registros con el nombre especificado. Redshift exporta datos de registro mediante el grupo de registro existente. Puede utilizar la configuración automática, como la que proporciona AWS CloudFormation. para crear grupos de registros con periodos de retención de registros predefinidos, filtros de métricas y acceso de clientes.
- No existe un grupo de registros con el nombre especificado. Cuando se detecta una entrada de registro coincidente en el registro de la instancia, Amazon Redshift sin servidor crea automáticamente un nuevo grupo de registros en Amazon CloudWatch Logs. El grupo de registros utiliza el periodo de retención de registros predeterminado de Never Expire (Nunca caduca). Utilice la consola de Amazon CloudWatch Logs, la AWS CLI o la API de Amazon CloudWatch Logs para modificar el periodo de retención de registros. Para obtener más información acerca de cómo cambiar los periodos de retención de registro en CloudWatch Logs, consulte Cambiar la retención de datos de registro en Trabajar con grupos y flujos de registros.

Para buscar información en los eventos de registro, use la consola de registros de Amazon CloudWatch, la AWS CLI o la API de registros de Amazon CloudWatch. Para obtener más información sobre la búsqueda y el filtrado de datos de registro, consulte Búsqueda y filtrado de datos de registros.

Métricas de Amazon Redshift sin servidor

Las métricas de Amazon Redshift sin servidor se dividen en métricas informáticas y métricas de datos y almacenamiento, incluidos en los conjuntos de dimensiones de grupo de trabajo y espacio de nombres, respectivamente. Para obtener más información acerca de los grupos de trabajo y espacios de nombres, consulte Información general de los grupos de trabajo y espacios de nombres de Amazon Redshift sin servidor.

Las métricas informáticas de CloudWatch son las siguientes:

Métricas informáticas de CloudWatch

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
`QueriesCompletedPerSecond`	Número de consultas	Número de consultas completadas por segundo.	{Database, LatencyRange, Workgroup}, {LatencyRange, Workgroup}

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
QueryDuration	Microsegundos	Tiempo medio que tarda en completarse una consulta.	{Database, LatencyRange, Workgroup}, {LatencyRange, Workgroup}
QueriesRunning	Número de consultas	Número de consultas en ejecución en un momento determinado.	{Database , QueryType , Workgroup }, {QueryType, Workgroup}
QueriesQueued	Número de consultas	Número de consultas en cola en un momento determinado.	{Database , QueryType , Workgroup }, {QueryType, Workgroup}
DatabaseConnections	Número de conexiones	Número de conexiones a una base de datos en un momento determinado.	{Database, Workgroup}, {Workgroup}
QueryRuntimeBreakdown	Milisegundos	El tiempo total que las consultas que se ejecutaron, por etapa de consulta.	{Database, Stage, Workgroup}, {Stage, Workgroup}

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
ComputeCapacity	RPU	Número medio de unidades de computación asignadas durante los últimos 30 minutos, redondeadas al entero más cercano.	{Workgroup}
ComputeSeconds	Segundos de RPU	Segundos acumulados de unidades de computación utilizados en los últimos 30 minutos.	{Workgroup}
QueriesSucceeded	Número de consultas	Número de consultas que se han realizado correctamente en los últimos 5 minutos.	{Database, QueryType, Workgroup}, {QueryType, Workgroup}
QueriesFailed	Número de consultas	Número de consultas que han producido un error en los últimos 5 minutos.	{Database, QueryType, Workgroup}, {QueryType, Workgroup}

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
`UsageLimitAvailable`	Horas de RPU o TB	Según el UsageType, UsageLimitAvailable devuelve lo siguiente: • Si UsageType es SERVERLESS_COMPUTE, UsageLimitAvailable devuelve el número restante de horas de RPU que el grupo de trabajo puede consultar en el límite dado. • Si UsageType es CROSS_REGION_DATASHARING, UsageLimitAvailable devuelve el número restante de TB que el cliente puede	{UsageLimitId, UsageType, Workgroup}

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
		analizar en el límite dado.	

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
`UsageLimitConsumed`	Horas de RPU o TB	Según UsageType, UsageLimitConsumed devuelve lo siguiente: • Si UsageType es SERVERLESS_COMPUTE, UsageLimitConsumed devuelve el número de horas de RPU que el grupo de trabajo ya ha consultado o en el límite dado. • Si UsageType es CROSS_REGION_DATASHARING, UsageLimitConsumed devuelve el número de TB que el cliente ya ha utilizado para	{UsageLimitId, UsageType, Workgroup}

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
		analizar en el límite dado.	

Las métricas de datos y almacenamiento de CloudWatch son las siguientes:

Métricas de almacenamiento y datos de CloudWatch

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
`TotalTableCount`	Número de tablas	El número de tablas de usuario existentes en un momento. Este total no incluye tablas de Amazon Redshift	{Database, Namespace}
`DataStorage`	Megabytes	El número de megabytes utilizados, en disco o espacio de almacenamiento, para los datos de Redshift.	{Namespace}

La métrica `SnapshotStorage` es independiente del espacio de nombres y del grupo de trabajo. La métrica `SnapshotStorage` de CloudWatch es como sigue:

Métrica SnapshotStorage de CloudWatch

Nombre de métrica	Unidades	Descripción	Conjuntos de dimensiones
`SnapshotStorage`	Megabytes	El número de megabytes utilizados, en disco o espacio de almacenamiento, para instantáneas.	{}

Los conjuntos de dimensiones son las dimensiones de agrupación aplicadas a las métricas. Puede utilizar estos grupos de dimensiones para especificar cómo se recuperan las estadísticas.

En la tabla siguiente se detallan las dimensiones y los valores de dimensión de métricas específicas:

Dimensiones y valores de dimensión de CloudWatch

Dimensión	Descripción y valores
`DatabaseName`	El nombre de la base de datos. Un valor personalizado.
`Latency`	Los valores posibles son los siguientes: • corta: menos de 10 segundos • mediana: entre 10 segundos y 10 minutos • larga: más de 10 minutos
`QueryType`	Los valores posibles son `INSERT`, `DELETE`, `UPDATE`, `UNLOAD`, `LOAD`, `SELECT`, `CTAS` e `OTHER`.
`stage`	Fases de ejecución de una consulta. Los valores posibles son los siguientes:

Dimensión	Descripción y valores
	• QueryPlanning: tiempo invertido en procesar y optimizar instrucciones SQL. • QueryWaiting: tiempo invertido en esperar en la cola de WLM. • QueryExecutingRead: tiempo invertido en ejecutar consultas de lectura. • QueryExecutingInsert: tiempo invertido en ejecutar consultas de inserción. • QueryExecutingDelete: tiempo invertido en ejecutar consultas de eliminación. • QueryExecutingUpdate: tiempo invertido en ejecutar consultas de actualización. • QueryExecutingCtas: tiempo invertido en ejecutar consultas CREATE TABLE AS. • QueryExecutingUnload: tiempo invertido en ejecutar consultas de descarga. • QueryExecutingCopy: tiempo invertido en ejecutar consultas de copia. • QueryCommit: tiempo invertido en confirmar operaciones.
`Namespace`	El nombre del espacio de nombres. Un valor personalizado.
`Workgroup`	El nombre del grupo de trabajo. Un valor personalizado.
`UsageLimitId`	El identificador del límite de uso.

Dimensión	Descripción y valores
UsageType	La característica de Amazon Redshift sin servidor está limitada. Los valores posibles son los siguientes: • SERVERLESS_COMPUTE • CROSS_REGION_DATASHARING

Trabajo con instantáneas y puntos de recuperación

Una copia de seguridad en Amazon Redshift sin servidor es una representación puntual de los objetos y datos del espacio de nombres. Hay dos tipos de copias de seguridad: las instantáneas que se crean manualmente y los puntos de recuperación que Amazon Redshift sin servidor crea automáticamente para usted. Los puntos de recuperación se crean cada 30 minutos y se mantienen durante 24 horas.

Si desea recuperar los datos de una instantánea o de un punto de recuperación, puede restaurar una instantánea en un espacio de nombres sin servidor o en un clúster aprovisionado. Existen tres situaciones en las que puede restaurar instantáneas:

- Restaure una instantánea sin servidor en un espacio de nombres sin servidor.
- Restaure una instantánea de sin servidor en un clúster aprovisionado.
- Restaure una instantánea de clúster aprovisionada en un espacio de nombres sin servidor.

Al restaurar una instantánea sin servidor en un clúster aprovisionado, debe elegir el tipo de nodo que se va a utilizar, como RA3, y el número de nodos, lo que permite controlar la configuración en el nivel de clúster o nodo.

Para restaurar una instantánea de clúster aprovisionada en un espacio de nombres sin servidor, comience desde la consola aprovisionada de Redshift, elija la instantánea que desea restaurar y, a continuación, elija Restore from snapshot (Restaurar desde instantánea), Restore to serverless namespace (Restaurar en espacio de nombres sin servidor). Amazon Redshift convierte las tablas con claves intercaladas en claves de clasificación compuestas al restaurar una instantánea de clúster aprovisionada en un espacio de nombres sin servidor. Para obtener más información sobre claves de clasificación, consulte Uso de claves de clasificación.

Si desea agregar un contexto adicional, puede etiquetar las instantáneas y los puntos de recuperación con pares de clave-valor que proporcionen metadatos e información a las instantáneas y los puntos de recuperación. Para obtener más información sobre los recursos de etiquetado, consulte Información general de los recursos de etiquetado.

Por último, también puede compartir instantáneas con otras cuentas de AWS, lo que les permite acceder a los datos de la instantánea y ejecutar consultas.

Instantáneas

Puede restaurar una instantánea que haya creado en la consola de Amazon Redshift Serverless a un espacio de nombres disponible asociado a un grupo de trabajo. Un espacio de nombres está disponible una vez que está listo para consultas o modificaciones. Puede restaurar una instantánea cifrada con una clave KMS administrada por AWS en un espacio de nombres sin servidor.

Para ver una lista de todas las instantáneas, en la consola Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).

Para crear una instantánea

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Seleccione Create snapshot (Crear instantánea).
3. Elija un espacio de nombres del que crear una instantánea.
4. Ingrese un identificador de instantáneas.
5. (Opcional) Elija un periodo de retención. Si elige Custom value (Valor personalizado), elija el número de días. La cantidad que elija debe estar entre 1 y 3653 días, ambos incluidos. El valor predeterminado es retenerlo indefinidamente.
6. Seleccione Crear.

Para crear una instantánea a partir de la configuración del espacio de nombres

1. En la consola de Amazon Redshift Serverless, elija Namespace configuration (Configuración de espacio de nombres).
2. Elija el espacio de nombres del que crear una instantánea. Solo puede crear instantáneas de espacios de nombres asociados a un grupo de trabajo y cuyos estados están disponibles.
3. Elija la pestaña Data backup (Copia de seguridad de datos).
4. Seleccione Create snapshot (Crear instantánea).

5. Ingrese un identificador de instantáneas.
6. (Opcional) Elija un periodo de retención. Si elige Custom value (Valor personalizado), elija el número de días. La cantidad que elija debe estar entre 1 y 3653 días, ambos incluidos.
7. Seleccione Crear.

Para actualizar el periodo de retención de una instantánea

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Elija una instantánea que desea actualizar.
3. Elija Actions (Acciones), Set manual snapshot settings (Configuración de instantáneas manual).
4. Elija un periodo de retención. Si elige Custom value (Valor personalizado), elija el número de días.
5. Elija Guardar cambios.

Eliminar una instantánea

> **Note**
>
> No puede eliminar una instantánea que se haya compartido con otra cuenta. Primero debe eliminar el acceso de esa cuenta a la instantánea antes de eliminarla.

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Elija una instantánea que desea eliminar.
3. Elija Actions (Acciones), Delete (Eliminar).
4. Elija Eliminar.

Para crear una instantánea final de todos los datos de un espacio de nombres antes de eliminar el espacio de nombres.

1. En la consola de Amazon Redshift Serverless, elija Namespace configuration (Configuración de espacio de nombres).
2. Elija el espacio de nombres que desea eliminar.
3. Elija Acciones, Eliminar.

4. Elija Create final snapshot (Crear instantánea final).
5. Ingrese un nombre para la instantánea.
6. Ingrese eliminar.
7. Elija Eliminar.

Para compartir una instantánea con otra cuenta de AWS o eliminar el acceso de una cuenta a una instantánea

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Elija una instantánea que desea compartir.
3. Elija Actions (Acciones), Manage access (Administrar acceso).
4. Para compartir una instantánea con otra cuenta, introduzca un ID de Cuenta de AWS. Para eliminar el acceso de una cuenta, seleccione Eliminar.
5. Elija Guardar cambios.

Restauración de instantáneas

La restauración de una instantánea en un espacio de nombres sin servidor sustituye la base de datos actual por la base de datos de la instantánea.

La restauración de una instantánea en un espacio de nombres sin servidor se completa en dos fases. La primera fase se completa en unos minutos, restaura los datos en el espacio de nombres y los pone a disposición para consultas. La segunda fase de la restauración es donde se ajusta la base de datos, lo que puede provocar problemas de rendimiento menores. Esta segunda fase puede durar desde unas horas hasta varios días y, en determinados casos, un par de semanas. La cantidad de tiempo depende del tamaño de los datos, pero el rendimiento mejora de forma progresiva según se ajusta la base de datos. Al final de esta fase, el espacio de nombres sin servidor se encuentra totalmente ajustado y puede enviar consultas sin problemas de rendimiento.

Para restaurar una instantánea en un espacio de nombres sin servidor

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Elija la instantánea que desea restaurar. Solo puede restaurar una instantánea a la vez.
3. Elija Actions (Acciones), Restore to serverless namespace (Restaurar en un espacio de nombres sin servidor).

4. Elija un espacio de nombres disponible en el que restaurar. Solo puede restaurar los espacios de nombres cuyos estados están disponibles.
5. Elija Restore (Restaurar).

Para restaurar una instantánea en un clúster aprovisionado

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Elija la instantánea que desea restaurar.
3. Elija Action (Acción), Restore to provisioned cluster (Restaurar en clúster aprovisionado).
4. Ingrese un identificador del clúster.
5. Elija un Node type (Tipo de nodo). El número de nodos depende del tipo de nodo.
6. Siga las instrucciones en la página de la consola para ingresar las propiedades de la Cluster configuration (Configuración del clúster). Para obtener más información, consulte Creación de un clúster.

Para obtener más información sobre las instantáneas de los clústeres aprovisionados, consulte Instantáneas y copias de seguridad de Amazon Redshift.

Puntos de recuperación

Los puntos de recuperación se crean en Amazon Redshift sin servidor aproximadamente cada 30 minutos y se guardan durante 24 horas.

En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos) para administrar los puntos de recuperación. Puede utilizar las siguientes operaciones:

- Restaure un punto de recuperación en un espacio de nombres sin servidor.
- convertir un punto de recuperación en una instantánea

Para restaurar un punto de recuperación en un espacio de nombres sin servidor

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. En Recovery points (Puntos de recuperación), elija el valor de Creation time (Hora de creación) del punto de recuperación que desea restaurar.
3. Elija Restore (Restaurar). Solo puede restaurar los espacios de nombres cuyos estados están disponibles.

4. Ingrese la palabra restaurar en el campo de entrada de texto y elija Restore (Restaurar).

Para convertir un punto de recuperación en una instantánea

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. En Recovery points (Puntos de recuperación), elija el valor de Creation time (Hora de creación) del punto de recuperación que desea convertir en una instantánea.
3. Elija Create snapshot from recovery point (Crear una instantánea desde el punto de recuperación).
4. Ingrese un valor en Snapshot identifier (Identificador de instantáneas).
5. Seleccione Crear.

Programación de instantáneas

Para controlar con precisión cuándo realizar una instantánea, puede crear una programación de instantáneas para espacios de nombres específicos. Al programar la creación de instantáneas, puede crear un evento único o utilizar expresiones cron de Unix para crear una programación recurrente. Las expresiones cron admiten tres campos y están separadas por espacios en blanco.

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

Campos	Valores	Caracteres comodín
Minutos	0–59	, - * /
Horas	0–23	, - * /
Día del mes	1–31	, - * ? / L W
Mes	1–12 o ENE-DIC	, - * /
Día de la semana	1–7 o DOM-SÁB	, - * ? L #
Año	1970-2199	, - * /

Caracteres comodín

- El carácter comodín , (coma) incluye valores adicionales. En el campo `Day-of-week`, `MON,WED,FRI` incluiría lunes, miércoles y viernes. El total de valores está limitado a 24 por campo.
- El carácter comodín - (guion) especifica los intervalos. En el campo `Hour`, 1–15 incluiría desde la 1 hasta las 15 horas del día especificado.
- El * (asterisco) incluye todos los valores del campo. En el campo `Hours`, * incluiría cada hora.
- El comodín / (barra inclinada) especifica incrementos. En el campo `Hours`, puede escribir **`1/10`** para especificar cada 10 horas, empezando por la primera hora del día (por ejemplo, 01:00, 11:00 y 21:00).
- El comodín ? (signo de interrogación) especifica uno u otro. En el campo `Day-of-month` puede escribir 7 y si no le importa qué día de la semana era el séptimo, podría escribir ? en el campo Day-of-week.
- El comodín L en los campos `Day-of-month` o `Day-of-week` especifica el último día del mes o de la semana.
- El comodín W en el campo `Day-of-month` especifica un día de la semana. En el campo `Day-of-month`, `3W` especifica el día más cercano al tercer día de semana del mes.
- El comodín # en el campo Día de la semana especifica una instancia concreta del día de la semana de un mes. Por ejemplo, 3#2 sería el segundo martes del mes: el número 3 hace referencia al martes, ya que es el tercer día de la semana en el calendario anglosajón, mientras que 2 hace referencia al segundo día de ese tipo dentro de un mes.

> **Note**
>
> Si utiliza un carácter '#', solo puede definir una expresión en el campo Día de la semana. Por ejemplo, “3#1,6#3” no es válido porque se interpreta como dos expresiones.

Límites

- No se pueden especificar los campos `Day-of-month` y `Day-of-week` en la misma expresión Cron. Si especifica un valor en uno de los campos, debe utilizar un ? (signo de interrogación) en el otro.
- Las programaciones de instantáneas no admiten las siguientes frecuencias:
  - Instantáneas programadas con una frecuencia superior a una por hora.

- Instantáneas programadas con una frecuencia inferior a una por día (24 horas).

Si tiene programaciones solapadas que programan instantáneas en un periodo de una hora, se produce un error de validación.

La siguiente tabla contiene algunos ejemplos de cadenas cron.

Minutos	Horas	Día de la semana	Significado
0	14-20/1	TUE	Cada hora entre las dos y las ocho de la tarde del martes.
0	21	MON-FRI	Todas las noches a las 21 h de lunes a viernes.
30	0/6	SAT-SUN	Cada seis horas el sábado y el domingo empezando 30 minutos después de la medianoche (00:30) de ese día. Esto produce una instantánea a las [00:30, 06:30, 12:30 y 18:30] todos los días.
30	12/4	*	Cada cuatro horas a partir de las 12:30 todos los días. Esto se resuelve en [12:30, 16:30, 20:30].

En el siguiente ejemplo se muestra cómo crear una programación que se ejecute en incrementos de dos horas a partir de las 15:15 horas cada día.

```
cron(15 15/2 *)
```

En la actualidad, solo puede utilizar la API de Amazon Redshift sin servidor o la AWS CLI para crear una programación de instantáneas. Para obtener más información sobre estas operaciones, consulte Uso de la API de la AWS CLI y de Amazon Redshift sin servidor.

Copia de las copias de seguridad en otra Región de AWS

Puede configurar Amazon Redshift sin servidor para que copie automáticamente las instantáneas y los puntos de recuperación en otra Región de AWS. Al crear una instantánea en la Región de AWS de origen, se copia en una región de destino. Puede configurar su espacio de nombres para que solo copie las instantáneas y los puntos de recuperación en una Región de AWS de destino a la vez. Para obtener una lista de las Regiones de AWS donde Amazon Redshift sin servidor está disponible, consulte los puntos de conexión enumerados para la API de Redshift sin servidor en la Referencia general de Amazon Web Services.

Al configurar las copias de seguridad, también puede especificar un período de retención durante el cual Amazon Redshift sin servidor debe conservar la instantánea copiada. No puede cambiar los períodos de retención de los puntos de recuperación, que deben ser de 1 día. Los periodos de retención de las instantáneas en la región de destino son distintos del periodo de retención de las instantáneas de la región de origen. De forma predeterminada, el período de retención es para conservar la instantánea indefinidamente. Si elige Valor personalizado, elija el número de días. La cantidad que elija debe estar entre 1 y 3653 días, ambos incluidos.

Para cambiar la región de destino a la que se van a copiar las instantáneas, primero desactive la opción de copiar las copias de seguridad y, a continuación, especifique la nueva región de destino cuando vuelva a habilitar la copia.

Una vez que se copia una instantánea o un punto de recuperación en una región de destino, puede utilizarlos para restaurar los datos en la región.

De forma predeterminada, sus datos se cifran con una clave que AWS administra en su nombre. Para usar una clave diferente, elija la clave que desee usar al configurar la copia de seguridad en la Región de AWS de origen y Amazon Redshift sin servidor creará automáticamente una concesión que habilitará el cifrado de instantáneas en la Región de AWS de destino.

Para copiar las copias de seguridad en otra región, asegúrese de que dispone de los siguientes permisos de IAM:

```
redshift-serverless:CreateSnapshotCopyConfiguration
redshift-serverless:UpdateSnapshotCopyConfiguration
redshift-serverless:ListSnapshotCopyConfigurations
redshift-serverless:DeleteSnapshotCopyConfiguration
```

Si utiliza su propia clave de KMS para cifrar las copias de seguridad, también necesitará los siguientes permisos:

```
kms:CreateGrant
kms:DescribeKey
```

Para configurar la copia de las instantáneas o puntos de recuperación a otra Región de AWS

1. En la consola de Amazon Redshift sin servidor, elija el espacio de nombres para el que desee configurar la copia de instantáneas o puntos de recuperación.
2. Elija Acciones y Configurar la copia de seguridad entre regiones.
3. Elija la Región de AWS de destino en la que desea copiar la instantánea.
4. (Opcional) Elija durante cuánto tiempo desea retener la instantánea. Si elige Valor personalizado, debe indicar la cantidad de días. La cantidad que elija debe estar entre 1 y 3653 días, ambos incluidos. El valor predeterminado es retenerlo indefinidamente.
5. (Opcional) Elija una clave de AWS KMS diferente para usar el cifrado en la región de destino.
6. Seleccione Guardar configuración.

Restauración de una tabla

También puede restaurar una tabla específica a partir de una instantánea o un punto de recuperación. Al hacerlo, debe especificar la instantánea o el punto de recuperación de origen, la base de datos, el esquema, la tabla, la base de datos de destino y el nuevo nombre de la tabla. Esta nueva tabla no puede tener el mismo nombre que una existente. Si desea reemplazar una tabla existente mediante la restauración de una tabla, primero debe cambiar el nombre de la tabla o eliminarla antes de restaurarla.

La tabla de destino se crea utilizando las definiciones de columnas, los atributos de tabla y los atributos de columna de la tabla de origen, a excepción de las claves externas. Para evitar conflictos de dependencias, la tabla de destino no hereda las claves externas de la tabla de origen. Cualquier dependencia, como vistas o permisos concedidos en la tabla de origen, no se aplica a la tabla de destino.

Si el propietario de la tabla de origen existe, ese usuario es el propietario de la tabla restaurada, dado que el usuario tiene los permisos suficientes para volverse el propietario de una relación en la base de datos y el esquema especificados. De lo contrario, la tabla restaurada es propiedad del usuario administrador que se creó cuando se lanzó el clúster.

La tabla restaurada vuelve al estado en el que estaba en el momento que se realizó el backup. Esto incluye las reglas de visibilidad de las transacciones definidas en virtud del cumplimiento de Amazon Redshift con el aislamiento serializable, lo que significa que los datos estarán visibles de inmediato para las transacciones en tránsito que se inicien después de la copia de seguridad.

Puede utilizar la consola de Amazon Redshift sin servidor para restaurar tablas a partir de una instantánea.

La restauración de una tabla a partir de una copia de seguridad de datos tiene las siguientes limitaciones:

- Solo puede restaurar una tabla cada vez.
- Cualquier dependencia, como vistas o permisos concedidos en la tabla de origen, no se aplica a la tabla de destino.
- Si la seguridad en el nivel de fila está activada para una tabla que se está restaurando, Amazon Redshift sin servidor restaura la tabla con la seguridad a nivel de fila activada.

Para restaurar una tabla mediante la consola de Amazon Redshift sin servidor

1. En la consola de Amazon Redshift Serverless, elija Data backup (Copia de seguridad de datos).
2. Elija la instantánea o el punto de recuperación que contiene la tabla que desea restaurar.
3. Seleccione Acciones, Restaurar la tabla a partir de la instantánea o Restaurar la tabla a partir del punto de recuperación.
4. Indique la información sobre la instantánea o el punto de recuperación de origen y la tabla de destino; a continuación, elija Restaurar tabla.

Uso de la API de la AWS Command Line Interface y de Amazon Redshift sin servidor

Aparte de utilizar la consola de AWS, también puede utilizar AWS CLI o la API de Amazon Redshift Serverless para interactuar con instantáneas y puntos de recuperación. En la siguiente tabla, se

enumeran las operaciones de la API y la CLI que puede usar para administrar las instantáneas y los puntos de recuperación.

Operación de la API	Command de la CLI	Descripción
CreateSnapshot	create-snapshot	Crea una instantánea. Las instantáneas deben estar asociadas a un espacio de nombres, por lo que debe incluir el nombre de un espacio de nombres en la solicitud. De forma predeterminada, Amazon Redshift sin servidor mantiene instantáneas durante un periodo indefinido, pero puede especificar un periodo de retención.
RestoreFromSnapshot	restore-from-snapshot	Restaura las bases de datos en una instantánea en su espacio de nombres. Si va a realizar restauraciones de una instantánea de Amazon Redshift Serverless en un clúster aprovisionado, debe especificarel `snapshotArn` de la instantánea que va a restaurar. De lo contrario, si va a restaurar de sin servidor a sin servidor, puede especificar `snapshotArn` o `snapshotName`, pero no ambos.
RestoreTableFromSnapshot	restore-table-from-snapshot	Restaure una tabla a partir de una instantánea en su espacio

Operación de la API	Command de la CLI	Descripción
		de nombres de Amazon Redshift sin servidor. No puede usar esta operación para restaurar tablas con claves de clasificación intercaladas.
GetSnapshot	get-snapshot	Obtiene información sobre una instantánea.
ListSnapshots	list-snapshots	Obtiene información de varias instantáneas.
DeleteSnapshot	delete-snapshot	Elimina una instantánea.
RestoreFromRecoveryPoint	restore-from-recovery-point	Restaura los datos de un punto de recuperación en su espacio de nombres.
RestoreTableFromRecoveryPoint	restore-table-from-recovery-point	Restaura una tabla a partir de un punto de recuperación en su espacio de nombres de Amazon Redshift sin servidor. No puede usar esta operación para restaurar tablas con claves de clasificación intercaladas.
ConvertRecoveryPointToSnapshot	convert-recovery-point-to-snapshot	Convierte un punto de recuperación en una instantánea.
GetRecoveryPoint	get-recovery-point	Obtiene información sobre un punto de recuperación.
ListRecoveryPoints	list-recovery-points	Obtiene información sobre varios puntos de recuperación.

Para programar la creación de instantáneas, use las siguientes operaciones de la API.

Operación de la API	Command de la CLI	Descripción
CreateScheduledAction	create-scheduled-action	Crea una acción programada que contiene un programa y una acción de Amazon Redshift sin servidor. Por ejemplo, puede crear una ejecución programada para ejecutar la operación de la API `CreateSnapshot` .
DeleteScheduledAction	delete-scheduled-action	Elimina una acción programada.
GetScheduledAction	get-scheduled-action	Obtiene información de una acción programada.
ListScheduledActions	list-scheduled-actions	Obtiene información de una lista de acciones programadas.
UpdateScheduledAction	update-scheduled-action	Actualiza una acción programada.

Uso compartido de datos en Amazon Redshift sin servidor

Utilice el uso compartido de datos para compartir la información más actualizada y coherente a medida que se actualiza en Amazon Redshift sin servidor.

Uso compartido de datos en Amazon Redshift sin servidor

Con data sharing (uso compartido de datos), dispone de acceso en directo a los datos para que los usuarios puedan ver la información más actualizada y coherente a medida que se actualiza en Amazon Redshift sin servidor.

Introducción al uso compartido de datos en Amazon Redshift sin servidor

Puede compartir datos con fines de lectura entre diferentes instancias de Amazon Redshift sin servidor en las Cuentas de AWS o entre ellas.

Puede comenzar a compartir datos usando la interfaz SQL o la consola de Amazon Redshift. Para obtener más información, consulte Introducción al uso compartido de datos mediante la interfaz SQL o Introducción al uso compartido de datos con la consola en la Guía para desarrolladores de bases de datos de Amazon Redshift en la Guía para desarrolladores de bases de datos Amazon Redshift.

Con el uso compartido de datos, los espacios de nombres de Amazon Redshift sin servidor y los clústeres aprovisionados pueden compartir datos activos entre sí, tanto si se encuentran en una Cuenta de AWS en varias Cuentas de AWS como en varias Regiones de AWS. Para obtener más información, consulte Regiones en las que está disponible el uso compartido de datos.

Para comenzar a compartir datos dentro de una Cuenta de AWS, abra la AWS Management Console y, a continuación, elija la consola de Amazon Redshift. Elija Namespace configuration (Configuración de espacio de nombres) y, a continuación, Datashares (Recursos compartidos de datos). Siga los procedimientos indicados en Introducción al uso compartido de datos mediante la consola en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para comenzar a compartir datos entre Cuentas de AWS, abra la AWS Management Console y, a continuación, elija la consola de Amazon Redshift. Seleccione Datashares (Recursos compartidos de datos). Siga los procedimientos indicados en Introducción al uso compartido de datos mediante la consola en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para comenzar a consultar datos en un recurso compartido de datos, cree una base de datos en un espacio de nombres que tenga un grupo de trabajo asociado a él. Desde un recurso compartido de datos especificado, elija un espacio de nombres que tenga un grupo de trabajo asociado a él y cree una base de datos para consultar datos. Siga los procedimientos indicados en Creación de bases de datos a partir de recursos compartidos de datos.

Concesión de acceso para ver recursos compartidos de datos mediante la consola

Un superusuario puede proporcionar acceso a los usuarios que no son superusuarios para que puedan ver los recursos compartidos de datos creados por todos los usuarios.

Para conceder acceso a un recurso compartido de datos a un usuario, utilice el siguiente comando para proporcionar acceso a un recurso compartido de datos a un usuario, donde datashare_name

es el nombre del recurso compartido de datos y user-name es el nombre del usuario al que desea proporcionar acceso.

```
grant share on datashare datashare_name to "IAM:test_user";
```

Para conceder acceso a un recurso compartido de datos a un grupo de usuarios, cree primero un grupo de usuarios con usuarios. Para obtener información sobre cómo crear grupos de usuarios, consulte CREATE GROUP. Después, conceda acceso al recurso compartido de datos a un usuario mediante el siguiente comando, donde datashare_name es el nombre del recurso compartido de datos y user-group es el nombre del grupo de usuarios al que desea conceder acceso.

```
grant share on datashare datashare_name to group user_group;
```

Para obtener información sobre cómo utilizar la instrucción GRANT, consulte GRANT.

Aspectos a tener en cuenta a la hora de compartir datos en Amazon Redshift sin servidor

A continuación, se indican los aspectos que se deben tener en cuenta para trabajar con el uso compartido de datos en Amazon Redshift sin servidor:

- Amazon Redshift solo admite clústeres aprovisionados de tipo de instancia ra3.16xlarge, ra3.4xlarge y ra3.xlplus, y punto de conexión sin servidor como productores o consumidores de uso compartido de datos.
- Amazon Redshift sin servidor está cifrado de forma predeterminada.

Para obtener una lista de las limitaciones del recurso compartido de datos, incluidos los objetos de base de datos compatibles, los requisitos de cifrado y los requisitos de clave de clasificación, consulte Consideraciones al utilizar el recurso compartido de datos en Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Información general de recursos de etiquetado

En AWS, el usuario define las etiquetas, que se componen de pares de clave-valor. Amazon Redshift Serverless admite el etiquetado para proporcionar metadatos sobre los recursos de un vistazo.

Las etiquetas no son obligatorias para los recursos, pero ayudan a proporcionar contexto. Es posible que desee etiquetar recursos con metadatos con información relacionada con el recurso. Por

ejemplo, suponga que desea hacer un seguimiento de qué recursos pertenecen a un entorno de prueba y a un entorno de producción. Puede crear una clave denominada entorno y proporcionar el valor de prueba o de producción para identificar los recursos que se utilizan en cada entorno. Si utiliza etiquetas en otros servicios de AWS o si tiene categorías estándar en su negocio, le recomendamos que cree los mismos pares clave-valor para los recursos para mantener la coherencia.

Si elimina un recurso, se eliminarán todas las etiquetas asociadas. Puede usar la consola de AWS CLI y Amazon Redshift Serverless para etiquetar los recursos sin servidor. Las operaciones de la API disponibles son `TagResource`, `UntagResource` y `ListTagsForResource`.

Cada recurso tiene un conjunto de etiquetas, que es una colección de una o varias etiquetas asignadas al recurso. Cada recurso puede tener hasta 50 etiquetas por cada conjunto de etiquetas. Puede añadir etiquetas al crear un recurso y después de que se haya creado. Puede agregar etiquetas a los siguientes tipos de recursos sin servidor:

- Grupos de trabajo
- Espacios de nombres
- Instantáneas
- Puntos de recuperación

Las etiquetas tienen los siguientes requisitos:

- Las claves no pueden tener el prefijo `aws:`.
- Las claves deben ser únicas dentro de un conjunto de etiquetas.
- Una clave debe tener entre 1 y 128 caracteres permitidos.
- Un valor debe tener entre 0 y 256 caracteres permitidos.
- No es necesario que los valores sean únicos dentro de un conjunto de etiquetas.
- Los caracteres permitidos para las claves y los valores son letras y dígitos Unicode, espacios en blanco y cualquiera de estos símbolos: _ . : / = + - @.
- Las claves y los valores distinguen entre mayúsculas y minúsculas.

Para administrar etiquetas de los recursos de Amazon Redshift Serverless

1. En la consola de Amazon Redshift Serverless, elija Manage Tags (Administrar etiquetas).

2. Ingrese el tipo de recurso que desea buscar y elija Search resources (Buscar recursos). Elija el recurso cuyas etiquetas desea administrar y, a continuación, elija Manage tags (Administrar etiquetas).
3. Especifique las claves y los valores opcionales que desea agregar al recurso. Al modificar una etiqueta, puede cambiar el valor de la etiqueta, pero no la clave.
4. Cuando haya terminado de agregar, eliminar o modificar etiquetas, elija Save changes (Guardar cambios) y, a continuación, elija Apply (Aplicar) para guardar los cambios.

Clústeres aprovisionados de Amazon Redshift

En las secciones siguientes, podrá aprender los conceptos básicos de la creación de un almacenamiento de datos mediante el lanzamiento de un conjunto de nodos informáticos llamado clúster de Amazon Redshift.

Temas

- Información general de Amazon Redshift
- Usar EC2-VPC al crear el clúster
- Alarma predeterminada de espacio en disco
- Estado del clúster
- Consideraciones para el uso de clústeres aprovisionados de Amazon Redshift
- Operaciones de clúster
- Configuración de la implementación multi-AZ
- Administración de clústeres a través de la consola
- Administración de clústeres mediante la AWS CLI y la API de Amazon Redshift
- Administración de clústeres en una VPC
- Historial de versiones del clúster

Información general de Amazon Redshift

Un almacenamiento de datos de Amazon Redshift es una colección de recursos informáticos denominados nodos que se organizan en un grupo llamado clúster. Cada clúster ejecuta un motor de Amazon Redshift y contiene una o más bases de datos.

> **Note**
>
> En este momento, está disponible la versión 1.0 del motor de Amazon Redshift. No obstante, como el motor está actualizado, puede seleccionar entre varias versiones disponibles de motores de Amazon Redshift.

Clústeres y nodos de Amazon Redshift

Un clúster de Amazon Redshift se compone de nodos. Cada clúster tiene un nodo principal y uno o más nodos de computación. El nodo principal recibe consultas de las aplicaciones cliente, las analiza y desarrolla planes de ejecución de las consultas. Luego, el nodo principal coordina una ejecución en paralelo de esos planes con los nodos de computación y agrega los resultados intermedios de dichos nodos. Finalmente, devuelve los resultados a las aplicaciones cliente.

Los nodos de computación procesan los planes de ejecución de consultas y transmiten datos entre ellos para atender a esas consultas. Los resultados intermedios envían al nodo principal para agregación antes de que vuelvan a las aplicaciones cliente. Para obtener más información acerca de los nodos principales y los nodos informáticos, consulte Arquitectura del sistema de almacenamiento de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.

> **Note**
>
> Cuando se crea un clúster en la consola de Amazon Redshift (https://console.aws.amazon.com/redshiftv2/), se puede obtener una recomendación de la configuración del clúster en función del tamaño de los datos y de las características de las consultas. Para utilizar esta calculadora de tamaño, busque Help me choose (Ayúdeme a elegir) en la consola en regiones de AWS que admitan tipos de nodos RA3. Para obtener más información, consulte Creación de un clúster.

Cuando se lanza un clúster, una de las opciones que se debe especificar es el tipo de nodo. El tipo de nodo determina la capacidad de la CPU, la RAM, el almacenamiento y el tipo de unidad de almacenamiento de cada nodo.

Amazon Redshift ofrece diferentes tipos de nodos para alojar sus cargas de trabajo. Le recomendamos elegir los nodos RA3 o DC2 en función del rendimiento requerido, el tamaño de los datos y su crecimiento previsto.

Los nodos RA3 con almacenamiento administrado le permiten optimizar su almacenamiento de datos mediante el escalado y pago de las capacidades de cómputo y almacenamiento administrado de forma independiente. Con RA3, elige la cantidad de nodos que necesita en función de requisitos de rendimiento y solo paga por el almacenamiento administrado que utilice. Dimensione su clúster de RA3 en función de la cantidad de datos que procesa diariamente. Puede lanzar clústeres que usen los tipos de nodos RA3 en una nube virtual privada (VPC). No puede lanzar clústeres RA3 en EC2-Classic. Para obtener más información, consulte Creación de un clúster en una VPC.

El almacenamiento administrado de Amazon Redshift utiliza grandes unidades de estado sólido de alto rendimiento en cada nodo RA3 para lograr un almacenamiento local rápido y utiliza Amazon S3 para lograr un almacenamiento duradero a largo plazo. Si el volumen de los datos de un nodo aumenta y supera el tamaño de las grandes unidades de estado sólido locales, el almacenamiento administrado de Amazon Redshift descarga automáticamente dichos datos en Amazon S3. Se paga la misma tarifa reducida por el almacenamiento administrado de Amazon Redshift, con independencia de si los datos residen en unidades de estado sólido de alto rendimiento o en Amazon S3. Para las cargas de trabajo que requieren un almacenamiento cada vez mayor, el almacenamiento administrado permite escalar automáticamente la capacidad de almacenamiento de datos de forma separada de los nodos de computación.

Los nodos DC2 permiten tener almacenamientos de datos con uso intensivo de cómputo con almacenamiento SSD local incluido. Debe elegir la cantidad de nodos que necesita en función del tamaño de los datos y los requisitos de rendimiento. Los nodos DC2 almacenan sus datos localmente para obtener un alto rendimiento y, a medida que el tamaño de los datos aumenta, puede agregar más nodos informáticos con objeto de incrementar la capacidad de almacenamiento del clúster. Para conjuntos de datos de menos de 1 TB (sin comprimir), recomendamos los tipos de nodos DC2 para lograr el mejor rendimiento al menor precio. Si espera que sus datos crezcan, recomendamos usar nodos RA3 para que pueda dimensionar el cómputo y el almacenamiento de forma independiente para lograr el mejor precio y rendimiento. Puede lanzar clústeres que usen los tipos de nodos DC2 en una nube virtual privada (VPC). No puede lanzar clústeres DC2 en EC2-Classic. Para obtener más información, consulte Creación de un clúster en una VPC.

Los nodos DS2 le permiten crear grandes almacenamientos de datos con unidades de disco duro (HDD), pero recomendamos usar nodos RA3. Si utiliza nodos DS2, consulte Actualización a tipos de nodo RA3 para obtener instrucciones de actualización. Si utiliza ocho o más nodos de ds2.xlarge o cualquier cantidad de nodos ds2.8xlarge, pueden actualizar a RA3 y obtener el doble de almacenamiento y un mejor rendimiento por el mismo costo bajo demanda.

Hay disponibles tipos de nodos de diferentes tamaños. El tamaño y la cantidad de nodos determinan el almacenamiento total de un clúster. Para obtener más información, consulte Detalles acerca de los tipos de nodos.

Algunos tipos de nodos admiten un único nodo (nodo único) o dos o más nodos (nodo múltiple). El número mínimo de nodos para clústeres de algunos tipos de nodos es de dos nodos. En un clúster de nodo único, se comparte ese nodo para la funcionalidad principal y para la de computación. No se recomiendan clústeres de nodo único para ejecutar cargas de trabajo de producción. En un clúster de nodos múltiples, el nodo principal es independiente de los nodos de computación. El

nodo principal es del mismo tipo de nodo que los nodos de computación. Solo paga por nodos de computación.

Amazon Redshift aplica cuotas a los recursos de cada cuenta de AWS en cada región de AWS. La cuota limita la cantidad de recursos que una cuenta puede crear para un tipo de recurso determinado, como los nodos o las instantáneas, dentro de una región de AWS. Para obtener más información sobre las cuotas predeterminadas que se aplican a los recursos de Amazon Redshift, consulte Límites de Amazon Redshift en la Referencia general de Amazon Web Services. Para solicitar un aumento, envíe un formulario de aumento de límites de Amazon Redshift.

El costo del clúster depende de la región de AWS, del tipo de nodo, de la cantidad de nodos y de si los nodos se reservan de manera anticipada. Para obtener más información acerca de los costos de los nodos, visite la página Precios de Amazon Redshift.

Detalles acerca de los tipos de nodos

En las siguientes tablas, se resumen las especificaciones de cada tipo y tamaño de nodo. Los títulos de las tablas tienen estos significados:

- vCPU es la cantidad de CPU virtuales de cada nodo.
- RAM es la cantidad de memoria en gibibytes (GiB) de cada nodo.
- Sectores predeterminados por nodo es el número predeterminado de sectores en los que se particiona un nodo de computación cuando se crea un clúster o se cambia el tamaño con el cambio de tamaño clásico.

  El número de sectores por nodo podría cambiar si se cambia el tamaño del clúster mediante el cambio de tamaño elástico. No obstante, el número total de sectores en todos los nodos de computación del clúster sigue siendo el mismo después del cambio de tamaño elástico.

  Al crear un clúster con la operación de restauración desde instantánea, el número de sectores del clúster resultante podría cambiar respecto al clúster original si cambia el tipo de nodo.
- Almacenamiento es la capacidad y el tipo almacenamiento de cada nodo.
- Rango de nodos es la cantidad mínima y máxima de nodos que admite Amazon Redshift según el tipo y el tamaño de los nodos.

> **Note**
>
> Puede tener restricciones para utilizar menos nodos según la cuota que se aplica a su cuenta de AWS en la región de AWS seleccionada. Para solicitar un aumento, envíe un formulario de aumento de límites de Amazon Redshift.

- Capacidad total es la capacidad total de almacenamiento del clúster si se implementa la cantidad máxima de nodos especificada en el rango de nodos.

Tipos de nodo RA3

Tipo de nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Límite de almacenamiento administrado por nodo [1]	Rango de nodos con Crear clúster	Capacidad total de almacenamiento administrado [2]
ra3.xlplus (nodo único)	4	32	2	4 TB	1	4 TB[3]
ra3.xlplus (varios nodos)	4	32	2	32 TB	2–16[4]	1024 TB[4]
ra3.4xlarge	12	96	4	128 TB	2–32[5]	8192 TB[5]
ra3.16xlarge	48	384	16	128 TB	2–128	16 384 TB

[1] El límite de almacenamiento para el almacenamiento administrado de Amazon Redshift. Este es un límite invariable.

[2] El límite total de almacenamiento administrado es el número máximo de nodos multiplicado por el límite de almacenamiento administrado de cada nodo.

[3] Para cambiar el tamaño de un clúster de un solo nodo a uno de varios, solo se admite el método de redimensionamiento clásico.

[4] Puede crear un clúster con el tipo de nodo ra3.xlplus (de varios nodos) que tenga hasta 16 nodos. Para clústeres de varios nodos, puede cambiar el tamaño con el redimensionamiento elástico a un máximo de 32 nodos.

[5] Puede crear un clúster con el tipo de nodo ra3.4xlarge con hasta 32 nodos. Puede cambiar su tamaño con el redimensionamiento elástico a un máximo de 64 nodos.

Tipos de nodos de almacenamiento de alta densidad

Tipo de nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Almacenamiento por nodo	Rango de nodos	Capacidad total	
ds2.xlarge	4	31	2	HDD de 2 TB	1–32	64 TB	
ds2.8xlarge	36	244	16	HDD de 16 TB	2–128	2 PB	

Tipos de nodos de computación de alta densidad

Tipo de nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Almacenamiento por nodo	Rango de nodos	Capacidad total	
dc2.large	2	15	2	SSD NVMe de 160 GB	1–32	5.12 TB	
dc2.8xlarge	32	244	16	SSD NVMe de 2,56 TB	2–128	326 TB	

Tipo de nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Almacenamiento por nodo	Rango de nodos	Capacidad total
dc1.large[1]	2	15	2	SSD de 160 GB	1–32	5.12 TB
dc1.8xlarge[1]	32	244	32	SSD de 2,56 TB	2–128	326 TB

[1] Recomendamos los tipos de nodos DC2 frente a los tipos de nodos DC1. Para obtener más información sobre cómo actualizar, consulte Actualización de tipos de nodo DC1 a tipos de nodo DC2.

Nombres anteriores de los tipos de nodos

En versiones anteriores de Amazon Redshift, algunos tipos de nodos tenían nombres diferentes. Puede usar los nombres anteriores en la AWS CLI y la API de Amazon Redshift. No obstante, recomendamos que actualice cualquier script que haga referencia a esos nombres para usar los nombres actuales en su lugar. A continuación, se detallan los nombres actuales y anteriores.

Nombre actual	Nombres anteriores
ds2.xlarge	ds1.xlarge, dw.hs1.xlarge, dw1.xlarge
ds2.8xlarge	ds1.8xlarge, dw.hs1.8xlarge, dw1.8xlarge
dc1.large	dw2.large
dc1.8xlarge	dw2.8xlarge

Determinar cuál es la cantidad de nodos

Como Amazon Redshift distribuye y ejecuta consultas en paralelo en todos los nodos informáticos de un clúster, puede aumentar el rendimiento de las consultas agregando nodos al clúster. Cuando ejecuta un clúster con al menos dos nodos de computación, los datos de cada nodo se reflejan en discos de otro nodo para reducir el riesgo de pérdida de datos.

Puede supervisar el rendimiento de las consultas en la consola de Amazon Redshift y con las métricas de Amazon CloudWatch. También puede agregar o eliminar nodos según sea necesario para lograr el equilibrio entre precio y rendimiento de su clúster. Cuando solicita un nodo adicional, Amazon Redshift se encarga de todos los detalles de implementación, equilibrio de carga y mantenimiento de datos. Para obtener más información acerca del rendimiento de un clúster, consulte Monitoreo del rendimiento de clústeres de Amazon Redshift.

Los nodos reservados son adecuados para cargas de trabajo de producción de estado estable y aportan descuentos significativos en comparación con los precios bajo demanda. Puede comprar nodos reservados después de ejecutar experimentos y pruebas de conceptos para validar la configuración de producción. Para obtener más información, consulte Adquisición de nodos reservados de Amazon Redshift.

Cuando se pausa un clúster, suspende la facturación bajo demanda durante el tiempo en que se detiene el clúster. Durante este tiempo de pausa, solo paga por el almacenamiento de copia de seguridad. De este modo, puede olvidarse de planificar y adquirir capacidad para el almacenamiento de datos antes de necesitarla, lo que le permite administrar de manera rentable entornos de desarrollo o pruebas.

Para obtener más información acerca de los precios de los nodos bajo demanda y reservados, consulte Precios de Amazon Redshift.

Usar EC2-VPC al crear el clúster

Los clústeres de Amazon Redshift se ejecutan en las instancias de Amazon EC2 que están configuradas para el tipo y el tamaño de nodos de Amazon Redshift que haya seleccionado. Cree su clúster con EC2-VPC. Si sigue utilizando EC2-Classic, le recomendamos que use EC2-VPC para mejorar el rendimiento y la seguridad. Para obtener más información acerca de estas plataformas de redes, consulte Plataformas compatibles en la Guía del usuario de Amazon EC2 para instancias de Linux. La configuración de su cuenta de AWS determina si EC2-VPC o EC2-Classic están disponibles para usted.

> **Note**
>
> Para evitar problemas de conexión entre las herramientas de cliente SQL y la base de datos de Amazon Redshift, le recomendamos realizar alguna de estas dos operaciones. Puede configurar una regla de entrada que permita a los hosts negociar el tamaño del paquete. También puede desactivar las tramas gigantes de TCP/IP estableciendo la unidad máxima de transmisión (MTU) en 1500 en la interfaz de red (NIC) de sus instancias de Amazon EC2. Para obtener más información acerca de estos métodos, consulte Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster.

EC2-VPC

Cuando se utiliza EC2-VPC, el clúster se ejecuta en una nube virtual privada (VPC) que está aislada lógicamente en su cuenta de AWS. Si aprovisiona su clúster en EC2-VPC, controla el acceso a su clúster asociando uno o más grupos de seguridad de la VPC con el clúster. Para obtener más información, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.

Para crear un clúster en una VPC, primero debe crear un grupo de subred de clúster de Amazon Redshift proporcionando información de la subred de su VPC y, luego, al lanzar el clúster, debe proporcionar el grupo de subred. Para obtener más información, consulte Grupos de subredes del clúster de Amazon Redshift.

Para obtener más información acerca de Amazon Virtual Private Cloud (Amazon VPC), consulte la página de detalles del producto de Amazon VPC.

EC2-Classic

La plataforma EC2-Classic se retirará el 15 de agosto de 2022. Le recomendamos que migre los clústeres de la plataforma EC2-Classic a una plataforma EC2-VPC. Para obtener más informaci ón, consulte Actualización de un clúster DS2 en EC2-Classic para EC2-VPC y EC2-Classic Networking se retira: cómo prepararse.

En la plataforma EC2-Classic, el clúster se ejecuta en una única red plana que usted comparte con otros clientes de AWS. Si aprovisiona el clúster en la plataforma EC2-Classic, controla el acceso al clúster asociando uno o más grupos de seguridad de clúster de Amazon Redshift con el clúster. Para obtener más información, consulte Grupos de seguridad del clúster de Amazon Redshift.

Lance un clúster

Su cuenta de AWS puede lanzar instancias de EC2-VPC y de EC2-Classic, o solo de EC2-VPC, región por región. Para determinar qué plataforma de red admite su cuenta y, a continuación, lanzar un clúster, haga lo siguiente:

1. Decida en qué región de AWS desea implementar un clúster. Para obtener una lista de las regiones de AWS en las que Amazon Redshift está disponible, consulte Puntos de conexión de Amazon Redshift en la Referencia general de Amazon Web Services.
2. Averigüe qué plataformas de Amazon EC2 admite su cuenta en la región de AWS que haya elegido. Puede encontrar esta información en la consola de Amazon EC2. Para obtener instrucciones paso a paso, consulte Plataformas compatibles en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Si su cuenta es compatible con ambas plataformas, le recomendamos EC2-VPC. Si su cuenta solo es compatible con EC2-VPC, debe implementar su clúster en la VPC.
4. Lance su clúster de Amazon Redshift. Puede crear un clúster con la consola o la API de Amazon Redshift, la AWS CLI o las bibliotecas SDK. Para obtener más información acerca de estas opciones y enlaces a documentación relacionada, consulte ¿Qué es Amazon Redshift?.

Alarma predeterminada de espacio en disco

Cuando crea un clúster de Amazon Redshift, tiene la opción de configurar una alarma de Amazon CloudWatch para supervisar el porcentaje promedio del espacio de disco utilizado en todos los nodos del clúster. Nos referiremos a esta alarma como la alarma predeterminada de espacio en disco.

El objetivo de la alarma predeterminada de espacio en disco es ayudarle a supervisar la capacidad de almacenamiento de su clúster. Puede configurar esta alarma en función de las necesidades de su data warehouse. Por ejemplo, puede usar la advertencia como un indicador de que tal vez tenga que ajustar el tamaño del clúster. Puede cambiar el tamaño a un tipo de nodo diferente o agregar nodos, o quizás comprar nodos reservados para una futura ampliación.

La alarma predeterminada de espacio en disco se activa cuando el uso del disco alcanza o supera un porcentaje específico una determinada cantidad de veces y con una duración específica. De manera predeterminada, esta alarma se activa cuando se alcanza el porcentaje que haya especificado y cuando permanece, o supera, en ese porcentaje durante cinco minutos o más tiempo. Puede editar los valores predeterminados después de lanzar su clúster.

Cuando se desencadena la alarma de CloudWatch, Amazon Simple Notification Service (Amazon SNS) envía una notificación a los destinatarios especificados para avisarles que se ha alcanzado el límite de porcentaje indicado. Amazon SNS utiliza un tema para especificar los destinatarios y el mensaje que se envía en las notificaciones. Puede utilizar un tema de Amazon SNS existente o, de lo contrario, se puede crear un tema en función de la configuración que especificó cuando lanzó el clúster. Puede editar el tema de esta alarma después de lanzar el clúster. Para obtener más información acerca de cómo crear temas de Amazon SNS, consulte Introducción a Amazon Simple Notification Service.

Después de lanzar el clúster, puede ver y editar la alarma desde la ventana Estado del clúster, bajo Alarmas de CloudWatch. El nombre es percentage-disk-space-used-default-**<*cadena*>**. Puede abrir la alarma para ver el tema de Amazon SNS con el que está asociada y editar la configuración de la alarma. Si no seleccionó un tema de Amazon SNS existente, el tema que se cree se llamará **<*nombredelclúster*>**-default-alarms (**<*destinatario*>**); por ejemplo, clústerdeejemplo-default-alarms (notificar@ejemplo.com).

Para obtener más información acerca de cómo configurar y editar la alarma predeterminada de espacio en disco, consulte Creación de un clúster y Crear o editar una alarma de espacio en disco.

> **Note**
>
> Si elimina el clúster, no se eliminará la alarma asociada con el clúster, pero tampoco se activará. Si ya no necesita la alarma, puede eliminarla desde la consola de CloudWatch.

Estado del clúster

El estado del clúster muestra el estado actual del clúster. En la siguiente tabla, se proporciona una descripción de cada estado del clúster.

Estado	Descripción
`available`	El clúster se está ejecutando y está disponible.
`available, prep-for-resize`	Se está preparando el clúster para un cambio de tamaño elástico. El clúster está en ejecución y disponible para consultas de lectura y escritura, aunque las operaciones de clúster, como crear instantáneas, no están disponibles.

Estado	Descripción
`available, resize-cleanup`	Una operación de cambio de tamaño elástico está completando la transferencia de datos a los nuevos nodos del clúster. El clúster está en ejecución y disponible para consultas de lectura y escritura, aunque las operaciones de clúster, como crear instantáneas, no están disponibles.
`cancelling-resize`	Se está cancelando la operación de cambio de tamaño.
`creating`	Amazon Redshift está creando el clúster. Para obtener más información, consulte Creación de un clúster.
`deleting`	Amazon Redshift está eliminando el clúster. Para obtener más informaci ón, consulte Eliminación de un clúster.
`final-snapshot`	Amazon Redshift está realizando una instantánea final del clúster antes de eliminarlo. Para obtener más información, consulte Eliminación de un clúster.
`hardware-failure`	Se detectó un error de hardware en el clúster. Si tiene un clúster de nodo único, el nodo no puede reemplazarse. Para recuperar su clúster, restaure una snapshot. Para obtener más informaci ón, consulte Instantáneas y copias de seguridad de Amazon Redshift.
`incompatible-hsm`	Amazon Redshift no puede conectarse al módulo de seguridad de hardware (HSM). Compruebe la configuración del HSM entre el clúster y el HSM. Para obtener más información, consulte Cifrado de Amazon Redshift con módulos de seguridad de hardware.
`incompatible-network`	Hay un problema con la configuración de red subyacente. Asegúrese de que la VPC en la que lanzó el clúster exista y de que está bien configura da. Para obtener más información, consulte Administración de clústeres en una VPC.

Estado	Descripción
`incompatible-parameters`	Hay un problema con uno o más valores de parámetros en el grupo de parámetros asociados y no se pueden aplicar los valores del parámetro . Modifique el grupo de parámetros y actualice todo valor que no sea válido. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift.
`incompatible-restore`	Hubo un problema al restaurar el clúster desde la snapshot. Vuelva a restaurar el clúster con una snapshot diferente. Para obtener más información, consulte Instantáneas y copias de seguridad de Amazon Redshift.
`modifying`	Amazon Redshift está aplicando cambios al clúster. Para obtener más información, consulte Modificación de un clúster.
`paused`	El clúster está en pausa. Para obtener más información, consulte Pausa y reanudación de clústeres.
`rebooting`	Amazon Redshift está reiniciando el clúster. Para obtener más informaci ón, consulte Reinicio de un clúster.
`renaming`	Amazon Redshift está aplicando un nuevo nombre al clúster. Para obtener más información, consulte Cambio de nombre de los clústeres.
`resizing`	Amazon Redshift está cambiando el tamaño del clúster. Para obtener más información, consulte Redimensionamiento de un clúster.
`rotating-keys`	Amazon Redshift está rotando las claves de cifrado del clúster. Para obtener más información, consulte Rotación de claves de cifrado en Amazon Redshift.
`storage-full`	El clúster alcanzó su capacidad de almacenamiento. Cambie el tamaño del clúster para agregar nodos o elija un tamaño de nodo diferente. Para obtener más información, consulte Redimensionamiento de un clúster.
`updating-hsm`	Amazon Redshift está actualizando la configuración de HSM.

Consideraciones para el uso de clústeres aprovisionados de Amazon Redshift

Una vez creado el clúster, en esta sección encontrará información sobre las regiones en las que están disponibles las características, las tareas de mantenimiento, los tipos de nodos y los límites de uso.

Temas

- Consideraciones sobre regiones y zonas de disponibilidad
- Mantenimiento de clústeres
- Administración de los límites de uso en Amazon Redshift
- Características de red compatibles con los nodos RA3
- Tipos de nodos

Consideraciones sobre regiones y zonas de disponibilidad

Amazon Redshift está disponible en varias regiones de AWS. De manera predeterminada, Amazon Redshift aprovisiona su clúster en una zona de disponibilidad (AZ) seleccionada de manera aleatoria dentro de la región de AWS que haya elegido. Todos los nodos del clúster se aprovisionan en la misma zona de disponibilidad.

Opcionalmente, puede solicitar una zona de disponibilidad específica si Amazon Redshift está disponible en dicha zona. Por ejemplo, si ya dispone de una instancia de Amazon EC2 que se ejecuta en una zona de disponibilidad, es posible que desee crear el clúster de Amazon Redshift en la misma zona para reducir la latencia. Por otro lado, es posible que desee elegir otra zona de disponibilidad para obtener una mayor disponibilidad. Puede suceder que Amazon Redshift no esté disponible en todas las zonas de disponibilidad de una región de AWS.

Para obtener una lista de las regiones de AWS admitidas en las que se puede aprovisionar un clúster de Amazon Redshift, consulte Puntos de conexión de Amazon Redshift en la Referencia general de Amazon Web Services.

Mantenimiento de clústeres

Amazon Redshift realiza tareas de mantenimiento de forma periódica para aplicar actualizaciones al clúster. Durante estas actualizaciones, su clúster de Amazon Redshift no está disponible para las

operaciones habituales. Existen varias formas de controlar cómo realizamos el mantenimiento de su clúster. Por ejemplo, puede controlar cuando implementamos actualizaciones en sus clústeres. También puede elegir si su clúster ejecuta la versión más reciente o la versión anterior a la versión más reciente. Finalmente, tiene la opción de posponer las actualizaciones de mantenimiento que no son obligatorias.

Temas

- Periodos de mantenimiento
- Posponer el mantenimiento
- Elección de pistas de mantenimiento del clúster
- Administración de versiones del clúster
- Reversión de la versión del clúster
- Determinación de la versión de mantenimiento del clúster

Periodos de mantenimiento

Amazon Redshift asigna un periodo aleatorio de mantenimiento de 30 minutos en un bloque de 8 horas por región de AWS, que se lleva a cabo un día aleatorio de la semana (de lunes a domingo, inclusive).

Periodos de mantenimiento predeterminados

En la siguiente lista, se muestran los bloques de tiempo de cada región de AWS desde la que se asignan los periodos de mantenimiento predeterminados:

- Región EE. UU. Este (Norte de Virginia): de 03:00 a 11:00 UTC
- Región EE. UU. Este (Ohio): de 03:00 a 11:00 UTC
- Región EE. UU. Oeste (Norte de California): de 06:00 a 14:00 UTC
- Región EE. UU. Oeste (Oregón): de 06:00 a 14:00 UTC
- Región África (Ciudad del Cabo): de 20:00 a 04:00 UTC
- Región Asia-Pacífico (Hong Kong): de 13:00 a 21:00 UTC
- Región Asia-Pacífico (Hyderabad): de 16:30 a 00:30 UTC
- Región Asia-Pacífico (Yakarta): de 15:00 a 23:00 UTC
- Región Asia-Pacífico (Melbourne): de 12:00 a 20:00 UTC

- Región Asia-Pacífico (Mumbai): de 16:30 a 00:30 UTC
- Región Asia-Pacífico (Osaka): de 13:00 a 21:00 UTC
- Región Asia-Pacífico (Seúl): de 13:00 a 21:00 UTC
- Región Asia-Pacífico (Singapur): de 14:00 a 22:00 UTC
- Región Asia-Pacífico (Sídney): de 12:00 a 20:00 UTC
- Región Asia-Pacífico (Tokio): de 13:00 a 21:00 UTC
- Región Canadá (Central): de 03:00 a 11:00 UTC
- Región Oeste de Canadá (Calgary): de 04:00 a 12:00 UTC
- Región China (Pekín): de 13:00 a 21:00 UTC
- Región China (Ningxia): de 13:00 a 21:00 UTC
- Región Europa (Fráncfort): de 06:00 a 14:00 UTC
- Región Europa (Irlanda): de 22:00 a 06:00 UTC
- Región Europa (Londres): de 22:00 a 06:00 UTC
- Región Europa (Milán): de 21:00 a 05:00 UTC
- Región Europa (París): de 23:00 a 07:00 UTC
- Región Europa (Estocolmo): de 23:00 a 07:00 UTC
- Región Europa (Zúrich): de 20:00 a 04:00 UTC
- Región de Israel (Tel Aviv): de 20:00 a 04:00 UTC
- Región Europa (España): de 21:00 a 05:00 UTC
- Región Medio Oriente (Baréin): de 13:00 a 21:00 UTC
- Región Medio Oriente (EAU): de 18:00 a 02:00 UTC
- Región América del Sur (São Paulo): de 19:00 a 03:00 UTC

Si hay un evento de mantenimiento programado para una semana determinada, comienza dentro del periodo de mantenimiento de 30 minutos asignado. Mientras Amazon Redshift efectúa las tareas de mantenimiento, termina las consultas o cualquier otra operación que esté en progreso. La mayoría de las tareas de mantenimiento se completan dentro del periodo de mantenimiento de 30 minutos, pero es posible que algunas tareas sigan ejecutándose después de que termine el periodo. Si no es necesario realizar tareas de mantenimiento durante el periodo de mantenimiento programado, su clúster continúa funcionando de manera habitual hasta el próximo periodo de mantenimiento programado.

Puede cambiar el periodo de mantenimiento programado si modifica el clúster, ya sea mediante programación o la consola de Amazon Redshift. En la pestaña Mantenimiento, podrá encontrar el período de mantenimiento y configurar el día y la hora en que se realizará para el clúster.

Es posible que un clúster se reinicie fuera de un periodo de mantenimiento. Esto puede ocurrir por varios motivos. Otra razón común es que se ha detectado un problema en el clúster y se están realizando operaciones de mantenimiento para devolverlo a un estado correcto. Para obtener más información, consulte el artículo ¿Por qué se reinició mi clúster de Amazon Redshift fuera del periodo de mantenimiento?, que proporciona detalles sobre los motivos por los que esto podría ocurrir.

Posponer el mantenimiento

Para volver a programar el período de mantenimiento de su clúster, tiene la opción de posponer el mantenimiento hasta 45 días. Por ejemplo, si el periodo de mantenimiento del clúster está establecido el miércoles de 8:30 h a 9:00 h UTC y necesite acceder al clúster justo a esa hora, puede posponer el mantenimiento.

Si aplaza el mantenimiento, Amazon Redshift seguirá aplicando actualizaciones de hardware u otras actualizaciones de seguridad obligatorias a su clúster. Su clúster no está disponible durante estas actualizaciones.

Si hay programada una actualización de hardware u otra actualización de seguridad obligatoria durante el próximo periodo de mantenimiento, Amazon Redshift le enviará notificaciones por adelantado en la categoría Pendiente. Para obtener más información sobre las notificaciones de eventos pendientes, consulte Notificaciones de eventos de Amazon Redshift.

También puede elegir recibir notificaciones de eventos de Amazon Simple Notification Service (Amazon SNS). Para obtener más información sobre la suscripción a notificaciones de eventos de Amazon SNS, consulte Suscripción a notificaciones de eventos de clúster de Amazon Redshift.

Si pospone el mantenimiento del clúster, no se puede posponer el periodo de mantenimiento comience justo después del periodo de postergación.

> **Note**
>
> No se puede posponer el mantenimiento una vez que haya comenzado.

Para obtener más información sobre el mantenimiento de clústeres, consulte la siguiente documentación:

- Periodos de mantenimiento
- Administración de clústeres a través de la consola
- Modificación de un clúster

Elección de pistas de mantenimiento del clúster

Cuando Amazon Redshift lanza una nueva versión del clúster, este se actualiza durante el periodo de mantenimiento. Puede controlar si el clúster se actualiza a la versión aprobada más reciente o a la versión anterior.

La pista de mantenimiento controla qué versión del clúster se aplica durante un periodo de mantenimiento. Cuando Amazon Redshift lanza una nueva versión del clúster, esa nueva versión se asigna a la pista actual y la versión anterior se asigna a la pista anterior. Para establecer la pista de mantenimiento para el clúster, especifique uno de los siguientes valores.

- Current (Actual): para usar la versión del clúster aprobada más reciente.
- Trailing (Anterior): para usar la versión del clúster anterior a la versión actual.
- Preview (Previsualización): para usar la versión del clúster que contiene las nuevas características disponibles para versión preliminar.

Por ejemplo, imagine que el clúster en este momento está ejecutando la versión 1.0.2762 y la versión actual de Amazon Redshift es la 1.0.3072. Si establece el valor de pista de mantenimiento en Current (Actual), el clúster se actualiza a la versión 1.0.3072 (la siguiente versión aprobada) durante el siguiente periodo de mantenimiento. Si establece el valor de la pista de mantenimiento en Trailing (Anterior), el clúster no se actualizará hasta que haya una nueva versión posterior a la versión 1.0.3072.

Pistas de previsualización

Puede que no siempre haya una pista de previsualización disponible. Cuando elija una pista de previsualización, también deberá seleccionar un nombre de pista. Las pistas de previsualización y sus recursos relacionados son temporales, tienen limitaciones funcionales y pueden no contener todas las características actuales de Amazon Redshift que están disponibles en otras pistas. Cuando trabaje con pistas de previsualización:

- Utilice la nueva consola de Amazon Redshift cuando trabaje con pistas de previsualización. Por ejemplo, al crear un clúster para utilizarlo con las características de vista previa.

- No puede cambiar un clúster de una pista de previsualización a otra.
- No puede cambiar un clúster a una pista de previsualización desde una pista actual o anterior.
- No puede cambiar un clúster desde una pista de previsualización a una pista actual o anterior.
- No se puede restaurar desde una instantánea creada a partir de una pista de previsualización diferente.
- Solo puede usar la pista de previsualización cuando cree un nuevo clúster o al restaurar desde una instantánea.
- No puede restaurar desde una instantánea creada a partir de una pista de previsualización diferente o con una versión de mantenimiento del clúster posterior a la versión del clúster de la pista de previsualización. Por ejemplo, cuando se restaura un clúster a una pista de previsualización, solo se puede usar una instantánea creada a partir de una versión de mantenimiento del clúster anterior a la de la pista de previsualización.

Cambio entre pistas de mantenimiento

El cambio de pistas para un clúster es, por lo general, una decisión que se toma una única vez. Debe tener cuidado al cambiar pistas. Si cambia la pista de mantenimiento de Trailing (Anterior) a Current (Actual), actualizaremos el clúster a la versión de la pista Current (Actual) durante el siguiente periodo de mantenimiento. No obstante, si cambia la pista de mantenimiento del clúster a Trailing (Anterior), no actualizaremos el clúster hasta que haya una nueva versión después de la versión de la pista Current (Actual).

Pistas de mantenimiento y restauración

Una instantánea hereda la pista de mantenimiento del clúster de origen. Si cambia la pista de mantenimiento del clúster de origen después de tomar una instantánea, la instantánea y el clúster de origen estarán en pistas diferentes. Si realiza una restauración desde la instantánea, el nuevo clúster estará en la pista de mantenimiento que había heredado del clúster de origen. Puede cambiar la pista de mantenimiento cuando se complete la operación de restauración. Cambiar el tamaño de un clúster no afecta a la pista de mantenimiento del clúster.

Administración de versiones del clúster

Una pista de mantenimiento es una serie de versiones. Puede decidir si su clúster está en la pista Current (Actual) o en la pista Trailing (Anterior). Si pone su clúster en la pista Current (Actual), siempre se actualizará a la versión de clúster más reciente durante el periodo de mantenimiento. Si

pone su clúster en la pista Trailing (Anterior), siempre ejecutará la versión de clúster que se publicó inmediatamente anterior a la versión más reciente.

La columna Release status (Estado de la versión) que se encuentra en la lista de clústeres de la consola de Amazon Redshift indica si alguno de los clústeres está disponible para su actualización.

Reversión de la versión del clúster

Si el clúster está actualizado con la última versión, puede optar por revertirlo a la versión anterior.

Para obtener información detallada acerca de las características y mejoras incluidas con cada versión del clúster, consulte Historial de versiones del clúster.

Para revertir a una versión anterior del clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Seleccione el clúster que quiere revertir.
4. En Actions (Acciones), seleccione Roll back cluster version (Revertir versión del clúster). Aparecerá la página Roll back cluster version (Revertir versión del clúster).
5. SI hay una versión disponible para revertir, siga las instrucciones de la página.
6. Seleccione Roll back now (Revertir ahora).

Determinación de la versión de mantenimiento del clúster

Puede determinar la versión del motor y de la base de datos de Amazon Redshift con la consola de Amazon Redshift.

Para encontrar la versión de un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Supervisión de consultas), Databases (Bases de datos), Datashares (Recursos compartidos de datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).

3. Seleccione la pestaña Maintenance (Mantenimiento) para obtener más información.
4. En la sección Maintenance (Mantenimiento), busque Current cluster versión (Versión actual del clúster).

> **Note**
>
> Aunque la consola muestra esta información en un único campo, se trata de dos parámetros en la API de Amazon Redshift: `ClusterVersion` y `ClusterRevisionNumber`. Para obtener más información, consulte Clúster en la Referencia de la API de Amazon Redshift.

Administración de los límites de uso en Amazon Redshift

Puede definir límites para monitorear y controlar el uso y el costo asociado de algunas características de Amazon Redshift. Puede crear límites de uso diarios, semanales y mensuales, y definir acciones que Amazon Redshift realizará automáticamente si se alcanzan esos límites. Las acciones pueden ser, por ejemplo, incluir un evento en una tabla del sistema para registrar cualquier uso que exceda los límites definidos. Otras posibles acciones pueden ser el envío de alertas con Amazon SNS y Amazon CloudWatch para informar a un administrador y desactivar cualquier uso posterior para controlar los costos.

Puede definir límites de uso en cada clúster. Una vez que se ha creado el clúster, puede definir límites de uso para las siguientes características:

- Amazon Redshift Spectrum
- Escalado de simultaneidad de Amazon Redshift
- Uso compartido de datos entre regiones de Amazon Redshift

Los límites de uso están disponibles con la versión 1.0.14677 o posteriores en las regiones de AWS que disponen de la característica de escalado de simultaneidad de Amazon Redshift Spectrum y Amazon Redshift.

Los límites de Redshift Spectrum especifican el límite de la cantidad total de datos analizados en incrementos de 1 TB. Los límites de escalado de simultaneidad especifican el umbral del total de tiempo invertido en el escalado de simultaneidad en incrementos de 1 minuto. El límite de uso de recursos compartidos de datos entre regiones especifica el umbral de la cantidad total de datos analizados en incrementos de 1 TB.

Se puede establecer un límite diario, semanal o mensual (se utiliza el formato UTC para determinar el inicio y el final del período). Si crea un límite en mitad de un período, dicho límite se medirá desde ese punto hasta el final del período. Por ejemplo, si crea un límite mensual el 15 de marzo, el primer período mensual se medirá desde el 15 hasta el 31 de marzo.

Puede definir varios límites de uso para cada característica. Cada límite puede tener una acción diferente. Entre las posibles acciones se incluyen las siguientes:

- Registrar en la tabla del sistema: esta es la acción predeterminada. La información se registra en la tabla STL_USAGE_CONTROL. Este registro es útil para poder evaluar el uso pasado y decidir los límites de uso futuros. Para obtener más información acerca del contenido que se registra, consulte STL_USAGE_CONTROL en la Guía para desarrolladores de bases de datos Amazon Redshift.
- Alertar: Amazon Redshift emite métricas de CloudWatch para el uso disponible y consumido. Puede definir hasta tres límites de uso para cada característica. Si habilita la acción de alerta a través de la consola de Amazon Redshift, se creará automáticamente una alarma de CloudWatch en estas métricas. Si lo desea, puede asociar una suscripción de Amazon SNS a esa alarma. Si está utilizando una operación de API o AWS CLI, no olvide crear la alarma de CloudWatch manualmente. Cuando se alcance el umbral, los eventos también se registrarán en una tabla del sistema.
- Desactivar la característica: cuando se alcanza el límite, Amazon Redshift desactiva la característica hasta que se actualice la cuota para el próximo periodo (diario, semanal o mensual). Solo puede haber un límite en cada característica con la acción de desactivación. Los eventos también se registran en una tabla del sistema. Además, se pueden emitir alertas.

Los límites de uso se mantienen hasta que se elimina la propia definición del límite de uso o el clúster.

Puede definir y administrar los límites de uso con la nueva consola de Amazon Redshift, la AWS CLI o las operaciones de API de Amazon Redshift. Para definir un límite en la consola de Amazon Redshift, vaya al clúster y elija Configure usage limit (Configurar límite de uso) en Actions (Acciones). Para ver los límites de uso definidos previamente para el clúster, vaya al clúster y elija la pestaña Maintenance (Mantenimiento), sección Usage limits (Límites de uso). Para ver el uso disponible y consumido del clúster, desplácese hasta el clúster. Elija la pestaña Cluster performance (Rendimiento del clúster) y consulte los gráficos sobre el uso que se ha consumido en una característica.

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar los límites de uso. Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

- create-usage-limit
- describe-usage-limits
- modify-usage-limit
- delete-usage-limit

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar los límites de uso: Para obtener más información, consulte la Referencia de la API de Amazon Redshift.

- CreateUsageLimit
- DescribeUsageLimits
- ModifyUsageLimit
- DeleteUsageLimit

Vea el siguiente video para obtener información acerca de cómo crear y monitorear límites de uso mediante la consola de Amazon Redshift: Controles de costos para Amazon Redshift Spectrum y escalado de simultaneidad.

Características de red compatibles con los nodos RA3

Los nodos RA3 admiten una serie de características de red que no están disponibles para los nodos DS2 o DC2. En esta sección, se proporcionan breves descripciones de cada característica y enlaces a documentación adicional:

- Punto de conexión de VPC del clúster aprovisionado: cuando crea o restaura un clúster RA3, Amazon Redshift utiliza un puerto en los rangos 5431-5455 o 8191-8215. Cuando el clúster se configura en un puerto de uno de estos rangos, Amazon Redshift crea automáticamente un punto de conexión de VPC en su cuenta de AWS para el clúster y le asocia una dirección IP privada. Si configura el clúster para que sea de acceso público, Redshift crea una dirección IP elástica en su cuenta de AWS y la asocia al punto de conexión de VPC. Para obtener más información, consulte Configuración de las opciones de comunicación del grupo de seguridad para un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor.

- Clústeres RA3 de subred única: puede crear un clúster RA3 con una única subred, pero no puede utilizar las características de recuperación de desastres. Se produce una excepción si habilita la reubicación del clúster cuando la subred no tiene varias zonas de disponibilidad (AZ).
- Grupos de subredes y clústeres RA3 de varias subredes: puede crear un clúster RA3 con varias subredes si crea un grupo de subredes al aprovisionar el clúster en su nube privada virtual (VPC). Un grupo de subredes de clústeres le permite especificar un conjunto de subredes en su VPC y Amazon Redshift crea el clúster en una de ellas. Después de crear un grupo de subredes, puede quitar las subredes que agregó previamente o agregar más. Para obtener más información, consulte Grupos de subredes del clúster de Amazon Redshift.
- Acceso a puntos de conexión entre cuentas o entre VPC: puede acceder a un clúster aprovisionado o a un grupo de trabajo de Amazon Redshift sin servidor mediante la configuración de un punto de conexión de VPC administrado por Redshift. Puede configurarlo como una conexión privada entre una VPC que contenga un clúster o un grupo de trabajo y una VPC en la que ejecute una herramienta de cliente, por ejemplo. De esta forma, puede acceder al almacenamiento de datos sin usar una dirección IP pública ni enrutar el tráfico a través de Internet. Para obtener más información, consulte Uso de puntos de conexión de VPC administrados por Redshift en Amazon Redshift.
- Reubicación de clústeres: puede trasladar un clúster a otra zona de disponibilidad (AZ) sin pérdida de datos, cuando se produzca una interrupción del servicio. Se habilita en la consola. Para obtener más información, consulte Reubicación del clúster.
- Nombre de dominio personalizado: puede crear un nombre de dominio personalizado, también conocido como URL personalizada, para su clúster de Amazon Redshift. Es un registro DNS fácil de leer que dirige las conexiones de los clientes SQL al punto de conexión de su clúster. Para obtener más información, consulte Uso de un nombre de dominio personalizado para las conexiones de cliente.

Tipos de nodos

En estas secciones, se detallan las tareas disponibles para diversos tipos de nodos.

Temas

- Nodos RA3
- Nodos DC2 y DS2

Nodos RA3

En estas secciones, se detallan las tareas disponibles para los nodos RA3.

Temas

- Información general
- Actualización a tipos de nodo RA3

Información general

Se recomienda actualizar las cargas de trabajo existentes que se ejecutan en clústeres de tipo de nodo DS2 a tipos de nodo RA3 para aprovechar el rendimiento mejorado y obtener más capacidad de almacenamiento. Los nodos RA3 proporcionan las siguientes ventajas:

- Son flexibles para aumentar su capacidad de cómputo sin aumentar sus costos de almacenamiento. Además, escalan su almacenamiento sin aprovisionar en exceso la capacidad de cómputo.
- Utilizan unidades de estado sólido de alto rendimiento para los datos calientes y Amazon S3 para los datos fríos. Por lo tanto, proporcionan facilidad de uso, almacenamiento rentable y alto rendimiento de consultas.
- Utilizan redes de ancho de banda alto creadas en AWS Nitro System para reducir aún más el tiempo necesario para descargar datos en Amazon S3 y recuperarlos de dicho servicio.

Considere la posibilidad de seleccionar tipos de nodo RA3 en estos casos:

- Si necesita flexibilidad para escalar y pagar el cálculo por separado del almacenamiento.
- Consulta una fracción de los datos totales.
- El volumen de datos está creciendo rápidamente o se espera que crezca rápidamente.
- Desea flexibilidad para ajustar el tamaño del clúster en función únicamente de las necesidades de rendimiento.

Para utilizar tipos de nodo RA3, su región de AWS debe admitir RA3. Para obtener más información, consulte Disponibilidad del tipo de nodo RA3 en las regiones de AWS.

> **Important**
>
> Puede utilizar los tipos de nodo ra3.xlplus solo con la versión 1.0.21262 o posterior del clúster. Puede ver la versión de un clúster existente con la consola de Amazon Redshift. Para obtener más información, consulte Determinación de la versión de mantenimiento del clúster. Asegúrese de utilizar la nueva consola de Amazon Redshift cuando trabaje con tipos de nodo RA3.
>
> Además, para utilizar tipos de nodos RA3 con operaciones de Amazon Redshift que utilizan la pista de mantenimiento, el valor de la pista de mantenimiento debe establecerse en una versión de clúster que admita RA3. Para obtener más información sobre las pistas de mantenimiento, consulte Elección de pistas de mantenimiento del clúster.

Tenga en cuenta lo siguiente al utilizar los tipos de nodos RA3 de un solo nodo.

- Se admiten productores y consumidores de recursos para compartir datos.
- Para cambiar los tipos de nodos, solo se admite el redimensionamiento clásico. No se admite cambiar el tipo de nodo mediante el redimensionamiento elástico o la restauración de instantáneas. Se admiten los casos siguientes:
  - Redimensionamiento clásico de ds2.xlarge de 1 nodo a ra3.xlplus de 1 nodo y viceversa.
  - Redimensionamiento clásico de ds2.xlarge de 1 nodo a ra3.xlplus de varios nodos y viceversa.
  - Redimensionamiento clásico de ds2.xlarge de varios nodos a ra3.xlplus de 1 nodo y viceversa.
  - Redimensionamiento clásico de dc2.xlarge de 1 nodo a ra3.xlplus de 1 nodo y viceversa.
  - Redimensionamiento clásico de dc2.xlarge de 1 nodo a ra3.xlplus de varios nodos y viceversa.
  - Redimensionamiento clásico de dc2.xlarge de varios nodos a ra3.xlplus de 1 nodo y viceversa.

Uso del almacenamiento administrado de Amazon Redshift

Con el almacenamiento administrado de Amazon Redshift, puede almacenar y procesar todos sus datos en Amazon Redshift mientras obtiene más flexibilidad para escalar la capacidad de informática y de almacenamiento por separado. Siga adquiriendo datos con el comando COPY o INSERT. Para optimizar el rendimiento y administrar la colocación automática de datos en los niveles de almacenamiento, Amazon Redshift aprovecha las optimizaciones, como la temperatura del bloque de datos, la antigüedad del bloque de datos y los patrones de cargas de trabajo. Cuando es necesario, Amazon Redshift escala el almacenamiento de forma automática a Amazon S3 sin necesidad de ninguna acción manual.

Para obtener más información acerca de los costos de almacenamiento, consulte Precios de Amazon Redshift.

Administración de tipos de nodo RA3

Para aprovechar la separación del proceso de computación del almacenamiento, puede crear o actualizar el clúster con el tipo de nodo RA3. Para utilizar los tipos de nodo RA3, cree sus clústeres en una nube virtual privada (EC2-VPC).

Para cambiar la cantidad de nodos del clúster de Amazon Redshift con el tipo de nodo RA3, realice alguna de las siguientes acciones:

- Agregue o elimine nodos con la operación de cambio de tamaño elástico. En algunas situaciones, la eliminación de nodos de un clúster RA3 no se permite con el cambio de tamaño elástico. Por ejemplo, cuando una actualización de recuento de nodos 2:1 coloca el número de sectores por nodo en 32. Para obtener más información, consulte Cambio de tamaño de clústeres. Si el cambio de tamaño elástico no está disponible, use el cambio de tamaño clásico.
- Agregue o quite nodos con la operación clásica de cambio de tamaño. Elija esta opción cuando cambie el tamaño a una configuración que no esté disponible mediante el cambio de tamaño elástico. El cambio de tamaño elástico es más rápido que el cambio de tamaño clásico. Para obtener más información, consulte Cambio de tamaño de clústeres.

Disponibilidad del tipo de nodo RA3 en las regiones de AWS

Los tipos de nodo RA3 solo están disponibles en las siguientes regiones de AWS:

- Región EE. UU. Este (Norte de Virginia) (us-east-1)
- Región EE. UU. Este (Ohio) (us-east-2)
- Región EE. UU. Oeste (Norte de California) (us-west-1)
- Región EE. UU. Oeste (Oregón) (us-west-2)
- Región África (Ciudad del Cabo) (af-south-1)
- Región Asia-Pacífico (Hong Kong) (ap-east-1)
- Región Asia Pacífico (Hyderabad) (ap-south-2)
- Región Asia-Pacífico (Yakarta) (ap-southeast-3)
- Región Asia Pacífico (Melbourne) (ap-southeast-4)
- Región Asia-Pacífico (Mumbai) (ap-south-1)

- Región Asia-Pacífico (Osaka) (ap-northeast-3)
- Región Asia-Pacífico (Seúl) (ap-northeast-2)
- Región Asia-Pacífico (Singapur) (ap-southeast-1)
- Región Asia-Pacífico (Sídney) (ap-southeast-2)
- Región Asia-Pacífico (Tokio) (ap-northeast-1)
- Región Canadá (Central) (ca-central-1)
- Región Oeste de Canadá (Calgary) (ca-west-1)
- Región China (Pekín) (cn-north-1)
- Región China (Ningxia) (cn-northwest-1)
- Región Europa (Fráncfort) (eu-central-1)
- Región Europa (Zúrich) (eu-central-2)
- Región Europa (Irlanda) (eu-west-1)
- Región Europa (Londres) (eu-west-2)
- Región Europa (Milán) (eu-south-1)
- Región Europa (España) (eu-south-2)
- Región Europa (París) (eu-west-3)
- Región Europa (Estocolmo) (eu-north-1)
- Región de Israel (Tel Aviv) (il-central-1)
- Región Medio Oriente (Baréin) (me-south-1)
- Región Medio Oriente (me-central-1)
- Región América del Sur (São Paulo) (sa-east-1)
- AWS GovCloud (EE. UU. Este) (us-gov-east-1)
- AWS GovCloud (EE. UU. Oeste) (us-gov-west-1)

Actualización a tipos de nodo RA3

Para actualizar el tipo de nodo existente a RA3, tiene las siguientes opciones para cambiar el tipo de nodo:

- Restauración a partir de una instantánea: Amazon Redshift utiliza la instantánea más reciente de su clúster DS2 o DC2 y la restaura para crear un nuevo clúster RA3. Tan pronto como se complete

la creación del clúster (normalmente en cuestión de minutos), los nodos RA3 estarán listos para ejecutar toda la carga de trabajo de producción. Dado que la computación está separada del almacenamiento, los datos calientes se llevan a la caché local a velocidades rápidas gracias a un gran ancho de banda de red. Si restaura a partir de la última instantánea DS2 o DC2, RA3 conserva la información de bloques calientes de la carga de trabajo de DS2 o DC2 y rellena su caché local con los bloques más calientes. Para obtener más información, consulte Restauración de un clúster desde una instantánea.

Para mantener el mismo punto de conexión para las aplicaciones y los usuarios, puede cambiar el nombre del nuevo clúster RA3 por el mismo nombre que el clúster DS2 o DC2 original. Para cambiar el nombre del clúster, modifique el clúster en la consola de Amazon Redshift o la operación `ModifyCluster` de la API. Para obtener más información, consulte Cambio de nombre de los clústeres o la operación `ModifyCluster` de la API en la Referencia de la API de Amazon Redshift.

- Redimensionamiento elástico: cambie el tamaño del clúster mediante el redimensionamiento elástico. Cuando se utiliza el redimensionamiento elástico para cambiar el tipo de nodo, Amazon Redshift crea una instantánea y un nuevo clúster, elimina el antiguo clúster y cambia el nombre del nuevo clúster de forma automática. La operación de cambio de tamaño elástico puede ejecutarse bajo demanda o puede programarse para ejecutarse en un momento futuro. Puede actualizar rápidamente sus clústeres de tipo de nodo DS2 o DC2 existentes a RA3 con el cambio de tamaño elástico. Para obtener más información, consulte Elastic resize (Cambio de tamaño elástico).

En la siguiente tabla se muestran recomendaciones al actualizar a tipos de nodos RA3. (Estas recomendaciones también se aplican a los nodos reservados).

Las recomendaciones de esta tabla son tipos y tamaños de nodos de clústeres iniciales, pero dependen de los requisitos de computación de la carga de trabajo. Para calcular mejor sus requisitos, considere la posibilidad de realizar una prueba de concepto (POC) en la que se utilice Versiones de prueba para ejecutar posibles configuraciones. Aprovisione un clúster para el almacenamiento de datos de la POC en lugar de Redshift sin servidor. Para obtener más información sobre cómo realizar una prueba de concepto, consulte Realización de una prueba de concepto de Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Tipo de nodo existente	Cantidad existente de nodos	Nuevo tipo de nodo recomendado	Acción de actualización	
ds2.xlarge	1	ra3.xlplus	Cree un clúster ra3.xlplus de 1 nodo[1].	
ds2.xlarge	2	ra3.xlplus	Cree un clúster ra3.xlplus de 2 nodos[1].	
ds2.xlarge	3	ra3.xlplus	Cree un clúster ra3.xlplus de 2 nodos[1].	
ds2.xlarge	4	ra3.xlplus	Cree un clúster ra3.xlplus de 3 nodos[1].	
ds2.xlarge	5	ra3.xlplus	Cree un clúster ra3.xlplus de 4 nodos[1].	
ds2.xlarge	6	ra3.xlplus	Cree un clúster ra3.xlplus de 4 nodos[1].	
ds2.xlarge	7	ra3.xlplus	Cree un clúster ra3.xlplus de 5 nodos[1].	
ds2.xlarge	8	ra3.4xlarge	Cree un clúster ra3.4xlarge de 2 nodos[1].	

Tipo de nodo existente	Cantidad existente de nodos	Nuevo tipo de nodo recomendado	Acción de actualización
ds2.xlarge	9	ra3.4xlarge	Cree un clúster ra3.4xlarge de 3 nodos[1].
ds2.xlarge	10	ra3.4xlarge	Cree un clúster ra3.4xlarge de 3 nodos[1].
ds2.xlarge	11-128	ra3.4xlarge	Cree 1 nodo de ra3.4xlarge por cada 4 nodos de ds2.xlarge[1].
ds2.8xlarge	2–15	ra3.4xlarge	Cree 2 nodos de ra3.4xlarge por cada 1 nodo de ds2.8xlarge.[1].
ds2.8xlarge	16–128	ra3.16xlarge	Cree 1 nodo de ra3.16xlarge por cada 2 nodos de ds2.8xlarge.[1].
dc2.8xlarge	2–15	ra3.4xlarge	Cree 2 nodos de ra3.4xlarge para cada 1 nodo de dc2.8xlarge[1].
dc2.8xlarge	16–128	ra3.16xlarge	Cree 1 nodo de ra3.16xlarge por cada 2 nodos de dc2.8xlarge[1].

Tipo de nodo existente	Cantidad existente de nodos	Nuevo tipo de nodo recomendado	Acción de actualización	
dc2.large	1–4	Ninguno	Mantenga el clúster dc2.large existente.	
dc2.large	5–15	ra3.xlplus	Cree 3 nodos de ra3.xlplus por cada 8 nodos de dc2.large[1].	
dc2.large	16-32	ra3.4xlarge	Cree 1 nodo de ra3.4xlarge por cada 8 nodos de dc2.large[1,2].	

[1]Es posible que se necesiten nodos adicionales en función de los requisitos de carga de trabajo. Agregar o quitar nodos en función de los requisitos de computación del rendimiento de consulta requerido.

[2] Los clústeres con el tipo de nodo dc2.large están limitados a 32 nodos.

El número mínimo de nodos para clústeres de algunos tipos de nodos RA3 es de 2 nodos. Tenga esto en cuenta al crear un clúster RA3.

Actualice nodos reservados DS2 a nodos reservados RA3 durante el redimensionamiento elástico o la restauración de instantáneas

Si tiene nodos reservados DS2, puede actualizarlos con la característica de actualización de nodos reservados RA3, mediante la consola de Amazon Redshift o la AWS CLI. En la consola, hay un par de formas de realizar esta operación.

Una forma es actualizar los nodos reservados de DS2 a RA3 durante un redimensionamiento elástico. Si tiene nodos reservados y selecciona nodos RA3, la consola lo guiará a través del proceso de actualización de nodos reservados. Desde un punto de vista técnico, el redimensionamiento elástico funciona igual tanto para los nodos reservados como para los nodos que no están reservados.

Si cambia el tamaño del clúster del tamaño recomendado, cuando configura el redimensionamiento elástico, la actualización de nodos reservados RA3 no estará disponible y no aparecerá en la consola. (Aún puede actualizar los nodos reservados de DS2 a RA3, pero el redimensionamiento no incluye la actualización de nodos reservados RA3 como parte del proceso). Tenga en cuenta también que es posible que el tamaño del clúster que desee no esté disponible debido a las limitaciones de tamaño del clúster para el redimensionamiento elástico. Por ejemplo, si tiene un clúster de nodos reservados DS2 de 4 nodos, es posible que no pueda seleccionar un clúster RA3 de 3 nodos. En este caso, puede realizar un redimensionamiento clásico para obtener el tamaño del clúster que desee.

Se producen un par de pasos después del redimensionamiento del clúster. En primer lugar, los datos se migran al clúster RA3. A continuación, la concesión de nodos reservados DS2 se convierte en un alquiler de nodos reservados RA3. Tenga en cuenta que el tiempo de migración de datos puede variar, en función del tamaño del clúster y de si el redimensionamiento es elástico o clásico. En el caso de un redimensionamiento clásico, es habitual que la migración de datos tarde varias horas.

Después de iniciar el redimensionamiento, realice un seguimiento del progreso viendo los mensajes en Events (Eventos), disponible en el Amazon Redshift dashboard (Panel de Amazon Redshift). Habrá una notificación de evento para el redimensionamiento y otra para la actualización del nodo reservado. Para obtener más información sobre el trabajo con eventos, consulte Eventos de Amazon Redshift. Después del redimensionamiento, el clúster redimensionado activo aparece en la AWS Management Console. También puede ver la concesión de los nodos reservados RA3 convertidos. Es posible que los nodos reservados DS2 de origen sigan apareciendo en la consola durante aproximadamente un día. No se cobra por esto. No elimine el nodo reservado DS2 de origen hasta que compruebe que el clúster RA3 está activo y que se haya generado la concesión de nodos reservados convertidos.

La otra forma de utilizar la característica de actualización de nodos reservados RA3 es cuando restaura desde una instantánea. Si selecciona el tipo de nodo RA3 y tiene nodos reservados DS2, en ese momento, puede seleccionar la característica de actualización de nodos reservados RA3. Cuando restaura desde una instantánea, se restaura a un clúster de nodos reservados RA3. Como se mencionó anteriormente, si elige un tamaño de clúster distinto del tamaño recomendado, la selección de actualización de nodos reservados RA3 no estará disponible en la consola.

Para obtener más información sobre el redimensionamiento de clústeres y la actualización de nodos, consulte Cambio de tamaño de clústeres. Allí encontrará una descripción detallada del proceso y también respuestas sobre lo que sucede con el clúster y los datos en el redimensionamiento. Para obtener más detalles acerca de los pasos del proceso de redimensionamiento elástico, consulte

Elastic resize (Cambio de tamaño elástico). Para obtener más información acerca de la restauración desde una instantánea, consulte Restauración de un clúster desde una instantánea.

Si tiene más preguntas sobre cómo actualizar los nodos reservados a RA3, por ejemplo, sobre la actualización de los nodos reservados de DC2 a RA3, contacte con AWS Support. Para obtener más información acerca de los precios de los nodos bajo demanda y reservados, consulte Precios de Amazon Redshift.

Si ya ha adquirido nodos reservados DS2, contacte con AWS para obtener ayuda para convertir los nodos reservados DS2 en nodos reservados RA3. Para contactar con AWS y obtener más información, consulte Instancias RA3 de Amazon Redshift con almacenamiento administrado.

Nodos DC2 y DS2

En estas secciones, se detallan las tareas disponibles para los nodos DC2 y DS2.

Temas

- Actualización de tipos de nodo DC1 a tipos de nodo DC2
- Actualización de un clúster DS2 en EC2-Classic para EC2-VPC

Actualización de tipos de nodo DC1 a tipos de nodo DC2

Para aprovechar las mejoras de rendimiento, puede actualizar sus clústeres DC1 a tipos de nodo DC2.

Los clústeres que usan el tipo de nodo DC2 deben lanzarse en una nube virtual privada (EC2-VPC).

Si el clúster DC1 no está en una VPC:

1. Cree una instantánea de su clúster DC1. Para obtener más información, consulte Instantáneas y copias de seguridad de Amazon Redshift.
2. Cree una VPC o elija una VPC existente en su cuenta. Para obtener más información, consulte Administración de clústeres en una VPC.
3. Restaure la instantánea en el nuevo clúster DC2 de la VPC. Para obtener más información, consulte Restauración de un clúster desde una instantánea.

Si el clúster DC1 ya está en una VPC, elija uno de los métodos siguientes:

- Cambie el tamaño del clúster DC1 y cambie el tipo de nodo a DC2 como parte de la operación. El clúster no está disponible durante un periodo de tiempo durante la operación de cambio de tamaño. Para obtener más información, consulte Cambio de tamaño de clústeres.
- Cree una instantánea del clúster DC1 y, a continuación, restaure la instantánea en un clúster DC2 en la VPC. Para obtener más información, consulte Restauración de un clúster desde una instantánea.

Tenga en cuenta lo siguiente al actualizar de tipos de nodos DC1 a DC2.

- Es posible que los clústeres DC1 que están 100% llenos no se actualicen a un número equivalente de nodos DC2. Si necesita más espacio en disco, puede.
  - Cambiar el tamaño a una configuración con más espacio en disco disponible.
  - Limpie los datos innecesarios mediante el truncamiento de tablas o la eliminación de filas.
- Los clústeres de DC2 no admiten redes de EC2-Classic. Si su clúster de CD1 no se está ejecutando en una VPC, cree una para su migración de DC2. Para obtener más información, consulte Administración de clústeres en una VPC.
- Si cambia el tamaño del clúster, podría ponerse en modo de solo lectura durante el periodo que dure la operación. Para obtener más información, consulte Cambio de tamaño de clústeres.
- Si ha adquirido nodos reservados DC1, puede actualizar sus nodos reservados DC1 a nodos DC2 durante el resto de su oferta. Para obtener más información sobre cómo cambiar la reserva con la AWS CLI, consulte Actualizar nodos reservados con AWS CLI.
- Si utiliza restaurar para actualizar de dc1.large a dc2.large y cambia el número de nodos, la instantánea debe haberse creado en la versión del clúster 1.0.10013 o posterior.
- Si utiliza restaurar para actualizar de dc1.8xlarge a dc2.8xlarge, la instantánea debe haberse creado en la versión del clúster 1.0.10013 o posterior.
- Si utiliza el cambio de tamaño elástico para actualizar de DC1 a DC2 y cambia el número de nodos, el clúster debe estar en la versión 1.0.10013 o posterior del clúster.
- Si una instantánea del clúster dc1.8xlarge que se va a actualizar es de un clúster anterior a la versión 1.0.10013, primero restaure la instantánea desde el clúster dc1.8xlarge en un nuevo clúster dc1.8xlarge con el mismo número de nodos. A continuación, utilice alguno de los métodos siguientes para actualizar el nuevo clúster dc1.8xlarge:
  - Utilice una instantánea del nuevo clúster restaurado para actualizarlo a dc2.8xlarge.
  - Utilice el redimensionamiento elástico para actualizar el nuevo clúster restaurado a dc2.8xlarge.

Actualización de un clúster DS2 en EC2-Classic para EC2-VPC

Los clústeres de Amazon Redshift se ejecutan en instancias de Amazon EC2 que están configuradas para el tipo y el tamaño de nodo de Amazon Redshift que usted elija. Para mejorar el rendimiento y la seguridad, le recomendamos actualizar el clúster en EC2-Classic para lanzarlo en una VPC con EC2-VPC.

Para actualizar su clúster DS2 en EC2-Classic para EC2-VPC

1. Cree una instantánea de su clúster DS2. Para obtener más información, consulte Instantáneas y copias de seguridad de Amazon Redshift.
2. Cree una VPC o elija una VPC existente en su cuenta. Para obtener más información, consulte Administración de clústeres en una VPC.
3. Restaure la instantánea en el nuevo clúster DS2 en la VPC. Para obtener más información, consulte Restauración de un clúster desde una instantánea.

Operaciones de clúster

Después de haber creado el clúster, hay varias operaciones que puede realizar en él. Las operaciones incluyen el cambio de tamaño, la pausa, la reanudación, el cambio de nombre y la eliminación.

Temas

- Cambio de tamaño de clústeres
- Pausa y reanudación de clústeres
- Cambio de nombre de los clústeres
- Cierre y eliminación de clústeres
- Reubicación del clúster
- Instantáneas y copias de seguridad de Amazon Redshift

Cambio de tamaño de clústeres

A medida que la capacidad y el rendimiento del almacenamiento de datos necesitan cambiar, se puede cambiar el tamaño del clúster para llevar a cabo el mejor uso de las opciones de computación y almacenamiento que proporciona Amazon Redshift.

La operación de cambio de tamaño está disponible en dos tipos:

- Cambio de tamaño elástico: puede agregar o eliminar nodos del clúster. También puede cambiar el tipo de nodo, como de nodos DS2 a nodos RA3. Un cambio de tamaño elástico se completa rápidamente y tarda una media de diez minutos. Por este motivo, lo recomendamos como primera opción. Cuando se lleva a cabo un cambio de tamaño elástico, se redistribuyen los sectores de datos, que son particiones a las que se les asigna memoria y espacio de disco en cada nodo. El cambio de tamaño elástico es adecuado en las siguientes situaciones:
  - Agrega o reduce nodos en un clúster existente, pero no cambia el tipo de nodo: esto se llama comúnmente cambio de tamaño in situ. Al realizar este tipo de cambio de tamaño, algunas consultas en ejecución se completan correctamente, pero otras se pueden eliminar como parte de la operación.
  - Cambiar el tipo de nodo de un clúster: al cambiar el tipo de nodo, se crea una instantánea y los datos se redistribuyen del clúster de origen a un clúster compuesto por el nuevo tipo de nodo. Al finalizar, se eliminan las consultas en ejecución. Al igual que en el cambio de tamaño in situ, se completa rápidamente.
- Cambio de tamaño clásico: puede cambiar el tipo de nodo, la cantidad de nodos o ambos de una manera similar al cambio de tamaño elástico. El cambio de tamaño clásico tarda más en completarse, pero puede resultar útil en los casos en que el cambio en el recuento de nodos o el tipo de nodo al que se va a migrar no se encuentre dentro de los límites del cambio de tamaño elástico. Esto se puede aplicar, por ejemplo, cuando el cambio en el recuento de nodos es muy grande.

Temas

- Elastic resize (Cambio de tamaño elástico)
- Classic resize (Cambio de tamaño clásico)

Elastic resize (Cambio de tamaño elástico)

Una operación de cambio de tamaño elástico, al agregar o eliminar nodos del mismo tipo, tiene las siguientes etapas:

1. El cambio de tamaño elástico toma una instantánea del clúster. Esta instantánea siempre incluye tablas sin copia de seguridad para los nodos en los que sea aplicable. (Algunos tipos de nodos, como RA3, no tienen tablas sin copia de seguridad). Si el clúster no tiene una instantánea reciente porque deshabilitó las instantáneas automatizadas, la operación de copia de seguridad puede

tardar más tiempo. (Para minimizar el tiempo antes de que dé comienzo la operación de cambio de tamaño, le recomendamos habilitar las instantáneas automatizadas o crear una instantánea manual antes de comenzar el cambio de tamaño). Cuando comienza un cambio de tamaño elástico y hay una operación de instantánea en curso, el cambio de tamaño puede devolver un error si la operación de instantánea no se completa en unos pocos minutos. Para obtener más información, consulte Instantáneas y copias de seguridad de Amazon Redshift.

2. La operación migra los metadatos del clúster. El clúster no está disponible durante unos minutos. La mayoría de las consultas quedan en pausa temporalmente y las conexiones se mantienen abiertas. Sin embargo, es posible que se eliminen algunas consultas. Esta etapa es breve.
3. Se restablecen las conexiones de la sesión y se reanudan las consultas.
4. El cambio de tamaño elástico redistribuye los datos a los sectores de nodos en segundo plano. El clúster está disponible para operaciones de lectura y escritura, aunque es posible que algunas consultas tarden más tiempo en ejecutarse.
5. Una vez completada la operación, Amazon Redshift envía una notificación de evento.

Cuando utiliza el cambio de tamaño elástico para cambiar el tipo de nodo, funciona de manera similar a cuando agrega o elimina nodos del mismo tipo. En primer lugar, se crea una instantánea. Se aprovisiona un clúster de destino nuevo con los datos más recientes de la instantánea y los datos se transfieren al nuevo clúster en segundo plano. Durante este periodo, los datos son de solo lectura. Cuando el cambio de tamaño está a punto de finalizar, Amazon Redshift actualiza el punto de conexión para que apunte al nuevo clúster y se eliminan todas las conexiones con el clúster de origen.

Es poco probable que se produzca un error en un cambio de tamaño elástico. Sin embargo, en caso de fallo, la reversión se produce automáticamente en la mayoría de los casos sin necesidad de intervención manual.

Si tiene nodos reservados, por ejemplo, nodos reservados DS2, puede actualizarlos a nodos reservados RA3 al realizar un cambio de tamaño. Puede hacer esto cuando efectúa un cambio de tamaño elástico o utiliza la consola para restaurar desde una instantánea. Este tutorial lo guía a través del proceso. Para obtener más información acerca de la actualización a nodos RA3, consulte Actualización a tipos de nodo RA3.

El cambio de tamaño elástico no ordena tablas ni recupera espacio en disco, por lo que no es un sustituto de una operación de limpieza. Para obtener más información, consulte Limpieza de tablas.

El cambio de tamaño elástico tiene las siguientes limitaciones:

- Clústeres de uso compartido de datos y cambio de tamaño elástico: si agrega o quita nodos en un clúster que actúa como productor para el uso compartido de datos, no podrá conectarse a él desde los consumidores mientras Amazon Redshift migre los metadatos del clúster. Del mismo modo, si realiza un cambio de tamaño elástico y elige un nuevo tipo de nodo, el uso compartido de datos no estará disponible mientras las conexiones se descartan y se transfieren al nuevo clúster de destino. En ambos tipos de cambio de tamaño elástico, el productor no está disponible durante varios minutos.
- Transferencia de datos desde una instantánea compartida: para ejecutar un cambio de tamaño elástico en un clúster que está transfiriendo datos desde una instantánea compartida, debe haber al menos una copia de seguridad disponible para el clúster. Puede ver las copias de seguridad en la lista de instantáneas de la consola de Amazon Redshift, el comando `describe-cluster-snapshots` de la CLI o la operación `DescribeClusterSnapshots` de la API.
- Restricción de plataforma: el cambio de tamaño elástico solo está disponible para clústeres que utilizan la plataforma EC2-VPC. Para obtener más información, consulte Usar EC2-VPC al crear el clúster.
- Consideraciones de almacenamiento: asegúrese de que la configuración del nuevo nodo tenga suficiente almacenamiento para los datos existentes. Es posible que deba agregar nodos adicionales o cambiar la configuración.
- Tamaño del clúster de origen frente al de destino: el número de nodos y el tipo de nodo al que es posible cambiar tamaño con el cambio de tamaño elástico viene determinado por el número de nodos del clúster de origen y el tipo de nodo elegido para el clúster con el tamaño cambiado. Para determinar las posibles configuraciones disponibles, puede usar la consola. También puede usar el comando `describe-node-configuration-options` de la AWS CLI con la opción `action-type resize-cluster`. Para obtener más información acerca de cómo cambiar el tamaño mediante la consola de Amazon Redshift, consulte Redimensionamiento de un clúster.

  En el siguiente ejemplo del comando de la CLI, se describen las opciones de configuración disponibles. En este ejemplo, el clúster denominado `mycluster` es un clúster `dc2.large` de 8 nodos.

  ```
  aws redshift describe-node-configuration-options --cluster-identifier mycluster --
  region eu-west-1 --action-type resize-cluster
  ```

  Este comando devuelve una lista de opciones con recomendaciones sobre los tipos de nodos, el número de nodos y el uso de disco de cada opción. Las configuraciones devueltas pueden variar

en función del clúster de entrada específico. Puede elegir una de las configuraciones devueltas cuando especifique las opciones del comando `resize-cluster` de la CLI.

- Límite de nodos adicionales: el cambio de tamaño elástico tiene límites en los nodos que puede agregar a un clúster. Por ejemplo, un clúster dc2 admite el cambio de tamaño elástico hasta duplicar el número de nodos. Para ilustrar, puede agregar un nodo a un clúster dc2.8xlarge de 4 nodos para convertirlo en un clúster de cinco nodos o agregar más nodos hasta que alcance ocho.

> **Note**
>
> Los límites de crecimiento y reducción se basan en el tipo de nodo original y en el número de nodos del clúster original o de su último cambio de tamaño clásico. Si un cambio de tamaño elástico va a superar los límites de crecimiento o reducción, utilice un cambio de tamaño clásico.

Con algunos tipos de nodos ra3, puede aumentar el número de nodos hasta cuatro veces el recuento existente. Específicamente, suponga que su clúster consta de nodos ra3.4xlarge o ra3.16xlarge. Entonces, puede utilizar el cambio de tamaño elástico para aumentar el número de nodos en un clúster de 8 nodos a 32. Otra opción es elegir un valor por debajo del límite. (Tenga en cuenta que la capacidad de aumentar el clúster cuatro veces depende del tamaño del clúster de origen). Si su clúster tiene nodos ra3.xlplus, el límite es doble.

Todos los tipos de nodos ra3 admiten una disminución en el número de nodos a una cuarta parte del recuento existente. Por ejemplo, puede reducir el tamaño de un clúster con nodos ra3.4xlarge de 12 nodos a 3, o a un número por encima del mínimo.

En la siguiente tabla, se enumeran los límites de crecimiento y reducción para cada tipo de nodo que admite el cambio de tamaño elástico.

Tipo de nodo original	Límite de crecimiento	Límite de reducción
ra3.16xlarge	4 veces (de 4 a 16 nodos, por ejemplo)	A una cuarta parte del número (de 16 a 4 nodos, por ejemplo)

Tipo de nodo original	Límite de crecimiento	Límite de reducción
ra3.4xlarge	4 veces	A una cuarta parte del número
ra3.xlplus	2 veces (de 4 a 8 nodos, por ejemplo)	A una cuarta parte del número
dc2.8xlarge	2 veces	A la mitad del número (de 16 a 8 nodos, por ejemplo)
dc2.large	2 veces	A la mitad del número
ds2.8xlarge	2 veces	A la mitad del número
ds2.xlarge	2 veces	A la mitad del número

> **Note**
>
> Elegir tipos de nodos heredados al cambiar el tamaño de un clúster RA3: si intenta cambiar el tamaño de un clúster con nodos RA3 a otro tipo de nodo, como DC2 o DS2, aparecerá un mensaje de advertencia de validación en la consola y la operación de cambio de tamaño no se completará. Esto ocurre porque no se admite cambiar tamaño a tipos de nodos heredados. De este modo, se evita que un cliente cambie de tamaño a un tipo de nodo obsoleto o que pronto lo estará. Esto se aplica al cambio de tamaño elástico y al cambio de tamaño clásico.

Classic resize (Cambio de tamaño clásico)

El cambio de tamaño clásico se encarga de los casos de uso en los que el cambio del tamaño del clúster o el tipo de nodo no se admiten por el cambio de tamaño elástico. Cuando realiza un cambio de tamaño clásico, Amazon Redshift crea un clúster de destino y migra sus datos y metadatos desde el clúster de origen.

El cambio de tamaño clásico a RA3 puede proporcionar una mejor disponibilidad

El cambio de tamaño clásico se ha mejorado cuando el tipo de nodo de destino es RA3. Para ello, utiliza una operación de copia de seguridad y restauración entre el clúster de origen y el de destino.

Cuando comienza el cambio de tamaño, el clúster de origen se reinicia y no está disponible durante unos minutos. Después, el clúster está disponible para operaciones de lectura y escritura mientras el cambio de tamaño continúa en segundo plano.

Verificación del clúster

Para asegurarse de obtener el mejor rendimiento y los mejores resultados cuando realice un cambio de tamaño clásico a un clúster RA3, complete esta lista de comprobación. Si no sigue la lista de verificación, es posible que no obtenga algunos de los beneficios del cambio de tamaño clásico con los nodos RA3, como la capacidad de realizar operaciones de lectura y escritura.

1. El tamaño de los datos debe ser inferior a dos petabytes. (Un petabyte equivale a 1000 terabytes). Para validar el tamaño de los datos, cree una instantánea y compruebe su tamaño. También puede ejecutar la siguiente consulta para comprobar el tamaño:

   ```
   SELECT
   sum(case when lower(diststyle) like ('%key%') then size else 0 end) distkey_blocks,
   sum(size) as total_blocks,
   ((distkey_blocks/(total_blocks*1.00)))*100 as Blocks_need_redist
   FROM svv_table_info;
   ```

   Solo los superusuarios pueden ver la tabla `svv_table_info`.
2. Antes de iniciar un cambio de tamaño clásico, asegúrese de que dispone de una instantánea manual que no tenga más de 10 horas de antigüedad. Si no es así, tome una instantánea.
3. La instantánea utilizada para realizar el cambio de tamaño clásico no puede utilizarse para restaurar una tabla ni para ningún otro fin.
4. El clúster debe estar en una VPC.

Operaciones de clasificación y distribución que se derivan del cambio clásico de tamaño a RA3

Durante el cambio de tamaño clásico a RA3, las tablas con distribución de claves migradas como distribución EVEN se vuelven a convertir a su estilo de distribución original. La duración de este período depende del tamaño de los datos y de lo ocupado que esté el clúster. Las cargas de trabajo de consulta tienen mayor prioridad para ejecutarse que la migración de datos. Para obtener más información, consulte Estilos de distribución. Durante este proceso de migración, en la base de datos funcionan tanto las lecturas como las escrituras, pero las consultas pueden tardar más en completarse. No obstante, el escalado de la simultaneidad puede aumentar el rendimiento durante este tiempo al agregar recursos para las cargas de trabajo de consulta. Puede ver el progreso de la

migración de datos en los resultados de las vistas SYS_RESTORE_STATE y SYS_RESTORE_LOG. A continuación, encontrará más información sobre la monitorización.

Después de cambiar el tamaño del clúster por completo, se produce el siguiente comportamiento de ordenación:

- Si al cambiar el tamaño el clúster tiene más sectores, las tablas de distribución KEY quedan parcialmente sin ordenar, pero las tablas EVEN permanecen ordenadas. Además, es posible que la información sobre la cantidad de datos ordenados no esté actualizada, justo después de cambiar tamaño. Tras la recuperación de la clave, la limpieza automática ordena la tabla a lo largo del tiempo.
- Si al cambiar tamaño el clúster tiene menos sectores, tanto la tabla de distribución KEY como la tabla de distribución EVEN quedan parcialmente sin ordenar. La limpieza automática ordena la tabla a lo largo del tiempo.

Para obtener más información sobre la limpieza automática de tablas, consulte Limpieza de tablas. Para obtener más información sobre los sectores en los nodos de computación, consulte Arquitectura del sistema de almacenamiento de datos.

Pasos clásicos del cambio de tamaño clásico cuando el clúster de destino es RA3

El cambio de tamaño clásico consta de los siguientes pasos, cuando el tipo de clúster de destino es RA3 y se cumplen los requisitos previos detallados en la sección anterior.

1. La migración se inicia del clúster de origen al clúster de destino. Cuando se aprovisiona el nuevo clúster de destino, Amazon Redshift envía una notificación de evento para indicar que comenzó el cambio de tamaño. Reinicia el clúster existente, cerrando así todas las conexiones. Si su clúster existente es un clúster productor de intercambio de datos, las conexiones con los clústeres consumidores también se cierran. El reinicio dura unos minutos.

   Tenga en cuenta que cualquier relación de base de datos, como una tabla o una vista materializada, creada con `BACKUP NO` no se retiene durante el cambio de tamaño clásico. Para obtener más información, consulte CREATE MATERIALIZED VIEW.
2. Tras el reinicio, la base de datos está disponible para lecturas y escrituras. Además, se reanuda el uso compartido de datos, lo que dura unos minutos adicionales.
3. Los datos se migran al clúster de destino. Cuando el tipo de nodo de destino es RA3, las lecturas y escrituras están disponibles durante la migración de datos.

4. Cuando el proceso de cambio de tamaño está a punto de finalizar, Amazon Redshift actualiza el punto de conexión del clúster de destino y se eliminan todas las conexiones al clúster de origen. El clúster de destino se convierte en el productor para el uso compartido de datos.
5. El cambio de tamaño se completa. Amazon Redshift envía una notificación de evento.

Puede ver el progreso del cambio de tamaño en la consola de Amazon Redshift. El tiempo que toma cambiar el tamaño de un clúster depende de la cantidad de datos.

> **Note**
>
> Elegir tipos de nodos heredados al cambiar el tamaño de un clúster RA3: si intenta cambiar el tamaño de un clúster con nodos RA3 a otro tipo de nodo, como DC2 o DS2, aparecerá un mensaje de advertencia de validación en la consola y la operación de cambio de tamaño no se completará. Esto ocurre porque no se admite cambiar tamaño a tipos de nodos heredados. De este modo, se evita que un cliente cambie de tamaño a un tipo de nodo obsoleto o que pronto lo estará. Esto se aplica al cambio de tamaño elástico y al cambio de tamaño clásico.

Supervisión de un cambio de tamaño clásico cuando el clúster de destino es RA3

Para monitorear un cambio de tamaño clásico de un clúster aprovisionado en curso, incluida la distribución de claves, utilice SYS_RESTORE_STATE. Muestra el porcentaje completado de la tabla que se está convirtiendo. Debe ser superusuario para acceder a los datos.

Elimine las tablas que no necesite cuando realice un cambio de tamaño clásico. De este modo, las tablas existentes podrán distribuirse con mayor rapidez.

Pasos de cambio de tamaño clásico cuando el clúster de destino no es RA3

El cambio de tamaño clásico consiste en lo siguiente, cuando el tipo de nodo de destino es cualquier otro que no sea RA3, como DS2, por ejemplo.

1. La migración se inicia del clúster de origen al clúster de destino. Cuando se aprovisiona el nuevo clúster de destino, Amazon Redshift envía una notificación de evento para indicar que comenzó el cambio de tamaño. Reinicia el clúster existente, cerrando así todas las conexiones. Si su clúster existente es un clúster productor de intercambio de datos, las conexiones con los clústeres consumidores también se cierran. El reinicio dura unos minutos.

Tenga en cuenta que cualquier relación de base de datos, como una tabla o una vista materializada, creada con `BACKUP NO` no se retiene durante el cambio de tamaño clásico. Para obtener más información, consulte CREATE MATERIALIZED VIEW.

2. Tras el reinicio, la base de datos estará disponible solo para lectura. Se reanuda el uso compartido de datos, lo que requiere unos minutos adicionales.
3. Los datos se migran al clúster de destino. La base de datos sigue siendo de solo lectura.
4. Cuando el proceso de cambio de tamaño está a punto de finalizar, Amazon Redshift actualiza el punto de conexión del clúster de destino y se eliminan todas las conexiones al clúster de origen. El clúster de destino se convierte en el productor para el uso compartido de datos.
5. El cambio de tamaño se completa. Amazon Redshift envía una notificación de evento.

Puede ver el progreso del cambio de tamaño en la consola de Amazon Redshift. El tiempo que toma cambiar el tamaño de un clúster depende de la cantidad de datos.

> **Note**
>
> El cambio de tamaño de un clúster con una gran cantidad de datos puede durar días o incluso semanas cuando el clúster de destino no es RA3 o no cumple los requisitos previos para un clúster de destino RA3 detallados en la sección anterior.
> Tenga en cuenta también que la capacidad de almacenamiento utilizada para el clúster puede aumentar después de un cambio de tamaño clásico. Este es el comportamiento normal del sistema cuando el clúster tiene sectores de datos adicionales que resultan del cambio de tamaño clásico. Este uso de capacidad adicional puede ocurrir incluso cuando la cantidad de nodos del clúster sigue igual.

Cambio de tamaño elástico frente a cambio de tamaño clásico

En la siguiente tabla, se compara el comportamiento entre los dos tipos de cambio de tamaño.

Cambio de tamaño elástico frente a cambio de tamaño clásico

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentos
Retención de datos del sistema	El cambio de tamaño elástico retiene los datos de registro del sistema.	El cambio de tamaño clásico no retiene las tablas ni los datos del sistema.	Si tiene habilitado el registro de auditoría en el clúster de origen, podrá seguir teniendo acceso a los registros en Amazon S3 o en CloudWatch después de un cambio de tamaño. Puede omitir

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentos
			o eliminar estos registros según lo especifiquen las políticas de datos.

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentarios
Cambios de tipos de nodos	Cambio de tamaño elástico, cuando el tipo de nodo no cambia: cambio de tamaño in situ; se conservan la mayoría de las consultas. Cambio de tamaño elástico, con un nuevo tipo de nodo seleccionado: se crea un clúster nuevo. Se eliminan las consultas cuando se completa el proceso de cambio de tamaño.	Cambio de tamaño clásico: se crea un clúster nuevo. Se eliminan las consultas durante el proceso de cambio de tamaño.	

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentos
Retención de sesiones y consultas	El cambio de tamaño elástico retiene las sesiones y las consultas cuando el tipo de nodo es el mismo en el clúster de origen y de destino. Si elige un nuevo tipo de nodo, las consultas se eliminan.	El cambio de tamaño clásico no retiene las sesiones ni las consultas. Las consultas se eliminan.	Cuando se eliminan las consultas, es posible que haya cierto deterioro en el rendimiento. Es mejor realizar una operación de cambio de tamaño durante un periodo de uso ligero.

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentos
Cancelación de una operación de cambio de tamaño	No se puede cancelar un cambio de tamaño elástico.	Para cancelar una operación de cambio de tamaño clásico antes de que se complete, elija Cancel resize (Cancelar cambio de tamaño) en los detalles del clúster que se muestran en la consola de Amazon Redshift.	La cantidad de tiempo que toma cancelar un cambio de tamaño depende de la fase en que cancela la operación de cambio de tamaño. Cuando lo hace, el clúster no está disponibl

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentarios
			e hasta que se completa la operación de cancelación. Si la operación de cambio de tamaño está en la etapa final, no podrá cancelarla. En el caso de cambio de tamaño clásico

Comportamiento	Elastic resize (Cambio de tamaño elástico)	Classic resize (Cambio de tamaño clásico)	Comentarios
			a un clúster RA3, no se puede cancelar.

Programación de un cambio de tamaño

Puede programar operaciones de cambio de tamaño para que el clúster se pueda escalar verticalmente para anticipar un uso elevado o reducir verticalmente para ahorrar costos. La programación funciona tanto para el cambio de tamaño elástico como para el clásico. Puede configurar una programación en la consola de Amazon Redshift. Para obtener más información, consulte Redimensionamiento de un clúster en Administración de clústeres a través de la consola. También puede utilizar las operaciones de la AWS CLI o de la API de Amazon Redshift para programar un cambio de tamaño. Para obtener más información, consulte create-scheduled-action en la Referencia de comandos de la AWS CLI o CreateScheduledAction en la Referencia de la API de Amazon Redshift.

Instantánea, restauración y cambio de tamaño

El cambio de tamaño elástico es el método más rápido de cambiar el tamaño de un clúster de Amazon Redshift. Si el cambio de tamaño elástico no es una opción y necesita acceso de escritura casi constante al clúster, utilice las operaciones de instantánea y restauración con el cambio de tamaño clásico descritas en la siguiente sección. Este enfoque requiere que cualquier dato que se escriba en el clúster de origen después de que se tomó la instantánea deba copiarse manualmente al clúster de destino después del cambio. Según el tiempo que tome la copia, es posible que deba repetir esto varias veces hasta que obtenga los mismos datos en ambos clústeres. A continuación, puede realizar el cambio al clúster de destino. Este proceso puede tener un impacto negativo en las consultas existentes hasta que el conjunto completo de datos esté disponible en el clúster de destino. No obstante, sí reduce la cantidad de tiempo en el que no puede escribir a la base de datos.

Para el método de instantánea, restauración y cambio de tamaño se utiliza el siguiente proceso:

1. Tome una instantánea del clúster existente. El clúster existente es el de origen.
2. Anote la hora a la que se realizó la instantánea. Esto sirve para que más adelante pueda identificar el punto temporal en el que tendrá que volver a ejecutar los procesos de extracción, transformación y carga (ETL) para cargar cualquier dato posterior a la instantánea en la base de datos de destino.
3. Restaure la instantánea en un clúster nuevo. Este clúster nuevo es el de destino. Compruebe que existan los datos de ejemplo en el clúster de destino.
4. Cambie el tamaño del clúster de destino. Elija el nuevo tipo de nodo, el número de nodos y otras configuraciones para el clúster de destino.
5. Revise las cargas de los procesos ETL que ocurrieron después de que tomó la instantánea del clúster de origen. Asegúrese de volver a cargar los mismos datos en el mismo orden en el clúster de destino. Si tiene cargas de datos en curso, repita este proceso varias veces hasta que los datos sean los mismos en el clúster de origen como en el de destino.
6. Detenga todas las consultas en ejecución en el clúster de origen. Para ello, puede reiniciar el clúster o puede registrarse como superusuario y utilizar los comandos PG_CANCEL_BACKEND y PG_TERMINATE_BACKEND. El reinicio del clúster es la forma más sencilla de asegurar que el clúster no esté disponible.
7. Cambie el clúster de origen. Por ejemplo, cambie el nombre de `examplecluster` a `examplecluster-source`.
8. Cambie el nombre del clúster de destino para utilizar el nombre del clúster de origen antes del cambio de nombre. Por ejemplo, cambie el nombre del clúster de destino anterior a `examplecluster`. A partir de este punto, cualquier aplicación que utilice el punto de conexión que contiene `examplecluster` se conecta al clúster de destino.
9. Elimine el clúster de origen después de cambiar al clúster de destino y compruebe que todos los procesos funcionen según lo previsto.

También puede cambiar el nombre de los clústeres de origen y de destino antes de volver a cargar los datos en el clúster de destino. Este enfoque funciona si no requiere que los sistemas e informes dependientes estén inmediatamente actualizados con los del clúster de destino. En este caso, el paso 6 se mueve al final del proceso descrito anteriormente.

El proceso de cambio de nombre solo se requiere si desea que las aplicaciones sigan utilizando el mismo punto de conexión para conectarse al clúster. Si no necesita esto, en su lugar puede actualizar cualquier aplicación que se conecte al clúster para utilizar el punto de conexión del clúster de destino sin cambiar el nombre del clúster.

Existen algunos beneficios en reutilizar el nombre de un clúster. Primero, no necesita actualizar las cadenas de conexión de aplicaciones ya que el punto de conexión no cambia, aunque cambia el clúster subyacente. En segundo lugar, los elementos relacionados, como las alarmas de Amazon CloudWatch y las notificaciones de Amazon Simple Notification Service (Amazon SNS), están asociados al nombre del clúster. Esta asociación significa que puede seguir utilizando las mismas alarmas y notificaciones que configuró para el clúster. Este uso continuo es principalmente un problema en los entornos de producción, donde se desea tener la flexibilidad para cambiar el tamaño del clúster sin tener que volver a configurar los elementos relacionados, como alarmas y notificaciones.

Pausa y reanudación de clústeres

Si tiene un clúster que solo tiene que estar disponible en momentos específicos, puede pausar el clúster y reanudarlo posteriormente. Mientras el clúster está en pausa, la facturación bajo demanda se suspende. Solo el almacenamiento del clúster incurre en cargos. Para obtener más información acerca de los precios, consulte la página de precios de Amazon Redshift.

Cuando pausa un clúster, Amazon Redshift crea una instantánea, comienza a terminar consultas y pone el clúster en estado de pausa. Si elimina un clúster en pausa sin solicitar una instantánea final, no podrá restaurar el clúster. No puede cancelar o deshacer una pausa o reanudar una operación después de que se haya iniciado.

Puede pausar y reanudar un clúster en la consola de Amazon Redshift con AWS CLI o con operaciones de la API de Amazon Redshift.

Puede programar acciones para pausar y reanudar un clúster. Cuando utiliza la nueva consola de Amazon Redshift para crear una programación periódica para pausar y reanudar, se crean dos acciones programadas para el intervalo de fechas que elija. Los nombres de las acciones programadas tienen el sufijo `-pause` y `-resume`. La longitud total del nombre debe ajustarse al tamaño máximo de un nombre de acción programada.

No puede pausar los siguientes tipos de clústeres:

- Clústeres clásicos de EC2.
- Clústeres que no están activos, por ejemplo, un clúster que se está modificando actualmente.
- Clústeres de módulo de seguridad de hardware (HSM)
- Clústeres que tienen instantáneas automatizadas desactivadas.

Cuando decida pausar un clúster, tenga en cuenta lo siguiente:

- Las conexiones o consultas al clúster no están disponibles.
- No puede ver la información de supervisión de consultas de un clúster pausado en la consola de Amazon Redshift.
- No se puede modificar un clúster en pausa. Las acciones programadas en el clúster no se realizan. Estas incluyen la creación de instantáneas, el cambio de tamaño de los clústeres y las operaciones de mantenimiento de clústeres.
- Las métricas de hardware no se crean. Actualice sus alarmas de CloudWatch si tiene alarmas establecidas en las métricas que faltan.
- No puede copiar las instantáneas automatizadas más recientes de un clúster en pausa en instantáneas manuales.
- Mientras un clúster está en pausa, no se puede reanudar hasta que se complete la operación de pausa.
- Cuando pausa un clúster, la facturación se suspende. No obstante, la operación de pausa normalmente se completa en 15 minutos, en función del tamaño del clúster.
- Los registros de auditoría se archivan y no se restauran al reanudar.
- Después de pausar un clúster, es posible que los seguimientos y los registros no estén disponibles para solucionar los problemas que se produjeron antes de la pausa.
- Las tablas sin copia de seguridad del clúster no se restauran al reanudar. Para obtener más información acerca de las tablas sin copia de seguridad, consulte Exclusión de tablas de instantáneas.
- Si administra sus credenciales de administrador con AWS Secrets Manager y pausa su clúster, el secreto del clúster no se eliminará y se le seguirá cobrando por el secreto. Para obtener más información sobre cómo administrar su contraseña de administrador de Redshift con AWS Secrets Manager, consulte Administración de las contraseñas de administrador de Amazon Redshift mediante AWS Secrets Manager.

Cuando reanude un clúster, tenga en cuenta lo siguiente:

- La versión del clúster reanudado se actualiza a la versión de mantenimiento en función de la ventana de mantenimiento del clúster.
- Si elimina la subred asociada a un clúster en pausa, es posible que tenga una red incompatible. En este caso, restaure el clúster a partir de la última instantánea.

- Si elimina una dirección IP elástica mientras el clúster está en pausa, se solicita una nueva dirección IP elástica.
- Si Amazon Redshift no puede reanudar el clúster con su interfaz de red elástica anterior, Amazon Redshift intenta asignar una nueva.
- Cuando se reanuda un clúster, las direcciones IP de los nodos pueden cambiar. Es posible que tenga que actualizar la configuración de la VPC para admitir estas nuevas direcciones IP para características como COPY desde Secure Shell (SSH) o COPY desde Amazon EMR.
- Si intenta reanudar un clúster que no está en pausa, la operación de reanudación devuelve un error. Si la operación de reanudación forma parte de una acción programada, modifique o elimine la acción programada para evitar errores futuros.
- En función del tamaño del clúster, puede tardar varios minutos en reanudar un clúster antes de que se puedan procesar las consultas. Además, el rendimiento de la consulta puede verse afectado durante algún periodo de tiempo mientras el clúster se vuelve a hidratar después de que se complete la reanudación.

Cambio de nombre de los clústeres

Puede cambiar el nombre de un clúster si desea que el clúster utilice un nombre diferente. Como el punto de conexión del clúster incluye el nombre del clúster (lo que también se conoce como identificador del clúster), el punto de conexión cambia y pasa a utilizar el nombre nuevo una vez que termina el cambio de nombre. Por ejemplo, si tiene un clúster denominado `examplecluster` y le cambia el nombre por `newcluster`, el punto de conexión pasa a utilizar el identificador `newcluster`. Se debe actualizar cualquier aplicación que se conecte al clúster con el nuevo punto de conexión.

Puede cambiar el nombre de un clúster si desea cambiar el clúster con el que se conectan sus aplicaciones sin tener que cambiar el punto de conexión en esas aplicaciones. En este caso, primero debe cambiar el nombre del clúster original y, luego, cambiar el del segundo clúster para volver a utilizar el nombre del clúster original antes del cambio. Es necesario hacer esto porque el identificador de clúster debe ser único dentro de su cuenta y región, por lo que el clúster original y el segundo clúster no pueden tener el mismo nombre. Si no desea cambiar las propiedades de conexión de ninguna de las aplicaciones dependientes, puede hacerlo restaurando el clúster desde una instantánea.

> **Note**
>
> Si elimina el clúster original, tendrá que eliminar todas las snapshots no deseadas del clúster.

Cuando cambia el nombre de un clúster, el estado del clúster cambia a `renaming` hasta que termina el proceso. El nombre del DNS anterior que utilizaba el clúster se elimina de inmediato, si bien puede quedar almacenado en caché por varios minutos. El nuevo nombre del DNS del clúster que fue renombrado se efectiviza, aproximadamente, a los 10 minutos. El clúster renombrado estará disponible una vez que se efectiviza el nombre nuevo. Se reiniciará el clúster y se perderá cualquier conexión establecida con el clúster. Después que se completa el proceso, el punto de conexión pasará a utilizar el nombre nuevo. Por este motivo, debe detener la ejecución de consultas antes de comenzar con el cambio de nombre y las debe reiniciar una vez que termina con el cambio.

Las snapshots del clúster quedan almacenadas y todas las snapshots asociadas con el clúster quedan asociadas con ese clúster después de que se le cambia el nombre. Por ejemplo, suponga que tiene un clúster que sirve a su base de datos de producción y que ese clúster tiene varias instantáneas. Si cambia el nombre del clúster y, a continuación, lo reemplaza en el entorno de producción por una instantánea, el clúster que renombró sigue teniendo esas instantáneas asociadas a él.

Las alarmas de Amazon CloudWatch y las notificaciones de eventos de Amazon Simple Notification Service (Amazon SNS) están asociadas al nombre del clúster. Si cambia el nombre del clúster, debe actualizar estos otros elementos asociados como corresponda. Puede actualizar las alarmas de CloudWatch en la consola de CloudWatch y puede actualizar las notificaciones de eventos de Amazon SNS en la consola de Amazon Redshift en el panel Events (Eventos). La carga y los datos de consulta del clúster muestran los datos antes y después del cambio de nombre. No obstante, los datos de rendimiento se reinician una vez que termina el proceso de cambio de nombre.

Para obtener más información, consulte Modificación de un clúster.

Cierre y eliminación de clústeres

Puede cerrar su clúster sin desea que deje de funcionar y generar cargos. Cuando lo cierra, puede crear una snapshot final. Si crea una instantánea final, Amazon Redshift creará una instantánea manual de su clúster antes de cerrarlo. Luego, puede restaurar la snapshot si desea reanudar la ejecución del clúster y la consulta de datos.

Si ya no necesita su clúster ni los datos de este, puede cerrarlo sin crear una snapshot final. En este caso, el clúster y los datos se eliminan de manera permanente. Para obtener más información acerca del cierre y la eliminación de clústeres, consulte Eliminación de un clúster.

Independientemente de que cierre su clúster con una snapshot manual final o no, todas las snapshots automatizadas asociadas con el clúster se eliminarán después de que se cierre el clúster. Se conservará toda snapshot manual asociada con el clúster. Cualquier instantánea manual que se retenga, incluida la instantánea final opcional, se cobrará con la tarifa de almacenamiento de Amazon Simple Storage Service si no hay ningún otro clúster en ejecución en el momento en que se cierre el clúster o si se supera la capacidad de almacenamiento gratuito disponible que se proporciona para ejecutar los clústeres de Amazon Redshift. Para obtener más información acerca de los cargos de almacenamiento de las instantáneas, consulte la página de precios de Amazon Redshift.

Al eliminar un clúster, también se eliminan todos los secretos de AWS Secrets Manager asociados.

Reubicación del clúster

Mediante el uso de la reubicación en Amazon Redshift, se permite que Amazon Redshift mueva un clúster a otra zona de disponibilidad (AZ) sin pérdida de datos ni cambios en las aplicaciones. Con la reubicación, puede continuar las operaciones cuando hay una interrupción del servicio en el clúster con un impacto mínimo.

Cuando la reubicación de clústeres está activada, Amazon Redshift puede elegir reubicar clústeres en algunas situaciones. En particular, esto sucede cuando los problemas de la zona de disponibilidad actual impiden la operación óptima del clúster o para mejorar la disponibilidad del servicio. También puede invocar la función de reubicación en los casos en que las restricciones de recursos en una zona de disponibilidad determinada interrumpan las operaciones del clúster. Un ejemplo es la capacidad de reanudar o cambiar el tamaño de un clúster. Amazon Redshift ofrece la característica de reubicación sin cargo adicional.

Cuando un clúster de Amazon Redshift se reubica en una nueva zona de disponibilidad, el nuevo clúster tiene el mismo punto de enlace que el clúster original. Sus aplicaciones pueden volver a conectarse al punto de enlace y continuar las operaciones sin modificaciones ni pérdida de datos. Sin embargo, es posible que la reubicación no siempre sea posible debido a posibles restricciones de recursos en una zona de disponibilidad determinada.

La reubicación de clústeres de Amazon Redshift solo se admite para los tipos de instancias RA3, como ra3.16xlarge, ra3.4xlarge y ra3.xlplus. Los tipos de instancias RA3 utilizan Redshift Managed Storage (RMS) como capa de almacenamiento duradera. La copia más reciente de los datos de un

clúster siempre está disponible en otras zonas de disponibilidad de una región de AWS. En otras palabras, puede reubicar un clúster de Amazon Redshift a otra zona de disponibilidad sin pérdida de datos.

Cuando activa la reubicación de su clúster, Amazon Redshift lo migra para que esté detrás de un proxy. Esto ayuda a implementar el acceso independiente de la ubicación a los recursos de cómputo de un clúster. La migración hace que se reinicie el clúster. Cuando un clúster se reubica en otra zona de disponibilidad, se produce una interrupción mientras el nuevo clúster vuelve a estar online en la nueva zona de disponibilidad. Sin embargo, no es necesario realizar ningún cambio en las aplicaciones porque el punto de enlace del clúster permanece sin cambios incluso después de que el clúster se reubica en la nueva zona de disponibilidad.

La reubicación de clústeres está desactivada de forma predeterminada en todos los clústeres RA3. Amazon Redshift asigna 5439 como puerto predeterminado al crear un clúster aprovisionado. Puede cambiar a otro puerto del intervalo de puertos 5431-5455 u 8191-8215. (No cambie a un puerto fuera de dichos internvalos pues se genera un error). Para cambiar el puerto predeterminado de un clúster aprovisionado, utilice la consola de Amazon Redshift, la AWS CLI o la API de Amazon Redshift. Para cambiar el puerto predeterminado de un grupo de trabajo sin servidor, utilice la AWS CLI o la API de Amazon Redshift sin servidor.

Si activa la reubicación y utiliza actualmente la dirección IP del nodo principal para acceder al clúster, asegúrese de cambiar ese acceso. En su lugar, utilice la dirección IP asociada al punto de enlace de la nube virtual privada (VPC) del clúster. Para buscar esta dirección IP del clúster, busque y utilice el punto de enlace de la VPC en la sección Network and security (Red y seguridad) de la página de detalles del clúster. Para obtener más detalles acerca del punto de enlace de la VPC, inicie sesión en la consola de Amazon VPC.

También puede recurrir a la AWS Command Line Interface (AWS CLI) a fin de utilizar el comando `describe-vpc-endpoints` para obtener la interfaz de red elástica asociada al punto de enlace. Puede utilizar el comando `describe-network-interfaces` para obtener la dirección IP asociada. Para obtener más información acerca de los comandos de la AWS CLI de Amazon Redshift, consulte Comandos disponibles en la Referencia de los comandos de la AWS CLI.

> **Note**
>
> Como recordatorio, la reubicación del clúster no es un requisito previo para configurar características de red de Redshift adicionales, como las que se utilizan para la recuperación de desastres u otros fines. Por ejemplo, puede complementarlo con la copia de instantáneas

entre regiones para proporcionar más resiliencia a su entorno, pero no es obligatorio. Tampoco es necesario que lo active para habilitar las siguientes características:

- Conexión desde una VPC con varias cuentas o regiones a Redshift: puede conectarse desde una nube privada virtual (VPC) de AWS a otra que contenga una base de datos de Redshift. Esto facilita la administración, por ejemplo, del acceso de los clientes desde cuentas o VPC dispares, sin que sea necesario proporcionar acceso de VPC local a las identidades que se conectan a la base de datos. Para obtener más información, consulte Conexión a Amazon Redshift sin servidor desde un punto de conexión de VPC de Redshift en otra cuenta o región.
- Configuración de un nombre de dominio personalizado: puede crear un nombre de dominio personalizado, también conocido como URL personalizada, para su clúster de Amazon Redshift o grupo de trabajo de Amazon Redshift sin servidor, a fin de que el nombre del punto de conexión sea sencillo y más fácil de recordar. Para obtener más información, consulte Uso de un nombre de dominio personalizado para las conexiones de cliente.

Limitaciones

Cuando utilice la reubicación de Amazon Redshift, tenga en cuenta las siguientes limitaciones:

- Es posible que la reubicación de clústeres no sea posible en todos los escenarios debido a posibles limitaciones de recursos en una zona de disponibilidad determinada. Si esto sucede, Amazon Redshift no cambia el clúster original.
- La reubicación no es compatible con las familias de productos de instancias DC1, DC2 o DS2.
- No se puede realizar una reubicación entre regiones de AWS.
- La reubicación de Amazon Redshift se establece de forma predeterminada en el número de puerto 5439. También puede cambiar a otro puerto del intervalo de puertos 5431 a 5455 u 8191 a 8215.
- La reubicación está disponible en las siguientes regiones:
  - Región Este de EE. UU. (Ohio) (us-east-2)
  - Región Este de EE. UU. (Norte de Virginia) (us-east-1)
  - Región EE. UU. Oeste (Norte de California) (us-west-1)
  - Región EE. UU. Oeste (Oregón) (us-west-2)
  - Región Asia Pacífico (Melbourne) (ap-southeast-4)

- Región Asia-Pacífico (Mumbai) (ap-south-1)
- Región Asia-Pacífico (Seúl) (ap-northeast-2)
- Región Asia-Pacífico (Singapur) (ap-southeast-1)
- Región Asia-Pacífico (Sídney) (ap-southeast-2)
- Región Asia-Pacífico (Tokio) (ap-northeast-1)
- Región Canadá (Central) (ca-central-1)
- Región Oeste de Canadá (Calgary) (ca-west-1)
- Región Europa (Fráncfort) (eu-central-1)
- Región Europa (Irlanda) (eu-west-1)
- Región Europa (Londres) (eu-west-2)
- Región Europa (París) (eu-west-3)
- Región Europa (Estocolmo) (eu-north-1)
- Región de Israel (Tel Aviv) (il-central-1)
- Región América del Sur (São Paulo) (sa-east-1)

Activación de la reubicación de clústeres

Puede activar y administrar la reubicación de clústeres desde la consola de Amazon Redshift, la AWS CLI y la API de Amazon Redshift.

Para activar la reubicación de clústeres, defina un grupo de subredes que incluya varias zonas de disponibilidad. Si Amazon Redshift identifica más de una zona de disponibilidad accesible, Amazon Redshift elige automáticamente de la lista de zonas de disponibilidad accesibles para reubicar el clúster.

Una vez completada la reubicación, se utiliza el mismo punto de enlace para acceder al clúster. Amazon Redshift elimina los recursos de cómputo del clúster original y los devuelve al grupo de recursos.

Administración de la reubicación mediante la consola

Puede administrar la configuración de la reubicación de clústeres mediante la consola de Amazon Redshift.

Activación de la reubicación al crear un nuevo clúster

Utilice el siguiente procedimiento para activar la reubicación cuando cree un nuevo clúster.

Para activar la reubicación de un nuevo clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Elija Create cluster (Crear clúster) para crear un nuevo clúster. Para obtener más información sobre cómo crear un clúster, consulte Crear un clúster de Amazon Redshift de muestra en la Guía de introducción a Amazon Redshift.
4. En Backup (Copia de seguridad), para Cluster relocation (Reubicación del clúster), elija Enabled (Habilitado). De forma predeterminada, la reubicación está desactivada.
5. Elija Create cluster.

Modificación de la reubicación de un clúster existente

Utilice el siguiente procedimiento para cambiar la configuración de reubicación de un clúster existente.

Para modificar la configuración de reubicación de un clúster existente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el nombre del clúster que desea modificar de la lista. Se abrirá la página de detalles del clúster.
4. Elija la pestaña Maintenance (Mantenimiento) y, a continuación, en la sección Backup details (Detalles de copia de seguridad), elija Edit (Editar).
5. En Backup (Copia de seguridad), elija Enabled (Habilitado). De forma predeterminada, la reubicación está desactivada.
6. Elija Modify Cluster (Modificar clúster).

Reubicación de un clúster

Utilice el siguiente procedimiento para reubicar manualmente un clúster en otra zona de disponibilidad. Esto resulta especialmente útil cuando desea probar la configuración de red en zonas de disponibilidad secundarias o cuando se encuentra con restricciones de recursos en la zona de disponibilidad actual.

Para reubicar un clúster en otra zona de disponibilidad

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el nombre del clúster que desea mover de la lista. Se abrirá la página de detalles del clúster.
4. En Actions (Acciones), elija Relocate (Reubicar). Se abrirá la página Relocate cluster (Reubicar clúster).
5. (Opcional) Elija una Availability Zone (Zona de disponibilidad). Si no elige una zona de disponibilidad, Amazon Redshift elige una para usted.

Amazon Redshift comienza la reubicación y muestra el clúster como en estado de reubicación. Una vez finalizada la reubicación, el estado del clúster cambia a disponible.

Administración de la reubicación mediante la CLI de Amazon Redshift

Puede administrar la configuración de la reubicación de clústeres mediante la AWS Command Line Interface (CLI).

Con la AWS CLI, el siguiente comando de ejemplo crea un clúster de Amazon Redshift denominado **`mycluster`** que tiene activada la reubicación.

```
aws redshift create-cluster --cluster-identifier mycluster --number-of-nodes 2 --
master-username enter a username --master-user-password enter a password --node-type
 ra3.4xlarge --port 5439 --availability-zone-relocation
```

Si el clúster actual utiliza un puerto diferente, debe modificarlo para que use el rango de puerto 5431-5455 o 8191-8215 antes de modificarlo para activar la reubicación. El valor predeterminado

es 5439. El siguiente comando de ejemplo modifica el puerto en caso de que el clúster no use uno de los intervalos dados.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

El siguiente comando de ejemplo incluye el parámetro availability-zone-relocation en el clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone-
relocation
```

El siguiente comando de ejemplo desactiva el parámetro availability-zone-relocation en el clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --no-availability-zone-
relocation
```

El siguiente comando de ejemplo invoca la reubicación en el clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone us-
east-1b
```

Instantáneas y copias de seguridad de Amazon Redshift

Temas

- Información general de las instantáneas
- Instantáneas automatizadas
- Programación de instantáneas automatizadas
- Formato de la programación de instantáneas
- Instantáneas manuales
- Administración del almacenamiento de instantáneas
- Exclusión de tablas de instantáneas
- Copia de instantáneas a otra región de AWS
- Restauración de un clúster desde una instantánea
- Restauración de una tabla a partir de una instantánea
- Uso compartido de instantáneas

- Administración de instantáneas mediante la consola
- Administración de instantáneas mediante la AWS CLI y la API de Amazon Redshift
- Uso de AWS Backup

Información general de las instantáneas

Las snapshots son backups de un momento determinado de un clúster. Existen dos tipos de instantáneas: automatizadas y manuales. Amazon Redshift almacena estas instantáneas internamente en Amazon S3 con una conexión de capa de conexión segura (SSL) cifrada.

Amazon Redshift realiza instantáneas progresivas de forma automática que hacen un seguimiento de los cambios realizados en el clúster desde la instantánea automatizada anterior. Las instantáneas automatizadas conservan todos los datos requeridos para restaurar un clúster a partir de una instantánea. Puede crear una programación de instantáneas para controlar cuándo se realizan las instantáneas automatizadas o realizar una instantánea manual en cualquier momento.

Cuando restaura datos a partir de una instantánea, Amazon Redshift crea un clúster nuevo y lo pone a disposición antes de que se carguen todos los datos, de modo que usted pueda empezar a consultar el clúster nuevo de inmediato. El clúster transmite datos bajo demanda desde la instantánea en respuesta a consultas activas, luego carga los datos restantes en un segundo plano.

Al lanzar un clúster, puede establecer el periodo de retención para las instantáneas automatizadas y manuales. Puede cambiar el periodo de retención predeterminado para las instantáneas automatizadas y manuales mediante la modificación del clúster. Puede cambiar el periodo de retención para una instantánea manual en el momento de crear la instantánea o modificando la instantánea.

Puede monitorizar el progreso de las instantáneas consultando los detalles de la propia instantánea en la AWS Management Console o llamando a describe-cluster-snapshots en la CLI o a la acción de API DescribeClusterSnapshots. Para una instantánea en proceso, estos muestran información como el tamaño de la instantánea incremental, la tasa de transferencia, el tiempo transcurrido y el tiempo restante estimado.

Para asegurarse de que las copias de seguridad estén siempre disponibles para el clúster, Amazon Redshift almacena instantáneas en un bucket de Amazon S3 administrado internamente que administra Amazon Redshift. Para administrar los cargos de almacenamiento, evalúe cuántos días necesita conservar las instantáneas automatizadas y configure el periodo de retención en consecuencia. Elimine las instantáneas manuales que ya no necesita. Para obtener más información

acerca del costo del almacenamiento de copias de seguridad, consulte la página Precios de Amazon Redshift.

Uso de instantáneas y copias de seguridad en Amazon Redshift sin servidor

Amazon Redshift sin servidor, al igual que un clúster aprovisionado, le permite realizar una copia de seguridad como una representación en un momento dado de los objetos y datos del espacio de nombres. Hay dos tipos de copias de seguridad en Amazon Redshift sin servidor: las instantáneas que se crean manualmente y los puntos de recuperación que Amazon Redshift sin servidor crea automáticamente. Puede encontrar más información sobre el uso de instantáneas para Amazon Redshift sin servidor en Trabajo con instantáneas y puntos de recuperación.

También puede restaurar una instantánea de un clúster aprovisionado a un espacio de nombres sin servidor. Para obtener más información, consulte Restauración de un espacio de nombres sin servidor desde una instantánea.

Instantáneas automatizadas

Cuando las instantáneas automatizadas están habilitadas para un clúster, Amazon Redshift realiza instantáneas de ese clúster periódicamente. De manera predeterminada, Amazon Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero. Si sus datos superan los 5 GB * número de nodos, el periodo de tiempo más breve entre la creación automática de instantáneas es de 15 minutos. También puede crear una programación de instantáneas para controlar cuándo se realizan las instantáneas automatizadas. Si utiliza programaciones personalizadas, el tiempo mínimo entre las instantáneas automatizadas es de una hora. Las instantáneas automatizadas se habilitan de manera predeterminada cuando crea un clúster.

Las instantáneas automatizadas se eliminan cuando finaliza un periodo de retención. El periodo de retención predeterminado es de un día, pero puede modificarlo a través de la consola de Amazon Redshift o mediante programación con la API o la CLI de Amazon Redshift.

Para desactivar las instantáneas automatizadas, establezca el período de retención en cero. Si desactiva las instantáneas automatizadas, Amazon Redshift deja de tomar instantáneas y elimina cualquier instantánea automatizada ya existente para el clúster. No puede deshabilitar las instantáneas automatizadas para los tipos de nodos RA3. Puede establecer un periodo de retención automatizado para el tipo de nodo RA3 de 1 a 35 días.

Solo Amazon Redshift puede eliminar una instantánea automatizada; por lo que no se pueden eliminar de forma manual. Amazon Redshift elimina las instantáneas automatizadas al final del

periodo de retención de la instantánea, cuando usted desactiva las instantáneas automatizadas para el clúster o cuando elimina el clúster. Amazon Redshift retiene la última instantánea automatizada hasta que usted desactiva las instantáneas automatizadas o elimina el clúster.

Si desea conservar una instantánea automatizada por un período más extenso, puede crear una copia de esta como una instantánea manual. La instantánea automatizada se conserva hasta que expire el periodo de retención, pero la instantánea manual correspondiente se conservará hasta que el usuario la elimine manualmente o hasta el final del periodo de retención.

Programación de instantáneas automatizadas

Para controlar con precisión cuándo se realizan las instantáneas, puede crear una programación de instantáneas y asociarla a uno o varios clústeres. Cuando modifica una programación de instantáneas, esta se modifica para todos los clústeres asociados. Si un clúster no tiene una programación de instantáneas asociada, utiliza la programación de instantáneas automatizadas predeterminada.

Una programación de instantáneas es un conjunto de reglas de programación. Puede definir una regla de programación sencilla basada en un intervalo específico, como cada 8 horas o cada 12 horas. También puede añadir reglas para realizar instantáneas determinados días de la semana, a horas específicas o durante periodos específicos. Las reglas se pueden definir también con expresiones cron de tipo Linux.

Formato de la programación de instantáneas

En la consola de Amazon Redshift, puede crear una programación de instantáneas. A continuación, puede asociar una programación a un clúster para activar la creación de una instantánea del sistema. Una programación se puede asociar con varios clústeres y se pueden crear varias definiciones cron en una programación para activar una instantánea.

Puede definir una programación para sus instantáneas con la sintaxis cron. La definición de estas programaciones utiliza una sintaxis cron similar a Unix modificada. La hora debe especificarse de acuerdo con el Tiempo universal coordinado (UTC). Puede crear programaciones con una frecuencia máxima de una hora y una precisión mínima de un minuto.

Las expresiones cron modificadas de Amazon Redshift tienen 3 campos obligatorios, que están separados por un espacio en blanco.

Sintaxis

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

Campos	Valores	Caracteres comodín
Minutos	0–59	, - * /
Horas	0–23	, - * /
Día del mes	1–31	, - * ? / L W
Mes	1–12 o ENE-DIC	, - * /
Día de la semana	1–7 o DOM-SÁB	, - * ? L #
Año	1970-2199	, - * /

Caracteres comodín

- El carácter comodín , (coma) incluye valores adicionales. En el campo `Day-of-week`, `MON,WED,FRI` incluiría lunes, miércoles y viernes. El total de valores está limitado a 24 por campo.
- El carácter comodín - (guion) especifica los intervalos. En el campo `Hour`, 1–15 incluiría desde la 1 hasta las 15 horas del día especificado.
- El * (asterisco) incluye todos los valores del campo. En el campo `Hours`, * incluiría cada hora.
- El comodín / (barra inclinada) especifica incrementos. En el campo `Hours`, puede escribir **`1/10`** para especificar cada 10 horas, empezando por la primera hora del día (por ejemplo, 01:00, 11:00 y 21:00).
- El comodín ? (signo de interrogación) especifica uno u otro. En el campo `Day-of-month` puede escribir 7 y si no le importa qué día de la semana era el séptimo, podría escribir ? en el campo Day-of-week.
- El comodín L en los campos `Day-of-month` o `Day-of-week` especifica el último día del mes o de la semana.
- El comodín W en el campo `Day-of-month` especifica un día de la semana. En el campo `Day-of-month`, `3W` especifica el día más cercano al tercer día de semana del mes.
- El comodín # en el campo Día de la semana especifica una instancia concreta del día de la semana de un mes. Por ejemplo, 3#2 sería el segundo martes del mes: el número 3 hace

referencia al martes, ya que es el tercer día de la semana en el calendario anglosajón, mientras que 2 hace referencia al segundo día de ese tipo dentro de un mes.

> **Note**
>
> Si utiliza un carácter '#', solo puede definir una expresión en el campo Día de la semana. Por ejemplo, “3#1,6#3” no es válido porque se interpreta como dos expresiones.

Límites

- No se pueden especificar los campos `Day-of-month` y `Day-of-week` en la misma expresión Cron. Si especifica un valor en uno de los campos, debe utilizar un ? (signo de interrogación) en el otro.
- Las programaciones de instantáneas no admiten las siguientes frecuencias:
  - Instantáneas programadas con una frecuencia superior a una por hora.
  - Instantáneas programadas con una frecuencia inferior a una por día (24 horas).

  Si tiene programaciones solapadas que programan instantáneas en un periodo de una hora, se produce un error de validación.

Cuando cree una programación, puede utilizar las siguientes cadenas Cron de ejemplo.

Minutos	Horas	Día de la semana	Significado			
0	14-20/1	TUE	Cada hora entre las dos y las ocho de la tarde del martes.			
0	21	MON-FRI	Todas las noches a las 21 h de lunes a viernes.			
30	0/6	SAT-SUN	Cada seis horas el sábado y el domingo empezando 30			

Minutos	Horas	Día de la semana	Significado			
			minutos después de la medianoche (00:30) de ese día. Esto produce una instantánea a las [00:30, 06:30, 12:30 y 18:30] todos los días.			
30	12/4	*	Cada cuatro horas a partir de las 12:30 todos los días. Esto se resuelve en [12:30, 16:30, 20:30].			

Por ejemplo, para ejecutar una programación diaria cada dos horas empezando a las 15:15 (lo que se resuelve en [15:15, 17:15, 19:15, 21:15, 23:15]), especifique:

```
cron(15 15/2 *)
```

Puede crear varias definiciones de programación cron en una programación. Por ejemplo, el siguiente comando de la AWS CLI contiene dos programaciones cron en una sola programación.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0
 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

Instantáneas manuales

También puede tomar una instantánea manual en cualquier momento. De manera predeterminada, las instantáneas manuales se conservarán de forma indefinida incluso después de que elimine el clúster. Puede especificar el periodo de retención en el momento de crear una instantánea manual o puede cambiar el periodo de retención modificando la instantánea. Para obtener más información acerca de cómo cambiar el periodo de retención, consulte Cambiar el periodo de retención de instantáneas manuales.

Si se elimina una instantánea, no puede comenzar ninguna operación nueva que haga referencia a esa instantánea. Sin embargo, si hay una operación de restauración en proceso, esta se ejecutará hasta su finalización.

Amazon Redshift tiene una cuota que limita el número total de instantáneas manuales que puede crear. Esta cuota se aplica por cuenta de AWS y por región de AWS. La cuota predeterminada se muestra en Cuotas y límites de Amazon Redshift.

Administración del almacenamiento de instantáneas

Dado que las instantáneas acumulan gastos de almacenamiento, es importante que las elimine cuando ya no las necesite. Amazon Redshift elimina las instantáneas automatizadas y manuales al final de sus respectivos periodos de retención. También puede eliminar las instantáneas manuales mediante la AWS Management Console o con el comando de la CLI batch-delete-cluster-snapshots.

Puede cambiar el periodo de retención para una instantánea manual modificando la configuración de la instantánea manual.

Para obtener información sobre la cantidad de almacenamiento que consumen las instantáneas, utilice la consola de Amazon Redshift o el comando de la CLI describe-storage.

Exclusión de tablas de instantáneas

De manera predeterminada, todas las tablas permanentes definidas por el usuario se incluyen en las instantáneas. Si no es necesario crear un backup para una tabla, como una tabla provisional, puede reducir de forma significativa el tiempo necesario para crear instantáneas y restaurar a partir de instantáneas. También se reduce el espacio de almacenamiento en Amazon S3 mediante el uso de una tabla sin backup. Para crear una tabla sin backup, incluya el parámetro BACKUP NO cuando cree la tabla. Para obtener más información, consulte CREATE TABLE y CREATE TABLE AS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Copia de instantáneas a otra región de AWS

Puede configurar Amazon Redshift para que copie de forma automática las instantáneas (automatizadas o manuales) de un clúster en otra región de AWS. Cuando se crea una instantánea en una región principal de AWS de un clúster, se copia en una región secundaria de AWS. Las dos regiones de AWS se denominan, respectivamente, región de AWS de origen y región de AWS de destino. Si almacena una copia de las instantáneas en otra región de AWS, podrá restaurar el clúster a partir de datos recientes si algo afecta a la región principal de AWS. Puede configurar el clúster

para que copie las instantáneas solo en una región de AWS de destino a la vez. Para obtener una lista de las regiones de Amazon Redshift, consulte Regiones y puntos de conexión en la Referencia general de Amazon Web Services.

Si habilita a Amazon Redshift para que copie instantáneas en otra región de AWS de forma automática, especifique la región de AWS de destino en la que desea que se copien. En el caso de las instantáneas automatizadas, también puede especificar el periodo de retención durante el cual deben conservarse en la región de AWS de destino. Cuando una instantánea automatizada se copia en la región de AWS de destino y alcanza el periodo de retención allí, se elimina de la región de AWS de destino. De este modo, el uso de instantáneas se mantiene en niveles bajos. Para conservar las instantáneas automatizadas durante un periodo más largo o más corto en la región de AWS de destino, cambie el periodo de retención.

El periodo de retención que establezca para las instantáneas automatizadas que se copian en la región de AWS de destino es distinto del periodo de retención para las instantáneas automatizadas de la región de AWS de origen. El período de retención predeterminado para las copias de instantáneas es de siete días. Ese período de siete días solo se aplica a las instantáneas automatizadas. En las regiones de AWS de origen y de destino, las instantáneas manuales se eliminan al final del periodo de retención de la instantánea o cuando se eliminan de forma manual.

Puede desactivar la copia de instantánea automática de un clúster en cualquier momento. Cuando desactive esta característica, las instantáneas dejarán de copiarse de la región de AWS de origen a la región de AWS de destino. Cualquier instantánea automatizada que se copie a la región de AWS de destino se eliminará cuando alcance el límite del periodo de retención, a menos que el usuario cree copias de instantánea manuales de estas. Estas instantáneas manuales, así como cualquier instantánea manual que se haya copiado de la región de AWS de destino, se conservarán en la región de AWS de destino hasta que el usuario las elimine de forma manual.

Para cambiar la región de AWS de destino en la que copia las instantáneas, desactive primero la característica de copia automática. Luego, habilítela de nuevo y especifique la región de AWS de destino nueva.

Cuando una instantánea se copia en la región de AWS de destino, se activa y se vuelve disponible en caso de que fuera necesario restaurar la información.

Para copiar instantáneas de clústeres cifrados de AWS KMS en otra región de AWS, cree una concesión para Amazon Redshift para que pueda utilizar una clave administrada del cliente en la región de AWS de destino. Luego, elija esa concesión cuando habilite la copia de instantáneas en la región de AWS de origen. Para obtener más información acerca de la configuración de

autorizaciones para copiar instantáneas, consulte Copia de instantáneas cifradas por AWS KMS en otra región de AWS.

Restauración de un clúster desde una instantánea

Las instantáneas contienen datos de las bases de datos que se ejecutan en el clúster. También contiene información sobre el clúster, como el número de nodos, el tipo de nodos y el nombre de usuario administrador. Si restaura el clúster a partir de una instantánea, Amazon Redshift utilizará la información del clúster para crear otro nuevo. Luego, restaurará todas las bases de datos a partir de los datos de la instantánea.

En el clúster que se crea a partir de la instantánea original, puede seleccionar la configuración, como el tipo y el número de nodos. El clúster se restaura en la misma región de AWS y en una zona de disponibilidad elegida aleatoriamente por el sistema, a menos que el usuario especifique otra zona de disponibilidad en la solicitud. Cuando se restaura un clúster a partir de una instantánea, se puede elegir una pista de mantenimiento compatible para el nuevo clúster.

> **Note**
>
> Cuando se restaura una instantánea en un clúster con una configuración diferente, la instantánea debe haberse tomado de un clúster con la versión 1.0.10013 u otra posterior.

Cuando una restauración está en curso, los eventos se emiten normalmente en el siguiente orden:

1. Se envía RESTORE_STARTED — REDSHIFT-EVENT-2008 cuando comienza el proceso de restauración.
2. Se envía RESTORE_SUCCEEDED – REDSHIFT-EVENT-3003 cuando se ha creado el clúster nuevo.

   El clúster está disponible para consultas.
3. Se envía DATA_TRANSFER_COMPLETED – REDSHIFT-EVENT-3537 cuando se completa la transferencia de datos.

> **Note**
>
> Los clústeres RA3 solo emiten eventos RESTORE_STARTED y RESTORE_SUCCEEDED. No hay ninguna transferencia explícita de datos que se realice después de que un

evento RESTORE tenga éxito, ya que los tipos de nodo RA3 almacenan datos en el almacenamiento administrado de Amazon Redshift. Con los nodos RA3, los datos se transfieren de forma continua entre los nodos RA3 y el almacenamiento administrado de Amazon Redshift como parte del procesamiento normal de consultas. Los nodos RA3 almacenan en caché los datos calientes localmente y mantienen los bloques consultados con menos frecuencia en el almacenamiento administrado de Amazon Redshift de forma automática.

Puede monitorizar el progreso de las restauraciones llamando a la acción DescribeClusters de la API o consultando los detalles del clúster en la AWS Management Console. Para una restauración en proceso, estos muestran información como el tamaño de los datos de la instantánea, la tasa de transferencia, el tiempo transcurrido y el tiempo restante estimado. Para ver una descripción de estas métricas, visite RestoreStatus.

No puede utilizar una instantánea para que un clúster activo vuelva a un estado anterior.

> **Note**
>
> Cuando restaura una instantánea en un clúster nuevo, se usan los grupos de parámetros y de seguridad predeterminados, a menos que especifique valores diferentes.

Es posible que quiera restaurar una instantánea en un clúster con una configuración diferente por las siguientes razones:

- Si un clúster se compone de tipos de nodos más pequeños y desea consolidarlos en un tipo de nodo más grande para que tenga menos nodos.
- Si ha monitorizado la carga de trabajo y ha determinado que es necesario cambiar a un tipo de nodo con más CPU y más almacenamiento.
- Si desea medir el rendimiento de cargas de trabajo de prueba con diferentes tipos de nodos.

La restauración tiene las siguientes restricciones:

- La configuración del nuevo nodo debe tener suficiente almacenamiento para los datos existentes. Incluso cuando se agregan nodos, es posible que la nueva configuración no disponga de suficiente almacenamiento por la forma en que se han redistribuido los datos.

- La operación de restauración verifica si la instantánea se creó en una versión de clúster compatible con la versión de clúster del clúster nuevo. Si el clúster nuevo tiene un nivel de versión demasiado nuevo, se produce un error en la operación de restauración y se brinda más información en un mensaje de error.
- Las configuraciones posibles (número de nodos y tipo de nodo) a las que puede restaurar están determinadas por el número de nodos del clúster original y el tipo de nodo de destino del nuevo clúster. Para determinar las posibles configuraciones disponibles, puede utilizar la consola de Amazon Redshift o el comando `describe-node-configuration-options` AWS CLI con `action-type restore-cluster`. Para obtener más información acerca de cómo restaurar con la consola de Amazon Redshift, consulte Restauración de un clúster desde una instantánea.

En el siguiente procedimiento, se toma un clúster con muchos nodos y se consolida en un tipo de nodo mayor con menos nodos utilizando la AWS CLI. En este ejemplo, empezaremos con un clúster de oirgen de 24 nodos `ds2.xlarge`. En este caso, supongamos que ya se ha creado una instantánea de este clúster y que queremos restaurarlo en un tipo de nodo más grande.

1. Ejecute el siguiente comando para obtener los detalles de un clúster `ds2.xlarge` de 24 nodos.

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
 mycluster-123456789012
```

2. Ejecute el siguiente comando para obtener los detalles de una instantánea.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
 mycluster-snapshot
```

3. Ejecute el siguiente comando para describir las opciones disponibles en esta instantánea.

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-
snapshot --region eu-west-1 --action-type restore-cluster
```

   Este comando devuelve una lista de opciones con recomendaciones sobre los tipos de nodos, el número de nodos y el uso de disco de cada opción. En este ejemplo, el comando anterior muestra las siguientes configuraciones de nodos posibles. Hemos decidido realizar la restauración en un clúster `ds2.8xlarge` de tres nodos.

```
{
    "NodeConfigurationOptionList": [
```

```
        {
            "EstimatedDiskUtilizationPercent": 65.26134808858235,
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 24
        },
        {
            "EstimatedDiskUtilizationPercent": 32.630674044291176,
            "NodeType": "ds2.xlarge",
            "NumberOfNodes": 48
        },
        {
            "EstimatedDiskUtilizationPercent": 65.26134808858235,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 3
        },
        {
            "EstimatedDiskUtilizationPercent": 48.94601106643677,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 4
        },
        {
            "EstimatedDiskUtilizationPercent": 39.156808853149414,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 5
        },
        {
            "EstimatedDiskUtilizationPercent": 32.630674044291176,
            "NodeType": "ds2.8xlarge",
            "NumberOfNodes": 6
        }
    ]
}
```

4. Ejecute el comando siguiente para restaurar la instantánea con la configuración de clúster elegida. Una vez restaurado el clúster, tenemos el mismo contenido que el clúster de origen, pero los datos se han consolidado en tres nodos `ds2.8xlarge`.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
 mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
 ds2.8xlarge --number-of-nodes 3
```

Si tiene nodos reservados, por ejemplo, DS2 o DC2, puede actualizarlos a nodos reservados RA3. Puede hacer esto cuando restaura desde una instantánea o realiza un redimensionamiento elástico. Puede utilizar la consola para guiarse a través de este proceso. Para obtener más información acerca de la actualización a nodos RA3, consulte Actualización a tipos de nodo RA3.

Restauración de una tabla a partir de una instantánea

Puede restaurar una tabla individual a partir de una instantánea, en lugar de restaurar todo un clúster. Cuando restaure una tabla individual a partir de una instantánea, especifique la instantánea de origen, la base de datos, el esquema y el nombre de la tabla, además de la base de datos de destino, el esquema y un nuevo nombre de tabla para la tabla restaurada.

El nuevo nombre de la tabla no puede ser el nombre de una tabla ya existente. Para sustituir una tabla existente por una tabla restaurada a partir de una instantánea, cambie el nombre o elimine la tabla ya existente antes de restaurar la tabla desde la instantánea.

La tabla de destino se crea utilizando las definiciones de columnas, los atributos de tabla y los atributos de columna de la tabla de origen, a excepción de las claves externas. Para evitar conflictos de dependencias, la tabla de destino no hereda las claves externas de la tabla de origen. Cualquier dependencia, como vistas o permisos concedidos en la tabla de origen, no se aplica a la tabla de destino.

Si el propietario de la tabla de origen existe, ese usuario de base de datos es el propietario de la tabla restaurada, dado que el usuario tiene los permisos suficientes para volverse el propietario de una relación en la base de datos y el esquema especificados. De lo contrario, la tabla restaurada es propiedad del usuario administrador que se creó cuando se lanzó el clúster.

La tabla restaurada vuelve al estado en el que estaba en el momento que se realizó el backup. Esto incluye las reglas de visibilidad de las transacciones definidas en virtud del cumplimiento de Amazon Redshift con el aislamiento serializable, lo que significa que los datos estarán visibles de inmediato para las transacciones en tránsito que se inicien después de la copia de seguridad.

La restauración de una tabla a partir de una instantánea tiene las siguientes limitaciones:

- Puede restaurar una tabla únicamente para el clúster actual en ejecución activa y a partir de una instantánea que se haya tomado de ese clúster.
- Puede restaurar solo una tabla a la vez.
- No se puede restaurar una tabla a partir de una instantánea de clúster que se haya tomado antes cambiarle el tamaño a un clúster. Como excepción, se puede restaurar una tabla después de un cambio de tamaño elástico si el tipo de nodo no ha cambiado.

- Cualquier dependencia, como vistas o permisos concedidos en la tabla de origen, no se aplica a la tabla de destino.
- Si la seguridad de nivel de fila está activada para una tabla que se está restaurando, Amazon Redshift restaura la tabla con la seguridad de nivel de fila activada.

Restauración de una tabla a partir de una instantánea

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y elija el clúster que quiere utilizar para restaurar una tabla.
3. Para Actions (Acciones), seleccione Restore table (Restaurar tabla) para mostrar la página Restore table (Restaurar tabla).
4. Introduzca la información sobre qué instantánea, tabla de origen y tabla de destino usar, y luego seleccione Restore table (Restaurar tabla).

Example Ejemplo: Restauración de una tabla a partir de una instantánea con la AWS CLI

En el siguiente ejemplo, se utiliza el comando `restore-table-from-cluster-snapshot` de la AWS CLI para restaurar la tabla`my-source-table` desde el esquema `sample-database` en la `my-snapshot-id`. Puede utilizar el comando `describe-table-restore-status` de la AWS CLI para consultar el estado de la operación de restauración. En el ejemplo se restaura la instantánea al clúster `mycluster-example` con un nombre de tabla nuevo de `my-new-table`.

```
aws redshift restore-table-from-cluster-snapshot --cluster-identifier mycluster-
example
                                                 --new-table-name my-new-table
                                                 --snapshot-identifier my-snapshot-id
                                                 --source-database-name sample-
database
                                                 --source-table-name my-source-table
```

Uso compartido de instantáneas

Puede compartir una instantánea manual ya existente con otras cuentas de clientes de AWS mediante la autorización de acceso a la instantánea. Puede autorizar hasta el 20 de cada

instantánea y el 100 de cada clave de AWS Key Management Service (AWS KMS). Es decir, si tiene 10 instantáneas que están cifradas con una sola clave de KMS, puede autorizar a 10 cuentas de AWS a restaurar cada instantánea u otras combinaciones que sumen hasta 100 cuentas y no excedan las 20 cuentas por cada instantánea. Una persona que haya iniciado sesión como usuario en una de las cuentas autorizadas puede describir la instantánea o restaurarla para crear un clúster de Amazon Redshift nuevo en su cuenta. Por ejemplo, si utiliza cuentas de clientes de AWS independientes para pruebas y producción, un usuario puede iniciar sesión con la cuenta de producción y compartir una instantánea con usuarios de la cuenta de pruebas. Alguien que haya iniciado sesión como usuario de la cuenta de pruebas puede restaurar la instantánea para crear un clúster nuevo que sea propiedad de la cuenta de pruebas para realizar pruebas y diagnósticos.

Una instantánea manual es propiedad permanente de la cuenta de cliente de AWS con la que fue creada. Solo los usuarios de la cuenta propietaria de la instantánea pueden autorizar a otras cuentas a obtener acceso a la instantánea o a revocar autorizaciones. Los usuarios de las cuentas autorizadas solo pueden describir o restaurar cualquier instantánea que se haya compartido con ellos; no pueden copiar o eliminar instantáneas que se hayan compartido con ellos. Una autorización permanece en vigor hasta que el propietario de la instantánea la revoque. Si se revoca una autorización, el usuario anteriormente autorizado pierde la visibilidad de la instantánea y no podrá lanzar ninguna acción nueva que haga referencia a la instantánea. Si la cuenta está en el proceso de restauración de la instantánea cuando se revoca el acceso, la restauración se ejecuta hasta finalizarse. No puede eliminar una instantánea mientras tenga autorizaciones activas, primero debe revocar todas las autorizaciones.

Las cuentas de clientes de AWS están autorizados de forma permanente a obtener acceso a las instantáneas propiedad de la cuenta. Los intentos de autorizar o revocar el acceso a la cuenta del propietario recibirán un error. No puede restaurar o describir una instantánea que sea propiedad de una cuenta de cliente de AWS inactiva.

Después de haber autorizado el acceso a una cuenta de cliente de AWS, ningún usuario de de esa cuenta podrá realizar acciones en la instantánea a menos que asuma un rol con políticas que les permitan hacerlo.

- Los usuarios de la cuenta del propietario de la instantánea pueden autorizar y revocar el acceso a una instantánea solo si asumen un rol una política de IAM que les permita realizar esas acciones con una especificación de recursos que incluya la instantánea. Por ejemplo, la siguiente política permite a un usuario o rol de la cuenta `012345678912` de AWS autorizar a otras cuentas para que obtengan acceso a la instantánea `my-snapshot20130829`:

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "redshift:AuthorizeSnapshotAccess",
          "redshift:RevokeSnapshotAccess"
          ],
      "Resource":[
           "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-snapshot20130829"
          ]
    }
  ]
}
```

- Los usuarios de una cuenta de AWS con la que se ha compartido una instantánea no pueden realizar acciones en esa instantánea a menos que tengan permisos que permitan esas acciones. Puede hacerlo mediante la asignación de la política a un rol y asumiéndolo.
  - Para enumerar o describir una instantánea, deben tener una política de IAM que permita la acción `DescribeClusterSnapshots`. En el siguiente código se muestra un ejemplo:

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "redshift:DescribeClusterSnapshots"
          ],
      "Resource":[
           "*"
          ]
    }
  ]
}
```

  - Para restaurar una instantánea, un usuario debe tener una política de IAM que permita la acción `RestoreFromClusterSnapshot` y tenga un elemento de recursos que abarque el clúster que están intentando crear y la instantánea. Por ejemplo, si un usuario de la cuenta `012345678912` ha compartido la instantánea `my-snapshot20130829` con la cuenta `219876543210`,

para crear un clúster mediante la restauración de la instantánea, un usuario de la cuenta `219876543210` debe asumir un rol con una política como la siguiente:

```
{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "redshift:RestoreFromClusterSnapshot"
          ],
      "Resource":[
           "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-
snapshot20130829",
           "arn:aws:redshift:us-east-1:219876543210:cluster:from-another-account"
          ]
    }
  ]
}
```

- Después de revocar el acceso a una instantánea desde una cuenta AWS, ningún usuario de esa cuenta puede acceder a la instantánea. Este es el caso incluso si esas cuentas tienen políticas de IAM que permiten acciones en el recurso de instantánea previamente compartido.

Administración de instantáneas mediante la consola

Amazon Redshift toma instantáneas automáticas y progresivas de los datos de forma periódica y las guarda en Amazon S3. Además, puede tomar snapshots manuales de sus datos cada vez que lo desee. En esta sección, puede descubrir cómo administrar sus instantáneas desde la consola de Amazon Redshift. Para obtener más información acerca de las instantáneas, consulte Instantáneas y copias de seguridad de Amazon Redshift.

Todas las tareas de instantáneas de la consola de Amazon Redshift se inician desde la lista de instantáneas. Puede filtrar la lista utilizando un intervalo de tiempo, el tipo de instantánea y el clúster asociado con la instantánea. Además, puede ordenar la lista por fecha, tamaño y tipo de instantánea. Según el tipo de instantánea que haya seleccionado, es posible que tenga diferentes opciones disponibles para trabajar con la instantánea.

Temas

- Creación de una programación de instantáneas

- Creación de una instantánea manual
- Cambiar el periodo de retención de instantáneas manuales
- Eliminar instantáneas manuales
- Copia de una instantánea automatizada
- Restauración de un clúster desde una instantánea
- Restauración de un espacio de nombres sin servidor desde una instantánea
- Compartir una instantánea de un clúster
- Configuración de la copia de una instantánea entre regiones para un clúster no cifrado
- Configurar la copia de instantáneas entre regiones para un clúster cifrado en AWS KMS
- Modificación del periodo de retención para una copia de instantáneas entre regiones

Creación de una programación de instantáneas

Para controlar con precisión cuándo se realizan las instantáneas, puede crear una programación de instantáneas y asociarla a uno o varios clústeres. Puede asociar una programación cuando cree un clúster o modificando el clúster. Para obtener más información, consulte Programación de instantáneas automatizadas.

Para crear una programación de instantáneas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la pestaña Snapshot schedules (Horarios de intantáneas). Se muestran los horarios de las instantáneas.
3. SeleccioneAdd schedule (Agregar horario) para mostrar la página para agregar un horario.
4. Introduzca las propiedades de la definición de programación, luego seleccione Add schedule (Agregar horario).
5. En la página que aparece, puede adjuntar clústeres a su nuevo horario de instantáneas, luego seleccione OK.

Creación de una instantánea manual

Puede crear una snapshot manual de un clúster desde la lista de snapshots de la siguiente manera. O bien puede tomar una snapshots de un clúster en el panel de configuración del clúster. Para obtener más información, consulte Crear una instantánea de un clúster.

Creación de una instantánea manual

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija Create snapshot (Crear instantánea). Se muestra la página de instantáneas para crear una instantánea manual.
3. Introduzca las propiedades de la definición de instantánea, luego seleccione Create snapshot (Crear instantánea). La instantánea puede tardar un poco en estar disponible.

Cambiar el periodo de retención de instantáneas manuales

Puede cambiar el periodo de retención para una instantánea manual modificando la configuración de la instantánea.

Para cambiar el periodo de retención de instantáneas manuales

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea manual para cambiar.
3. Para Actions (Acciones), seleccione Manual snapshot settings (Configuración de instantáneas manuales) para mostrar las propiedades de la instantánea manual.
4. Introduzca las propiedades editadas de la definición de instantánea, luego seleccione Save (Guardar).

Eliminar instantáneas manuales

Para eliminar instantáneas manuales, seleccione una o más instantáneas en la lista de instantáneas.

Pasos para eliminar una snapshot manual

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea que desea eliminar.
3. Para Actions (Acciones), seleccioneDelete snapshot (Borrar instantánea) para borrar la instantánea.
4. Confirme la eliminación de las instantáneas enumeradas, luego seleccione Delete (Eliminar).

Copia de una instantánea automatizada

Las snapshots automatizadas se eliminan de forma automática cuando expira el periodo de retención, cuando el usuario deshabilita la opción de snapshots automatizadas o cuando elimina un clúster. Si desea conservar una snapshot automatizada, puede copiarla a una snapshot manual.

Pasos para copiar una snapshot automatizada

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea que desea copiar.
3. Para Actions (Acciones), seleccione Copy automated snapshot (Copiar instantánea automática) para copiar la instantánea.
4. Actualice las propiedades de la nueva instantánea, luego seleccione Copy (Copiar).

Restauración de un clúster desde una instantánea

Cuando restaura un clúster a partir de una instantánea, Amazon Redshift crea un nuevo clúster con todos los datos de la instantánea en el clúster nuevo.

Pasos para restaurar un clúster desde una snapshot

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea que desea restaurar.

3. Seleccione Restore from snapshot (Restaurar desde instantánea) para ver los valores de laCluster configuration (Configuración de clúster) y los Cluster details (Detalles de clúster) del nuevo clúster que se creará utilizando la información de la instantánea.
4. Actualice las propiedades del nuevo clúster, luego seleccione Restore cluster from snapshot (Restaurar clúster desde instantánea).

Si AWS Secrets Manager no administraba la contraseña de administrador de su clúster, puede hacer que administre el clúster restaurado seleccionando Administrar credenciales de administrador en AWS Secrets Manager en la sección Configuración del clúster y especificando una clave de KSM. De lo contrario, el clúster se restaura con las credenciales de administrador que tenía en el momento de realizar la instantánea. Puede actualizar las credenciales de administrador del clúster en la página de detalles del clúster después de restaurarlo.

Si AWS Secrets Manager administraba la contraseña de administrador del clúster en el momento en que se realizó la captura de pantalla, debe seguir usando AWS Secrets Manager para administrar la contraseña de administrador. Para dejar de usar un secreto después de restaurar el clúster, debe actualizar las credenciales de administrador del clúster en la página de detalles del clúster.

Si tiene nodos reservados, por ejemplo, DS2 o DC2, puede actualizarlos a nodos reservados RA3. Puede hacer esto cuando restaura desde una instantánea o realiza un redimensionamiento elástico. Puede utilizar la consola para guiarse a través de este proceso. Para obtener más información acerca de la actualización a nodos RA3, consulte Actualización a tipos de nodo RA3.

Restauración de un espacio de nombres sin servidor desde una instantánea

La restauración de un espacio de nombres sin servidor desde una instantánea sustituye todas las bases de datos del espacio de nombres por las bases de datos de la instantánea. Para obtener más información sobre las instantáneas sin servidor, consulte Trabajo con instantáneas y puntos de recuperación. Amazon Redshift convierte automáticamente las tablas con claves intercaladas en claves compuestas al restaurar una instantánea de clúster aprovisionada en un espacio de nombres de Amazon Redshift sin servidor. Para obtener más información sobre claves de clasificación, consulte Uso de claves de clasificación.

Para restaurar una instantánea de su clúster aprovisionado a su espacio de nombres sin servidor.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea que desea usar.
3. Elija Restore from snapshot (Restaurar desde una instantánea), Restore to serverless namespace (Restaurar al espacio de nombres sin servidor).
4. Elija el espacio de nombres en el que desea restaurar.
5. Confirme que desea restaurar desde su instantánea. Elija Restore (Restaurar). Esta acción reemplaza todas las bases de datos en el espacio de nombres sin servidor por los datos de su clúster aprovisionado.

Compartir una instantánea de un clúster

Puede autorizar a otros usuarios a obtener acceso a una snapshot manual de su propiedad o puede revocar ese acceso más adelante cuando ya no sea necesario.

Para compartir una instantánea con otra cuenta de

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea manual para compartir.
3. Para Actions (Acciones), seleccione Manual snapshot settings (Configuración de instantáneas manuales) para mostrar las propiedades de la instantánea manual.
4. Introduzca la cuenta o cuentas para compartir en la sección Manage access (Administrar acceso), luego seleccione Save (Guardar).

Consideraciones de seguridad del uso compartido de instantáneas cifradas

Cuando proporciona acceso a una instantánea cifrada, Redshift requiere que la clave administrada por el cliente de AWS KMS utilizada para crear la instantánea se comparta con la cuenta o las cuentas que realizan la restauración. Si la clave no se comparte, al intentar restaurar la instantánea se producirá un error de acceso denegado. La cuenta receptora no necesita ningún permiso adicional para restaurar una instantánea compartida. Cuando autoriza el acceso a instantáneas y comparte la clave, la identidad que autoriza el acceso debe tener permisos `kms:DescribeKey` de la clave que se utilizó para cifrar la instantánea. Este permiso se describe con más detalle en Permisos de AWS KMS. Para obtener más información, consulte DescribeKey en la documentación de referencia de API de Amazon Redshift.

La política de claves administrada por el cliente se puede actualizar mediante programación o en la consola de AWS Key Management Service.

Habilitación de acceso a la clave de AWS KMS para una instantánea cifrada

Para compartir la clave administrada por el cliente de AWS KMS para una instantánea cifrada, actualice la política de claves realizando los siguientes pasos:

1. Actualice la política de claves de KMS con el nombre de recurso de Amazon (ARN) de la cuenta de AWS con la que va a compartir como `Principal` en la política de clave de KMS.
2. Permita la acción `kms:Decrypt`.

En el siguiente ejemplo de política de claves, el usuario `111122223333` es el propietario de la clave de KMS y el usuario `444455556666` es la cuenta con la que se comparte la clave. Esta política de claves da a la cuenta de AWS acceso a la clave de KMS de ejemplo al incluir el ARN de la identidad raíz de la cuenta de AWS del usuario `444455556666` como `Principal` para la política, y al permitir la acción `kms:Decrypt`.

```
{
    "Id": "key-policy-1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/KeyUser",
                    "arn:aws:iam::444455556666:root"
                ]
            },
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Una vez que se haya concedido acceso a la clave de KMS administrada por el cliente, la cuenta que restaura la instantánea cifrada debe crear un rol de IAM AWS Identity and Access Management, o un usuario, si aún no tiene uno. Además, dicha cuenta de AWS también debe asociar a ese usuario o rol de IAM una política de IAM que les permita restaurar una instantánea de base de datos cifrada con la clave de KMS.

Para obtener más información acerca de cómo proporcionar acceso a una clave de AWS KMS, consulte Permitir a los usuarios de otras cuentas utilizar una clave de KMS en la guía para desarrolladores de AWS Key Management Service.

Para obtener información general sobre las políticas de claves, consulte ¿Cómo Amazon Redshift utiliza AWS KMS?.

Configuración de la copia de una instantánea entre regiones para un clúster no cifrado

Puede configurar Amazon Redshift de manera que copie instantáneas de un clúster en otra región de AWS. Para configurar la copia de instantáneas entre regiones, debe habilitar esta característica de copia en cada clúster y configurar dónde desea copiar las instantáneas y por cuánto tiempo desea conservar las instantáneas automatizadas o manuales que se copiaron en la región de AWS de destino. Cuando se habilita la copia entre regiones de un clúster, se copian todas las instantáneas manuales y automatizadas en la región de AWS especificada. Los nombres de las instantáneas que se copian tienen el prefijo **`copy:`**.

Para configurar instantáneas entre regiones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y elija el clúster del que desea mover las instantáneas.
3. Para Actions (Acciones), elija Configure cross-region snapshot (Configurar instantánea entre regiones).

   Aparecerá el cuadro de diálogo Configure cross-Region (Configuración entre regiones).
4. Para Copy snapshots (Copiar instantáneas), elija Yes (Sí).
5. En Destination AWS Region (Región de AWS de destino), elija la región de AWS en la que desea copiar las instantáneas.

6. En Automated snapshot retention period (days) (Periodo de retención de instantáneas automatizadas [días]), elija la cantidad de días durante la que desea retener las instantáneas automatizadas en la región de AWS de destino antes de que se eliminen.
7. En Manual snapshot retention period (Periodo de retención de instantáneas manuales), elija el valor que represente la cantidad de días durante la que desea retener las instantáneas manuales en la región de AWS de destino antes de que se eliminen. Si elige Custom value (Valor personalizado), el periodo de retención debe ser entre 1 y 3653 días.
8. Elija Guardar.

Configurar la copia de instantáneas entre regiones para un clúster cifrado en AWS KMS

Cuando lance un clúster de Amazon Redshift, puede elegir cifrarlo con una clave raíz de AWS Key Management Service (AWS KMS). Las claves de AWS KMS son específicas de una región de AWS. Si desea habilitar la copia de instantáneas entre regiones para un clúster cifrado por AWS KMS, debe configurar una concesión de copia de instantánea para una clave raíz en la región de AWS de destino. Al hacer esto, habilita a Amazon Redshift para que realice operaciones de cifrado en la región de AWS de destino.

En el siguiente procedimiento, se describe el proceso para habilitar la copia de instantáneas entre regiones para un clúster cifrado en AWS KMS. Para obtener más información acerca del cifrado en Amazon Redshift y las concesiones de copia de instantáneas, consulte Copia de instantáneas cifradas por AWS KMS en otra región de AWS.

Para configurar una instantánea entre regiones de un clúster cifrado en AWS KMS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y elija el clúster del que desea mover las instantáneas.
3. Para Actions (Acciones), elija Configure cross-region snapshot (Configurar instantánea entre regiones).

   Aparecerá el cuadro de diálogo Configure cross-Region (Configuración entre regiones).
4. Para Copy snapshots (Copiar instantáneas), elija Yes (Sí).
5. En Destination AWS Region (Región de AWS de destino), elija la región de AWS en la que desea copiar las instantáneas.

6. En Automated snapshot retention period (days) (Periodo de retención de instantáneas automatizadas [días]), elija la cantidad de días durante la que desea retener las instantáneas automatizadas en la región de AWS de destino antes de que se eliminen.
7. En Manual snapshot retention period (Periodo de retención de instantáneas manuales), elija el valor que represente la cantidad de días durante la que desea retener las instantáneas manuales en la región de AWS de destino antes de que se eliminen. Si elige Custom value (Valor personalizado), el periodo de retención debe ser entre 1 y 3653 días.
8. Elija Guardar.

Modificación del periodo de retención para una copia de instantáneas entre regiones

Después de configurar la copia de instantáneas entre regiones, es posible que desee cambiar la configuración. Puede cambiar el periodo de retención fácilmente si selecciona otra cantidad de días y guarda los cambios.

> **Warning**
>
> Una vez que se haya configurado la copia de instantáneas entre regiones, no puede modificar la región de AWS de destino.
> Si desea copiar instantáneas en una región de AWS diferente, primero desactive la copia de instantáneas entre regiones. Luego, vuelva a habilitarla con una nueva región de AWS de destino y un nuevo periodo de retención. Las instantáneas automáticas copiadas se eliminan después de deshabilitar la copia de la instantánea entre regiones. Por lo tanto, debe determinar si desea conservar alguna y copiarlas en instantáneas manuales antes de deshabilitar la copia de instantáneas entre regiones.

Para modificar instantáneas entre regiones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el clúster del cual desea modificar las instantáneas.
3. En Actions (Acciones), elija Configure cross-region snapshot (Configurar instantánea entre regiones) para mostrar las propiedades de la instantánea.
4. Introduzca las propiedades editadas de la definición de instantánea, luego seleccione Save (Guardar).

Administración de instantáneas mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar las instantáneas.

- authorize-snapshot-access
- copy-cluster-snapshot
- create-cluster-snapshot
- delete-cluster-snapshot
- describe-cluster-snapshots
- disable-snapshot-copy
- enable-snapshot-copy
- modify-snapshot-copy-retention-period
- restore-from-cluster-snapshot
- revoke-snapshot-access

Puede utilizar las siguientes acciones de la API de Amazon Redshift para administrar las instantáneas.

- AuthorizeSnapshotAccess
- CopyClusterSnapshot
- CreateClusterSnapshot
- DeleteClusterSnapshot
- DescribeClusterSnapshots
- DisableSnapshotCopy
- EnableSnapshotCopy
- ModifySnapshotCopyRetentionPeriod
- RestoreFromClusterSnapshot
- RevokeSnapshotAccess

Para obtener más información acerca de las instantáneas de Amazon Redshift, consulte Instantáneas y copias de seguridad de Amazon Redshift.

Uso de AWS Backup

AWS Backup es un servicio totalmente administrado que le ayuda a centralizar y automatizar la protección de datos en todos los servicios de AWS, en la nube y en las instalaciones.

Con AWS Backup para Amazon Redshift, puede configurar las políticas de protección de datos y supervisar la actividad de los diferentes recursos de Amazon Redshift en un solo lugar. También puede crear y almacenar instantáneas en los clústeres aprovisionados de Amazon Redshift. Esto le permite automatizar y consolidar las tareas de copia de seguridad que antes tenía que hacer por separado, sin ningún proceso manual.

Una copia de seguridad, o punto de recuperación, representa el contenido de un recurso, como un clúster de Amazon Redshift, en un momento determinado. Una copia de seguridad se refiere generalmente a las diferentes copias de seguridad en servicios de AWS, como las instantáneas de Amazon Redshift. AWS Backup guarda las copias de seguridad en almacenes de copia de seguridad, que puede organizar según sus necesidades empresariales. Los términos punto de recuperación y copia de seguridad se utilizan indistintamente. Para obtener más información acerca de AWS Backup, consulte Uso de las copias de seguridad.

Amazon Redshift se integra de forma nativa con AWS Backup. Eso le permite definir sus planes de copia de seguridad y asignar recursos de Amazon Redshift a los planes de copia de seguridad. AWS Backup automatiza la creación de instantáneas manuales de Amazon Redshift y almacena de forma segura estas instantáneas en un almacén de copia de seguridad cifrado que usted designa en su plan de copia de seguridad. Para obtener información sobre almacenes, consulte Uso de almacenes de copia de seguridad. En el plan de copia de seguridad, puede definir la frecuencia, el intervalo, el ciclo de vida o el almacén de copia de seguridad. Para obtener información sobre los planes de copia de seguridad, consulte Administración de copias de seguridad mediante planes de copia de seguridad.

Temas

- Consideraciones sobre el uso de AWS Backup con Amazon Redshift
- Administración de AWS Backup con Amazon Redshift

Consideraciones sobre el uso de AWS Backup con Amazon Redshift

En las siguientes secciones se describen las consideraciones y limitaciones del uso de AWS Backup con Amazon Redshift.

Consideraciones sobre el uso de AWS Backup con Amazon Redshift

A continuación, se presentan las consideraciones a tener en cuenta para utilizar AWS Backup con Amazon Redshift:

- AWS Backup para Amazon Redshift está disponible cuando AWS Backup y Amazon Redshift están disponibles en las mismas Regiones de AWS. Para obtener información sobre dónde está disponible AWS Backup, consulte Disponibilidad de características por Regiones de AWS.
- Para empezar a usar AWS Backup, compruebe que cumple todos los requisitos previos. Para obtener más información, consulte Requisitos previos.
- Suscríbase en el servicio AWS Backup. Las opciones de suscripción se aplican a la cuenta y Región de AWS específicas. Es posible que tenga que suscribirse a varias regiones con la misma cuenta. Para obtener más información, consulte Introducción 1: suscripción al servicio.
- Desde la consola de Amazon Redshift, puede crear instantáneas manuales y automatizadas. AWS Backupsolo admite instantáneas manuales en este momento.
- Una vez que utilice AWS Backup para administrar la configuración de instantáneas, no podrá seguir administrando la configuración de instantáneas manuales con Amazon Redshift. En su lugar, puede seguir administrando la configuración mediante un plan de AWS Backup. Para obtener más información, consulte Administración de copias de seguridad mediante planes de copia de seguridad.
- Para ahorrar costos de almacenamiento cuando tenga buckets de Amazon S3 habilitados para el control de versiones de los que se harán copias de seguridad, le recomendamos que establezca una regla de caducidad del ciclo de vida. Para obtener más información sobre la especificación de una regla de ciclo de vida, consulte Ejemplo 6: especificación de una regla de ciclo de vida para un bucket habilitado para el control de versiones. Si no establece un periodo de caducidad del ciclo de vida, sus costos de almacenamiento de Amazon Redshift podrían aumentar, ya que AWS Backup conserva todas las versiones de sus datos de Amazon Redshift.

Limitaciones

A continuación, se detallan limitaciones para utilizar AWS Backup en Amazon Redshift:

- No puede utilizar AWS Backup para administrar las instantáneas automatizadas de Amazon Redshift. Para administrar las instantáneas automatizadas, utilice etiquetas. Para obtener información acerca de cómo etiquetar los recursos, consulte Etiquetado de recursos en Amazon Redshift.
- AWS Backup no admite con Amazon Redshift sin servidor.

Administración de AWS Backup con Amazon Redshift

Para proteger los recursos de los clústeres aprovisionados de Amazon Redshift, puede utilizar la consola de AWS Backup o utilizar mediante programación la API AWS Backup o AWS Command Line Interface (AWS CLI). Si tiene que recuperar un recurso, puede utilizar la consola de AWS Backup o bien la AWS CLI para encontrar y recuperar el recurso que necesita. Para obtener más información, consulte AWS Command Line Interface.

Al utilizar AWS Backup para Amazon Redshift, puede realizar las siguientes acciones:

- Crear copias de seguridad periódicas que inicien automáticamente las instantáneas de Amazon Redshift. Las copias de seguridad periódicas son útiles para satisfacer sus necesidades de retención de datos a largo plazo. Para obtener más información, consulte Copias de seguridad Amazon Redshift.
- Automatizar la programación y la retención de copias de seguridad mediante la configuración centralizada de los planes de copia de seguridad.
- Restaurar un clúster en la copia de seguridad guardada que elija. Establezca la frecuencia con la que desea realizar copias de seguridad de sus recursos. Para obtener más información, consulte Restaurar un clúster de Amazon Redshift.

Configuración de la implementación multi-AZ

Amazon Redshift admite implementaciones de múltiples zonas de disponibilidad (multi-AZ) para clústeres RA3 aprovisionados. Al utilizar implementaciones multi-AZ, su almacenamiento de datos de Amazon Redshift puede seguir funcionando en situaciones de error cuando se produce un evento inesperado en una zona de disponibilidad. Una implementación multi-AZ implementa recursos de computación en dos zonas de disponibilidad (AZ) a las que se puede acceder a través de un único punto de conexión. En caso de que se produzca un error en toda la zona de disponibilidad, los otros recursos de computación de la segunda zona de disponibilidad estarán disponibles para seguir procesando cargas de trabajo. Amazon Redshift cobra las mismas tarifas de computación por hora para RA3 cuando se ejecuta un almacenamiento de datos multi-AZ. Los costos de almacenamiento siguen siendo los mismos, ya que se comparten entre todas las zonas de disponibilidad dentro de la Región de AWS.

Actualmente, Amazon Redshift admite un objetivo de punto de recuperación (RPO) igual a cero, lo que permite que los datos estén actualizados en caso de que se produzca un error. Con la implementación multi-AZ, Amazon Redshift mejora aún más sus capacidades de recuperación

existentes y reduce su objetivo de tiempo de recuperación (RTO). Esto es posible porque una implementación multi-AZ puede recuperarse más rápido de un fallo o desastre, lo que eleva el acuerdo de nivel de servicio (SLA) de Amazon Redshift al 99,99 %, en comparación con el 99,9 % de un almacenamiento de datos single-AZ.

Configuración de la implementación multi-AZ

Al configurar una implementación multi-AZ, seleccione la opción multi-AZ y especifique la cantidad de nodos de computación que se van a aprovisionar en cada zona de disponibilidad. Amazon Redshift implementa automáticamente los mismos recursos de computación en dos zonas de disponibilidad y todos los recursos de computación están siempre disponibles para el procesamiento de lectura y escritura durante el funcionamiento normal. Esto permite que una implementación multi-AZ funcione como un único almacenamiento de datos con un único punto de conexión, lo que elimina la necesidad de cambiar las aplicaciones cuando se produce un desastre. Si bien una implementación multi-AZ procesa una consulta individual con los recursos de computación que residen en una sola zona de disponibilidad, puede distribuir automáticamente el procesamiento de varias consultas simultáneas a ambas zonas de disponibilidad para aumentar el rendimiento general para cargas de trabajo de alta simultaneidad.

También puede convertir un almacenamiento de datos single-AZ existente en un almacenamiento de datos multi-AZ o viceversa. Todo sigue igual, excepto que se aprovisionan recursos de computación adicionales en la segunda zona de disponibilidad. Al migrar a multi-AZ desde un clúster single-AZ existente, es posible que tenga que duplicar la cantidad de nodos de clúster necesarios para facilitar que se mantenga el rendimiento de una sola consulta. La mayoría de cargas de trabajo registran un aumento en el rendimiento general del procesamiento de consultas con un almacenamiento de datos multi-AZ, ya que hay el doble de recursos de computación disponibles.

En caso de que se produzca un error en una zona de disponibilidad, Amazon Redshift seguirá funcionando mediante el uso de los recursos de la zona de disponibilidad restante de forma automática. Sin embargo, es posible que se pierdan las conexiones de los usuarios y se deban restablecer. Además, las consultas que se estaban ejecutando en la zona de disponibilidad fallida pueden fallar y deben retenerse. Sin embargo, puede volver a conectarse al clúster y reprogramar las consultas inmediatamente. Amazon Redshift procesará las consultas en la zona de disponibilidad restante. Las consultas emitidas en el momento de producirse un error o después de este pueden sufrir retrasos en el tiempo de ejecución mientras se recupera el almacenamiento de datos de multi-AZ.

> **Note**
>
> Para lograr un mejor rendimiento y una mayor disponibilidad, le recomendamos que utilice SNAPSHOT ISOLATION con sus clústeres multi-AZ. Para obtener más información, consulte CREATE DATABASE.

Limitaciones

Un almacenamiento de datos multi-AZ tiene las mismas capacidades funcionales que un almacenamiento de datos single-AZ, excepto por las siguientes limitaciones que se aplican a un almacenamiento de datos multi-AZ:

- No puede crear un almacenamiento de datos multi-AZ no cifrado. Asegúrese de añadir un cifrado al crear un nuevo almacenamiento de datos multi-AZ, convertir un almacenamiento de datos single-AZ en multi-AZ o convertir un almacenamiento de datos single-AZ en multi-AZ.
- No puede crear una implementación multi-AZ de un solo nodo para ninguno de los tipos de instancia RA3. Elija dos o más nodos por zona de disponibilidad al crear una implementación multi-AZ.
- Las integraciones sin ETL no son compatibles con los almacenamientos de datos de destino que se configuran para la implementación multi-AZ.
- Amazon Redshift no admite una configuración de subred que permita menos de tres zonas de disponibilidad. Es decir, el grupo de subredes configurado requiere tres subredes más.
- No puede reubicar una implementación multi-AZ en otra zona de disponibilidad. Amazon Redshift determinará y llevará a cabo automáticamente la reubicación cuando se utilice la implementación multi-AZ.
- No puede pausar ni reanudar una implementación multi-AZ.
- No puede ejecutar su implementación multi-AZ fuera de los intervalos de puertos admitidos de 5431 a 5455 y de 8191 a 8215.
- No puede utilizar las vistas STL, SVCS, SVL, SVV ni STV con las implementaciones multi-AZ, ya que solo admiten vistas de monitoreo del sistema (vistas SYS_*). Cambie las consultas de monitoreo para utilizar las vistas de monitoreo del sistema (vistas SYS_*).
- No puede asociar una dirección IP de Elastic a un clúster existente con Multi-AZ habilitado.
- No puede convertir un clúster con una dirección IP de Elastic asociada de Single-AZ a Multi-AZ.

- La implementación multi-AZ de Amazon Redshift está disponible en las siguientes Regiones de AWS:
  - Este de EE. UU. (Ohio) (us-east-2)
  - Este de EE. UU. (Norte de Virginia) (us-east-1)
  - Oeste de EE. UU. (Oregón) (us-west-2)
  - África (Ciudad del Cabo) (af-south-1)
  - Asia-Pacífico (Hong Kong) (ap-east-1)
  - Asia Pacífico (Hyderabad) (ap-south-2)
  - Asia-Pacífico (Yakarta) (ap-southeast-3)
  - Asia Pacífico (Melbourne) (ap-southeast-4)
  - Asia Pacífico (Bombay) (ap-south-1)
  - Asia Pacific (Osaka) (ap-northeast-3)
  - Asia-Pacífico (Seúl) (ap-northeast-2)
  - Asia-Pacífico (Singapur) (ap-southeast-1)
  - Asia-Pacífico (Sídney) (ap-southeast-2)
  - Asia-Pacífico (Tokio) (ap-northeast-1)
  - Canadá (centro) (ca-central-1)
  - Europa (Fráncfort) (eu-central-1)
  - Europa (Irlanda) (eu-west-1)
  - UE (Milán) (eu-south-1)
  - UE (París) (eu-west-3)
  - Europa (España) (eu-south-2)
  - Europa (Estocolmo) (eu-north-1)
  - Europa (Zúrich) (eu-central-2)
  - Israel (Tel Aviv) (il-central-1)
  - Medio Oriente (Baréin) (me-south-1)
  - Medio Oriente (EAU) (me-central-1)

Temas

- Administración de la implementación multi-AZ
- Fallo en la implementación multi-AZ

- Monitoreo de consultas para multi-AZ

Administración de la implementación multi-AZ

Amazon Redshift Multi-AZ admite dos zonas de disponibilidad a la vez. Amazon Redshift selecciona las zonas de disponibilidad automáticamente en función del grupo de subredes elegido. Puede convertir un almacenamiento de datos existente de una única zona de disponibilidad en un almacenamiento de datos multi-AZ o restaurar desde una instantánea para configurarlo en un almacenamiento de datos multi-AZ.

Con la consola de Amazon Redshift, puede crear fácilmente nuevas implementaciones multi-AZ. Para crear una nueva implementación multi-AZ mediante la consola de Amazon Redshift, seleccione la opción multi-AZ al crear el almacenamiento de datos. Especifique la cantidad de nodos de computación necesarios en una sola zona de disponibilidad. Amazon Redshift implementará dicha cantidad de nodos en cada una de las dos zonas de disponibilidad. Todos los nodos se usarán para leer y escribir el proceso de carga de trabajo durante el funcionamiento normal. También puede usar el comando `create-cluster` de la AWS CLI para crear un nuevo almacenamiento de datos multi-AZ con el parámetro `multi-az`.

Puede convertir un almacenamiento de datos single-AZ existente en un almacenamiento de datos multi-AZ. Para ello, puede utilizar la consola de Amazon Redshift o el comando `modify-cluster` de la AWS CLI con el parámetro `multi-az`. O puede restaurar a partir de una instantánea para configurar un almacenamiento de datos single-AZ en un almacenamiento de datos multi-AZ mediante la consola de Amazon Redshift o el comando `restore-from-cluster-snapshot` de la AWS CLI con el parámetro `multi-az`.

La implementación multi-AZ solo admite los tipos de nodo RA3 que utilizan Amazon Redshift Managed Storage (RMS). Amazon Redshift almacena los datos en RMS, que utiliza Amazon S3 y es accesible en todas las zonas de disponibilidad de una Región de AWS, sin tener que replicar los datos en el nivel de Amazon Redshift.

Configuración de multi-AZ al crear un nuevo clúster

Puede configurar la implementación multi-AZ al crear un nuevo clúster mediante la consola de Amazon Redshift o la AWS Command Line Interface.

Mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Provisioned clusters dashboard (Panel de clústeres aprovisionados) y elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el botón Crear clúster para abrir la página de creación de clústeres.
4. Ingrese las propiedades del clúster. Para obtener información general acerca de cómo crear un clúster de base de datos, consulte Creación de un clúster.
5. Elija uno de los tipos de nodo RA3 de la lista desplegable Node type (Tipo de nodo). La opción de configuración AZ solo está disponible si se elige un tipo de nodo RA3.
6. En Configuración AZ, elija Multi-AZ.
7. En Número de nodos por zona de disponibilidad, introduzca al menos dos nodos para el clúster.
8. Tiene la opción de cargar datos de muestra o de trasladar sus propios datos:

   - En Sample data (Datos de muestra), elija Load sample data (Cargar datos de muestra) para cargar el conjunto de datos de muestra en el clúster de Amazon Redshift. Amazon Redshift carga el conjunto de datos de muestra Tickit en la base de datos dev y el esquema public predeterminados. Amazon Redshift carga automáticamente el conjunto de datos de muestra en el clúster de Amazon Redshift. Puede comenzar a utilizar el editor de consultas v2 para consultar datos.
   - Para llevar sus propios datos al clúster de Amazon Redshift, siga los pasos que se indican en Traer sus propios datos a Amazon Redshift.
9. Desplácese hasta Additional configurations (Configuraciones adicionales), expanda Network and security (Red y seguridad) y asegúrese de aceptar valor predeterminado de Cluster subnet group (Grupo de subredes del clúster) o elija otro. Si elige otro grupo de subredes del clúster, asegúrese de que haya tres zonas de disponibilidad en el grupo de subredes que ha seleccionado.
10. En Additional configurations (Configuraciones adicionales), expanda Database configurations (Configuraciones de base de datos).
11. Para usar una clave de AWS KMS personalizada de la clave de AWS Key Management Service predeterminada, haga clic en Personalizar la configuración de cifrado en Cifrado de base de datos.

12. En Choose an KMS key (Elegir una clave de KMS), puede elegir una clave de AWS Key Management Service o ingresar un ARN. O puede hacer clic en Crear una clave de AWS Key Management Service en la consola de AWS Key Management Service. Para obtener más información sobre la creación de claves KMS, consulte Creating Keys (Creación de claves) en la Guía para desarrolladores de AWS Key Management Service.
13. Haga clic en Create cluster. Cuando la restauración del clúster se realice correctamente, podrá ver los detalles en la página de detalles del clúster. Puede usar su cliente SQL para cargar y consultar datos.

Uso de la AWS Command Line Interface

Para configurar la opción multi-AZ al crear un clúster mediante la AWS Command Line Interface

- En la AWS CLI, utilice el comando `create-cluster` y el parámetro `multi-az` de la siguiente manera.

```
aws redshift create-cluster
    --port 5439
    --master-username master
    --master-user-password #####
    --node-type ra3.4xlarge
    --number-of-nodes 2
    --profile maz-test
    --endpoint-url https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz
    --multi-az
    --maintenance-track-name CURRENT
    --encrypted
```

Conversión de un almacenamiento de datos single-AZ en un almacenamiento de datos multi-AZ

Al convertir un almacenamiento de datos single-AZ en un almacenamiento de datos multi-AZ, su almacenamiento de datos estará altamente disponible con una garantía de SLA del 99,99 %. El rendimiento de una consulta individual seguirá siendo el mismo incluso con un almacenamiento de datos multi-AZ. En el caso de cargas de trabajo de mayor simultaneidad, verá un aumento

en el rendimiento general, ya que Amazon Redshift puede ejecutar solicitudes con recursos de computación en dos zonas de disponibilidad.

> **Note**
>
> Amazon Redshift no le permitirá dividir los recursos de computación existentes al pasar de single-AZ a multi-AZ, ni viceversa. Esta operación no se admite para mantener un rendimiento uniforme de las consultas individuales.

Mediante la consola

Para convertir un clúster single-AZ en un almacenamiento de datos multi-AZ mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Provisioned clusters dashboard (Panel de clústeres aprovisionados) y elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el clúster que desea convertir en implementación multi-AZ. Se abrirá la página de detalles del clúster.
4. En Acciones, elija Activar multi-AZ. Aparecerá la página de resumen de modificaciones. Haga clic en Activar multi-AZ.
5. Si se produce un error, realice una de las siguientes acciones y, a continuación, haga clic en Activar multi-AZ.

   - Cifrado de clúster: elija Propiedades para editar la configuración de cifrado en la sección Configuración de la base de datos, en la pestaña Propiedades de la página de detalles del clúster.
   - Grupo de subredes: elija Grupo de subredes para editar la configuración del grupo de subredes del clúster haciendo clic en el enlace del grupo de subredes. Si elige otro grupo de subredes del clúster, asegúrese de que haya tres zonas de disponibilidad en el grupo de subredes que ha seleccionado.
   - Configuración del puerto: elija Propiedades para editar la configuración del puerto en la sección Configuración de la base de datos, en la pestaña Propiedades de la página de detalles del clúster.

6. Puede usar su cliente SQL para cargar y consultar datos.

Uso de la AWS Command Line Interface

- En la AWS CLI, utilice el comando `modify-cluster` y el parámetro `multi-az` de la siguiente manera.

```
aws redshift modify-cluster
    --profile maz-test
    --endpoint-url https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz-11
    --multi-az
```

Conversión de un almacenamiento de datos multi-AZ en un almacenamiento de datos single-AZ

Al convertir un almacenamiento de datos multi-AZ en un almacenamiento de datos single-AZ, su almacenamiento de datos no recibirá la garantía de SLA del 99,99 % que ofrece la opción multi-AZ. El rendimiento de una consulta individual seguirá siendo el mismo, pero el rendimiento general se verá afectado porque los recursos de computación de la segunda zona de disponibilidad no estarán disponibles. Tiene la opción de habilitar el escalado simultáneo para escalar automáticamente el rendimiento y lograr un rendimiento uniforme, incluso con single-AZ.

> **Note**
>
> Amazon Redshift no le permitirá dividir los recursos de computación existentes al pasar de single-AZ a multi-AZ, ni viceversa. Esta operación no se admite para mantener un rendimiento uniforme de las consultas individuales.

Mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Provisioned clusters dashboard (Panel de clústeres aprovisionados) y elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la

Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.

3. Elija el clúster que desea convertir en implementación multi-AZ. Se abrirá la página de detalles del clúster.
4. En Acciones, elija Desactivar multi-AZ. Aparecerá la página de resumen de modificaciones. Haga clic en Desactivar multi-AZ.

Uso de la AWS Command Line Interface

- En la AWS CLI, utilice el comando `modify-cluster` y el parámetro `no-multi-az` de la siguiente manera.

```
aws redshift modify-cluster
    --profile maz-test
    --endpoint-url  https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz-11
    --no-multi-az
```

Después de convertir el almacenamiento de datos a single-AZ, perderá la garantía del SLA del 99,99 %. El rendimiento general también se verá afectado. Cuando se guarden los cambios, podrá ver los detalles en la página de detalles del clúster.

Cambio del tamaño de un almacenamiento de datos multi-AZ

Puede cambiar el tamaño de un almacenamiento de datos multi-AZ y especificar un número de nodos o un tipo de nodo diferente al de la configuración actual del almacenamiento de datos.

Mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Provisioned clusters dashboard (Panel de clústeres aprovisionados) y elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.

3. Elija el clúster en el que desea cambiar el tamaño del almacenamiento de datos multi-AZ. Se abrirá la página de detalles del clúster.
4. En Actions (Acciones), elija Resize (Cambiar tamaño). Se abrirá la página Resize cluster (Cambiar tamaño del clúster).
5. Siga las instrucciones de la página. Puede cambiar el tamaño del clúster ahora, una vez en un momento específico, o aumentar y disminuir el tamaño del clúster según una programación.
6. En Nueva configuración, elija uno de los tipos de nodo RA3 de la lista desplegable Tipo de nodo.
7. Haga clic en Cambiar el tamaño del clúster.

Uso de la AWS Command Line Interface

Para cambiar el tamaño de un almacenamiento de datos multi-AZ mediante la AWS Command Line Interface

- En la AWS CLI, utilice el comando `resize-cluster` para cambiar el número de nodos para una única zona de disponibilidad de la siguiente manera.

```
aws redshift resize-cluster \
    --cluster-identifier test-maz-11
    --cluster-type multi-node
    --node-type ra3.4xlarge
    --number-of-nodes 6
```

Configuración de una multi-AZ para un almacenamiento de datos restaurado a partir de una instantánea

También puede crear un clúster multi-AZ nuevo restaurándolo a partir de una instantánea.

Mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres), Snapshots (Instantáneas) y, a continuación, elija la instantánea que desea usar.
3. Elija Restore snapshot (Restaurar instantánea) y Restore to a provisioned cluster (Restaurar a un clúster aprovisionado).

4. Ingrese las propiedades del clúster. Para obtener información general acerca de cómo crear un clúster de base de datos, consulte Creación de un clúster.
5. Elija uno de los tipos de nodo RA3 de la lista desplegable Node type (Tipo de nodo). La opción de configuración AZ solo está disponible si se elige un tipo de nodo RA3.
6. En Configuración AZ, elija Multi-AZ.
7. En Número de nodos por zona de disponibilidad, introduzca al menos dos nodos para el clúster.
8. Tiene la opción de cargar datos de muestra o de trasladar sus propios datos:

   - En Sample data (Datos de muestra), elija Load sample data (Cargar datos de muestra) para cargar el conjunto de datos de muestra en el clúster de Amazon Redshift. Amazon Redshift carga el conjunto de datos de muestra Tickit en la base de datos dev y el esquema public predeterminados. Amazon Redshift carga automáticamente el conjunto de datos de muestra en el clúster de Amazon Redshift. Puede comenzar a utilizar el editor de consultas v2 para consultar datos.
   - Para llevar sus propios datos al clúster de Amazon Redshift, siga los pasos que se indican en Traer sus propios datos a Amazon Redshift.
9. Desplácese hasta Additional configurations (Configuraciones adicionales), expanda Network and security (Red y seguridad) y asegúrese de aceptar valor predeterminado de Cluster subnet group (Grupo de subredes del clúster) o elija otro. Si elige otro grupo de subredes del clúster, asegúrese de que haya tres zonas de disponibilidad en el grupo de subredes que ha seleccionado.
10. En Additional configurations (Configuraciones adicionales), expanda Database configurations (Configuraciones de base de datos).
11. En Database encryption (Cifrado de bases de datos), para usar una clave de KMS personalizada que no sea la clave AWS Key Management Service predeterminada, haga clic en Customize encryption settings (Personalizar la configuración de cifrado). Esta opción está seleccionada de forma predeterminada.
12. En Choose an KMS key (Elegir una clave de KMS), puede elegir una clave de AWS Key Management Service o ingresar un ARN. O puede hacer clic en Crear una clave de AWS Key Management Service en la consola de AWS Key Management Service. Para obtener más información sobre la creación de claves KMS, consulte Creating Keys (Creación de claves) en la Guía para desarrolladores de AWS Key Management Service.
13. Haga clic en Restore cluster from snapshot (Restaurar clúster a partir de una instantánea). Cuando la creación del clúster se realice correctamente, podrá ver los detalles en la página de detalles del clúster.

Uso de la AWS Command Line Interface

- En la AWS CLI, use el comando `restore-from-cluster-snapshot` de la siguiente manera.

```
aws redshift restore-from-cluster-snapshot
--region eu-west-1
--multi-az
--snapshot-identifier test-snap1
--cluster-identifier test-saz-11
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

Fallo en la implementación multi-AZ

Su almacenamiento de datos multi-AZ es un conjunto de recursos de computación implementados simultáneamente en dos zonas de disponibilidad. Los recursos de computación implementados en la zona de disponibilidad principal se denominan recursos de computación principales y los de las zonas de disponibilidad secundarias se denominan recursos de computación secundarios. Un almacenamiento de datos multi-AZ puede recuperarse automáticamente sin la intervención del usuario en el caso poco probable, por ejemplo, de que falle una zona de disponibilidad o una infraestructura. El proceso de recuperación implica la conmutación por error de la computación principal a la secundaria y la designación de los recursos de computación secundarios como principales. Además, los nuevos recursos de computación secundarios se aprovisionan en una tercera zona de disponibilidad. El proceso de recuperación automática se mide en términos de RTO y RPO.

- Objetivo de tiempo de recuperación (RTO) – El tiempo que tarda un sistema en volver a un estado operativo después de un desastre. En otras palabras, el RTO mide el tiempo de inactividad.
- Objetivo de punto de recuperación (RPO) – La cantidad de datos que se pueden perder (medidos en el tiempo). En el caso de un almacenamiento de datos multi-AZ de Amazon Redshift, el RPO suele ser cero, ya que todos los datos se almacenan en Amazon Redshift Managed Storage (RMS), respaldado por Amazon Simple Storage Service, que es de larga duración y disponibilidad de forma predeterminada.

> **Note**
>
> El rendimiento de una consulta individual no cambiará tras una conmutación por error. El rendimiento general del almacenamiento de datos se reducirá durante un breve período

debido a la falta de disponibilidad de los recursos de computación en una de las zonas de disponibilidad. Sin embargo, Amazon Redshift adquirirá automáticamente capacidad en otra zona de disponibilidad para garantizar que se restaure la misma capacidad de procesamiento del almacenamiento de datos.

Además del proceso de recuperación automática, también puede activar este proceso manualmente para su almacenamiento de datos mediante la opción Computación principal de conmutación por error. Puede usar este enfoque para probar cómo ayudaría la opción Multi-AZ a su aplicación para lograr una mayor disponibilidad y mejor continuidad.

Mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. Realice una de las acciones siguientes:
   - En el menú de navegación, elija Clusters (Clústeres). En Clusters (Clústeres), elija un clúster. Se abrirá la página de detalles del clúster.
   - En el panel de clústeres, elija un clúster.
3. En Acciones, elija Computación principal de conmutación por error.
4. Cuando se le solicite, haga clic en Confirm (Confirmar).

Uso de la AWS Command Line Interface

- En la AWS CLI, use el comando `failover-primary-compute` de la siguiente manera.

```
aws redshift failover-primary-compute
    --profile maz-test
    --endpoint-url  https://redshift.eu-west-1.amazonaws.com
    --region eu-west-1
    --cluster-identifier test-maz-11
```

Una vez confirmada la operación anterior, Amazon Redshift realizará los mismos pasos que en una recuperación automática debido a un fallo en una zona de disponibilidad o infraestructura. El proceso hará que los nodos de computación de la zona de disponibilidad principal dejen de estar disponibles y los recursos de computación de la zona de disponibilidad secundaria sean designados

como la computación principal. Cuando la recuperación del clúster se complete correctamente, la implementación multi-AZ estará disponible. Su almacenamiento de datos multi-AZ también aprovisionará automáticamente nueva computación en una tercera zona de disponibilidad en cuanto esté disponible.

Durante este proceso, el estado del clúster en la consola se muestra como modificado durante todo el tiempo, ya que el clúster se recupera automáticamente y se vuelve a configurar según la configuración de implementación multi-AZ. El clúster puede aceptar nuevas conexiones inmediatamente. Es posible que se eliminen las conexiones existentes y las consultas en curso. Puede volver a intentarlas inmediatamente.

Monitoreo de consultas para multi-AZ

Puede ver la información sobre las consultas que se han ejecutado en los últimos siete días, independientemente del tipo, el tamaño y el estado (pausa o reanudación) del clúster.

Visualización de consultas y cargas para almacenamientos de datos multi-AZ

La información que se muestra en la página Queries and loads (Consultas y cargas) se rellena con información de las tablas del sistema de Amazon Redshift (vistas SYS_*). Esta información le permite mostrar información adicional sobre sus consultas y ofrece siete días consecutivos de retención. Los diagnósticos de consultas son más rápidos, lo que le permite filtrar los datos por base de datos, nombre de usuario o tipo de instrucción SQL. Para ver estos filtros adicionales y la información de todas las consultas que se han ejecutado, tenga en cuenta los siguientes requisitos previos:

- Debe conectarse a una base de datos mediante la elección de Connect to database (Conectar a base de datos).
- El usuario de base de datos debe tener los roles y permisos sys:operator o sys:monitor para poder supervisar las consultas. Para obtener información sobre los roles del sistema, consulte Roles definidos por el sistema de Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Verá estos filtros adicionales y la información de consulta una vez que se conecte a una base de datos.

Para mostrar los datos de rendimiento de consultas desde Queries and loads (Consultas y cargas)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

2. En el menú de navegación, elija Queries and loads (Consultas y cargas) para mostrar la lista de consultas de la cuenta.
3. Es posible que tenga que conectarse a una base datos para ver el filtro adicional. Si es necesario, haga clic en Connect to database (Conectar a base de datos) y siga las instrucciones para conectarse a una base de datos.

   Por defecto, la lista muestra consultas de todos sus clústeres durante las últimas 24 horas. Puede cambiar el alcance de los datos mostrados en la consola.

Para mostrar los datos de rendimiento de las consultas desde Query monitoring (Supervisión de consultas)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). En Clusters (Clústeres), seleccione un clúster.
3. Elija Query monitoring (Supervisión de consultas).
4. Según la configuración o la versión del clúster, es posible que deba conectarse a una base de datos para ver los filtros adicionales. Si es necesario, haga clic en Connect to database (Conectar a base de datos) y siga las instrucciones para conectarse a una base de datos.

Supervisión de una consulta en una implementación multi-AZ

Una implementación multi-AZ utiliza recursos de computación implementados en ambas zonas de disponibilidad y puede seguir funcionando en caso de que los recursos de una zona de disponibilidad determinada no estén disponibles. Todos los recursos de computación se utilizarán en todo momento. Esto permite el funcionamiento completo a través de dos zonas de disponibilidad de forma activa-activa tanto para operaciones de lectura como de escritura.

Puede consultar las vistas SYS_ en el esquema pg_catalog para supervisar el tiempo de ejecución de las consultas en una implementación multi-AZ. Las vistas SYS_ muestran las actividades de ejecución de las consultas o las estadísticas de los clústeres primario y secundario. Para obtener una lista de las vistas de monitoreo, consulte Vistas de monitoreo.

Siga estos pasos para supervisar el tiempo de ejecución de las consultas para cada zona de disponibilidad en la implementación multi-AZ:

1. Vaya a la consola de Amazon Redshift, conéctese a la base de datos de su implementación multi-AZ y ejecute consultas mediante el editor de consultas.
2. Ejecute cualquier consulta de muestra en la implementación multi-AZ de Amazon Redshift.
3. En el caso de una implementación multi-AZ, puede identificar una consulta y la zona de disponibilidad en la que se ejecuta mediante la columna compute_type de la tabla SYS_QUERY_HISTORY. primary significa consultas ejecutadas en el clúster principal de la implementación multi-AZ y secondary significa consultas ejecutadas en el clúster secundario de la implementación multi-AZ.

   La siguiente consulta utiliza la columna compute_type para supervisar una consulta.

```
select (compute_type) as compute_type, left(query_text, 50) query_text from
 sys_query_history order by start_time desc;

 compute_type | query_text
--------------+------------------------
   secondary  | select count(*) from t1;
```

Finalización de una consulta de clústeres

Finalización de una consulta de clústeres

El procedimiento se aplica a los clústeres multi-AZ y single-AZ.

Para terminar una consulta

También puede utilizar la página Queries (Consultas) para finalizar una consulta que esté en proceso.

El usuario de la base de datos debe tener el rol y los permisos sys:operator para finalizar una consulta en ejecución. Para obtener información sobre los roles del sistema, consulte Roles definidos por el sistema de Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Queries and loads (Consultas y cargas) para mostrar la lista de consultas de la cuenta.

3. Seleccione la consulta en ejecución que quiera finalizar en la lista, y luego seleccione Terminate query (Finalizar consulta).

Administración de clústeres a través de la consola

Para crear, modificar, redimensionar, eliminar y reiniciar clústeres o hacer una copia de seguridad de ellos, utilice la sección Clusters (Clústeres) de la consola de Amazon Redshift.

Para ver clústeres

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas. Si no tiene ningún clúster, seleccione Create cluster (Crear clúster) para crear uno.
3. Seleccione el nombre del clúster en la lista para ver más detalles sobre un clúster.

Temas

- Creación de un clúster
- Crear un clúster de vista previa
- Modificación de un clúster
- Eliminación de un clúster
- Reinicio de un clúster
- Redimensionamiento de un clúster
- Actualizar la versión de lanzamiento de un clúster
- Obtención de información acerca de la configuración del clúster
- Obtención de información general acerca del estado del clúster
- Crear una instantánea de un clúster
- Crear o editar una alarma de espacio en disco
- Uso de los datos de rendimiento del clúster

Creación de un clúster

Antes de crear un clúster, lea Información general de Amazon Redshift y Clústeres y nodos de Amazon Redshift.

Pasos para crear un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Seleccione Create cluster (Crear clúster) para crearlo.
4. Siga las instrucciones en la página de la consola para introducir las propiedades de la Cluster configuration (Configuración del clúster).

   En el siguiente paso, se describe una consola de Amazon Redshift que se ejecuta en una Región de AWS que admite los tipos de nodo RA3. Para obtener una lista de las Regiones de AWS que admiten los tipos de nodo RA3, consulte Información general sobre los tipos de nodo RA3 en la Guía de administración de Amazon Redshift.

   Si no sabe cuál sería el tamaño adecuado para el clúster, elija Help me choose (Ayúdeme a elegir). De este modo, se inicia una calculadora de tamaño que le hace preguntas sobre el tamaño y las características de consulta de los datos que planea almacenar en el almacenamiento de datos. Si conoce el tamaño requerido para su clúster (es decir, el tipo de nodo y la cantidad de nodos), elija I'll choose (Yo elegiré). A continuación, elija el Node type (Tipo de nodo) y la cantidad de Nodes (nodos) para determinar el tamaño del clúster para la prueba de concepto.

   > **Note**
   >
   > Si su organización reúne los requisitos necesarios y su clúster se crea en una Región de AWS donde no está disponible Amazon Redshift sin servidor, es posible que pueda crear un clúster en el programa de prueba gratuita de Amazon Redshift. Elige Producción o Prueba gratuita para responder la pregunta ¿Para qué planifica usar este clúster? Si elige Prueba gratuita, cree una configuración con el tipo de nodo dc2.large. Para obtener más información sobre la elección de una prueba gratuita, consulte Prueba gratuita de Amazon Redshift. Para obtener una lista de las Regiones de AWS

donde Amazon Redshift sin servidor está disponible, consulte los puntos de conexión enumerados para la API de Redshift sin servidor en la Referencia general de Amazon Web Services.

5. En la sección Configuración de la base de datos, especifique un valor para Nombre de usuario del administrador. En Contraseña de administrador, puede elegir entre las siguientes opciones:

   - Generar contraseña: use una contraseña generada por Amazon Redshift.
   - Añadir manualmente una contraseña de administrador: use su propia contraseña.
   - Administrar las credenciales de administrador en AWS Secrets Manager: Amazon Redshift usa AWS Secrets Manager para generar y administrar su contraseña de administrador. El uso de AWS Secrets Manager para generar y administrar el secreto de la contraseña conlleva un gasto. Para obtener información sobre precios de AWS Secrets Manager, consulte Precios de AWS Secrets Manager.

6. (Opcional) Siga las instrucciones en la página de la consola para introducir las propiedades de Cluster permissions (Permisos del clúster). Proporcione permisos de clúster si su clúster necesita acceder a otros servicios de AWS por usted, por ejemplo, para cargar datos desde Amazon S3.
7. Seleccione Create cluster (Crear clúster) para crearlo. El clúster tardará varios minutos antes de estar listo para su uso.

Configuraciones adicionales

Cuando cree un clúster, puede especificar propiedades adicionales para personalizarlo. Puede encontrar más información sobre algunas de estas propiedades en la siguiente lista.

Tipo de dirección IP

Elija el tipo de dirección IP de su clúster. Puede elegir que sus recursos se comuniquen solo a través del protocolo de direccionamiento IPv4 o elegir el modo de doble pila, que permite que sus recursos se comuniquen a través de IPv4 e IPv6. Esta característica solo está disponible en las regiones AWS GovCloud (Este de EE. UU.) y AWS GovCloud (Oeste de EE. UU.). Para obtener más información sobre las regiones de AWS, consulte Regiones y zonas de disponibilidad.

Virtual Private Cloud (VPC) (Nube virtual privada [VPC])

Elija una VPC que tenga un grupo de subredes de clústeres. Después de crear el clúster, el grupo de subredes de clústeres no se puede cambiar.

Grupos de parámetros

Elija un grupo de parámetros para asociarlo al clúster. Si no lo elige, el clúster usará el grupo de parámetros predeterminado.

Cifrado

Elija si desea cifrar todos los datos dentro del clúster y sus instantáneas. Si deja el valor predeterminado, None (Ninguno), no se habilitará el cifrado. Si desea habilitar el cifrado, elija si desea utilizar AWS Key Management Service (AWS KMS) o un módulo de seguridad de hardware (HSM), y establezca la configuración correspondiente. Para obtener información acerca de cifrado en Amazon Redshift, consulte Cifrado de la base de datos de Amazon Redshift.

- KMS

  Elija Utilizar AWS Key Management Service (AWS KMS) si desea habilitar el cifrado y usar AWS KMS para administrar la clave de cifrado. No olvide elegir la clave que se debe utilizar. Puede elegir una clave predeterminada, una clave de la cuenta actual o una clave de otra cuenta.

  > **Note**
  >
  > Si desea utilizar una clave de otra cuenta de AWS, ingrese el nombre de recurso de Amazon (ARN) de la clave que se debe utilizar. Debe tener permisos para usar la clave. Para obtener más información acerca del acceso a las claves en AWS KMS, consulte Control del acceso a sus claves en la Guía para desarrolladores de AWS Key Management Service.

  Para obtener más información acerca de las claves de cifrado de AWS KMS en Amazon Redshift, consulte Cifrado de la base de datos de Amazon Redshift con AWS KMS.

- HSM

  Seleccione HSM si desea habilitar el cifrado y utilizar un módulo de seguridad de hardware (HSM) para administrar la clave de cifrado.

  Si selecciona HSM, elija valores de HSM Connection (conexión de HSM) y HSM Client Certificate (Certificado de cliente de HSM). Estos valores se necesitan para que Amazon Redshift y el HSM establezcan una conexión segura sobre la cual pueda pasar la clave del clúster. La conexión del HSM y el certificado de cliente se deben configurar en Amazon

Redshift antes de lanzar un clúster. Para obtener más información acerca de cómo configurar las conexiones del HSM y los certificados de clientes, consulte Cifrado de Amazon Redshift con módulos de seguridad de hardware.

Pista de mantenimiento

Puede elegir si la versión del clúster utilizada es la pista Actual, Anterior o, a veces, la de Previsualización.

Supervisión

Puede elegir si quiere crear alarmas de CloudWatch.

Configurar instantáneas entre regiones

Puede elegir si quiere habilitar las instantáneas entre regiones.

Automated Snapshot Retention Period (Periodo de retención de instantánea automatizada)

Puede elegir el número de días para retener estas instantáneas en un plazo de 35 días. Si el tipo de nodo es DC2 o DS2, puede elegir cero (0) días para no crear instantáneas automatizadas.

Manual snapshot retention period (Periodo de retención de instantáneas manuales)

Puede elegir el número de días o `Indefinitely` para retener estas instantáneas.

Crear un clúster de vista previa

Puede crear un clúster de Amazon Redshift en versión preliminar para probar las nuevas características de Amazon Redshift. No puede usar esas características en producción ni mover su clúster de versión preliminar a un clúster de producción o a un clúster de otra pista. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

Para crear un clúster en versión preliminar

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Provisioned clusters dashboard (Panel de clústeres aprovisionados) y elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.

3. Aparece un banner en la página de la lista Clusters (Clústeres) que presenta la versión preliminar. Elija el botón Create preview cluster (Crear clúster de versión preliminar para abrir la página de creación de clústeres.
4. Ingrese las propiedades del clúster. Elija en Preview track (Pista de versión preliminar) la pista de versión preliminar que contenga las características que desea probar. Le recomendamos que ingrese un nombre para el clúster que indique que se encuentra en una pista de versión preliminar. Elija las opciones de su clúster, incluidas las etiquetadas como -preview (-versión preliminar), para las características que desee probar. Para obtener más información sobre la creación de clústeres, consulte Creación de un clúster en la Guía de administración de clústeres de Amazon Redshift.
5. Elija Crear clúster de vista previa para crear un clúster de vista previa.

   > **Note**
   >
   > La pista `preview_2023` es la pista de versión preliminar más reciente disponible. Esta pista solo admite la creación de clústeres con tipos de nodo RA3. No se admiten los tipos de nodo DC2 y DS2 ni ningún tipo de nodo anterior.

6. Cuando el clúster de versión preliminar esté disponible, utilice su cliente de SQL para cargar y consultar datos.

Para obtener información sobre la versión preliminar en grupos de trabajo de Redshift sin servidor, consulte Crear un grupo de trabajo de vista previa.

Modificación de un clúster

Cuando modifica un clúster, se aplican cambios de inmediato a las siguientes opciones:

- VPC security groups
- Publicly accessible (Accesible públicamente)
- Admin user password (Contraseña del usuario administrador)
- Conexión del HSM
- HSM Client Certificate (Certificado del cliente HSM)
- Información de mantenimiento
- Snapshot preferences (Preferencias de instantáneas)

Los cambios en las siguientes opciones entran en vigor solamente después de reiniciar el clúster:

- Identificador de clúster

  Amazon Redshift reinicia el clúster de forma automática cuando cambia el valor de la opción Cluster identifier (Identificador del clúster).
- Enhanced VPC Routing

  Amazon Redshift reinicia el clúster de forma automática cuando cambia el valor de la opción Enhanced VPC routing (Enrutamiento de VPC mejorado).
- Grupo de parámetros del clúster
- Tipo de dirección IP

  Esta característica solo está disponible en las regiones AWS GovCloud (Este de EE. UU.) y AWS GovCloud (Oeste de EE. UU.). Para obtener más información sobre las regiones de AWS, consulte Regiones y zonas de disponibilidad.

Si disminuye el período de retención automatizado de snapshots, se eliminarán las snapshots automatizadas existentes cuya configuración no se ajusten al nuevo período de retención. Para obtener más información, consulte Instantáneas y copias de seguridad de Amazon Redshift.

Para obtener más información acerca de propiedades de clúster, consulte Configuraciones adicionales.

Pasos para modificar un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Elija el clúster que se va a modificar.
4. Elija Editar. Se abrirá la página Edit cluster (Editar clúster).
5. Actualizar propiedades del clúster. Algunas de las propiedades que puede modificar son:
   - Identificador de clúster
   - Retención de instantáneas
   - Reubicación de los clústeres

Para editar la configuración de Red y seguridad, Mantenimiento y Configuraciones de la base de datos, la consola proporciona enlaces a la pestaña de detalles del clúster correspondiente.

6. Elija Guardar cambios.

Eliminación de un clúster

Si ya no necesita su clúster, puede eliminarlo. Si planifica aprovisionar un nuevo clúster con los mismos datos y la misma configuración que el que está eliminado, necesitará una instantánea manual. Con una instantánea manual, puede restaurar la instantánea más tarde y continuar utilizando el clúster. Si elimina el clúster, pero no crea una instantánea manual final, se eliminarán los datos del clúster. En ambos casos, las snapshots automatizadas se eliminan luego de que se elimina el clúster, pero las snapshots manuales se conservan hasta que usted las elimine. Es posible que se apliquen tarifas de almacenamiento de Amazon Simple Storage Service para las instantáneas manuales en función de la cantidad de almacenamiento que tenga disponible para las instantáneas de Amazon Redshift en sus clústeres. Para obtener más información, consulte Cierre y eliminación de clústeres.

Al eliminar un clúster, también se eliminan todos los secretos de AWS Secrets Manager asociados.

Para eliminar un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Elija el clúster que quiere eliminar.
4. En Actions (Acciones), seleccione Delete (Eliminar). Se abrirá la página Delete cluster (Eliminar clúster).
5. Seleccione Delete cluster (Eliminar clúster).

Reinicio de un clúster

Cuando reinicia un clúster, el estado se establece en `rebooting` y se crea un evento de clúster cuando se completa el reinicio. Se aplican todas las modificaciones pendientes al clúster en este reinicio.

Pasos para reiniciar de un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Elija el clúster que quiere reiniciar.
4. En Actions (Acciones), elija Reboot cluster (Reiniciar clúster). Se abrirá la página Reboot cluster (Reiniciar clúster).
5. Seleccione Reboot cluster (Reiniciar clúster).

Redimensionamiento de un clúster

Cuando redimensione un clúster, especifique la cantidad de nodos o el tipo de nodo diferente de la configuración actual del clúster. Mientras el clúster está en proceso de redimensionamiento, no puede ejecutar consultas de escritura de lectura/escritura en el clúster; solo puede ejecutar consultas de solo lectura.

Para obtener más información acerca del redimensionamiento de clústeres, incluido el avance del proceso de redimensionamiento de clústeres utilizando diferentes enfoques, consulte Cambio de tamaño de clústeres.

Pasos para redimensionar un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Elija el clúster al que quiere cambiar el tamaño.
4. En Actions (Acciones), elija Resize (Cambiar tamaño). Se abrirá la página Resize cluster (Cambiar tamaño del clúster).
5. Siga las instrucciones de la página. Puede cambiar el tamaño del clúster ahora, una vez en un momento específico, o aumentar y disminuir el tamaño del clúster según una programación.
6. En función de sus opciones, elija Resize now (Cambiar tamaño ahora) o Schedule resize (Programar cambio de tamaño).

Si tiene nodos reservados, por ejemplo, nodos reservados DS2, puede actualizarlos a nodos reservados RA3. Puede hacer esto cuando utiliza la consola para restaurar desde una instantánea

o para realizar un redimensionamiento elástico. Puede utilizar la consola para guiarse a través de este proceso. Para obtener más información acerca de la actualización a nodos RA3, consulte Actualización a tipos de nodo RA3.

Actualizar la versión de lanzamiento de un clúster

Puede actualizar la versión de mantenimiento de un clúster que tiene un valor de Release Status (Estado de la versión) de New release available (Nueva actualización disponible). Puede optar por actualizar la versión de mantenimiento inmediatamente o en el siguiente período de mantenimiento.

> **Important**
>
> Si actualiza inmediatamente, el clúster está sin conexión hasta que finalice la actualización.

Para actualizar un clúster a una nueva versión de lanzamiento

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Elija el clúster que quiere actualizar.
4. En Actions (Acciones), seleccione Upgrade cluster version (Actualizar versión del clúster). Aparecerá la página Upgrade cluster version (Actualizar versión del clúster).
5. Siga las instrucciones de la página.
6. Seleccione Upgrade cluster version (Actualizar versión del clúster).

Obtención de información acerca de la configuración del clúster

Para mostrar información sobre un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Supervisión de consultas), Databases (Bases de datos), Datashares (Recursos compartidos de datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).

3. Seleccione cada pestaña para ver más información.

Obtención de información general acerca del estado del clúster

Para ver el estado de un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Vea el estado del clúster en la columna Status (Estado).

Crear una instantánea de un clúster

Para crear una instantánea de un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).
3. Seleccione el clúster del que quiere crear una instantánea.
4. En Actions (Acciones), seleccione Create alias (Crear alias). Aparecerá la página Create snapshot (Crear instantánea).
5. Siga las instrucciones de la página.
6. Seleccione Create snapshot (Crear instantánea).

Crear o editar una alarma de espacio en disco

Para crear una alarma de uso de espacio en disco para un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Alarms (Alarmas).
3. En Actions (Acciones), seleccione Create alarm (Crear alarma). Aparecerá la página Create alarm (Crear alarma).
4. Siga las instrucciones de la página.

5. Elija Crear alarma.

Uso de los datos de rendimiento del clúster

En la consola, puede trabajar con el rendimiento del clúster en la pestaña Cluster performance (Rendimiento del clúster) de la página de detalles del clúster.

Administración de clústeres mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la AWS CLI para administrar clústeres en Amazon Redshift.

- cancel-resize
- create-cluster
- delete-cluster
- describe-clusters
- describe-cluster-versions
- describe-node-configuration-options
- describe-orderable-cluster-options
- describe-resize
- modify-cluster
- pause-cluster
- reboot-cluster
- resize-cluster
- resume-cluster

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar clústeres.

- CancelResize
- CreateCluster
- DeleteCluster
- DescribeClusters

- DescribeClusterVersions
- DescribeNodeConfigurationOptions
- DescribeResize
- DescribeOrderableClusterOptions
- ModifyCluster
- PauseCluster
- RebootCluster
- ResizeCluster
- ResumeCluster

Administración de clústeres en una VPC

Temas

- Información general
- Creación de un clúster en una VPC
- Administración de grupos de seguridad de VPC para un clúster
- Configuración de las opciones de comunicación del grupo de seguridad para un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor
- Cómo funciona Amazon Redshift con el uso compartido de VPC para los recursos de AWS
- Grupos de subredes del clúster de Amazon Redshift

Información general

Amazon Redshift admite las plataformas EC2-VPC y EC2-Classic para lanzar un clúster en una nube virtual privada (VPC) en función del servicio de Amazon VPC. Para obtener más información, consulte Usar EC2-VPC al crear el clúster.

> **Note**
>
> Amazon Redshift no admite el lanzamiento de clústeres en las VPC de tenencia dedicada. Para obtener más información, consulte Instancias dedicadas en la Guía del usuario de Amazon VPC.

Cuando aprovisiona un clúster en la VPC, debe realizar lo siguiente:

- Proporcione la información de la VPC.

  Cuando solicite a Amazon Redshift que cree un clúster en su VPC, debe proporcionar la información de su VPC mediante la creación de un grupo de subredes del clúster. Esta información incluye el ID de la VPC y una lista de subredes en su VPC. Cuando lance un clúster, debe proporcionar el grupo de subredes del clúster para que Amazon Redshift pueda aprovisionar su clúster en una de las subredes de la VPC. Para obtener más información acerca de la creación de grupos de subredes en Amazon Redshift, consulte Grupos de subredes del clúster de Amazon Redshift. Para obtener más información acerca de la configuración de la VPC, consulte Introducción a Amazon VPC en la Guía de introducción a Amazon VPC.
- Si lo desea, puede configurar las opciones de acceso público.

  Si configura su clúster para que sea de acceso público, Amazon Redshift usa una dirección IP elástica para la dirección IP externa. Una dirección IP elástica es una dirección IP estática. Con ella, puede cambiar la configuración subyacente sin afectar la dirección IP que los clientes utilizan para conectarse al clúster. Esto puede ser útil para situaciones como la recuperación después de un error. La creación de una dirección IP elástica depende de la configuración de reubicación de la zona de disponibilidad. Dispone de dos opciones:

  1. Si tiene activada la reubicación de zonas de disponibilidad y desea habilitar el acceso público, no especifique una dirección IP elástica. Se asigna una dirección IP elástica administrada por Amazon Redshift. Está asociada a su cuenta de AWS.
  2. Si tiene desactivada la reubicación de zonas de disponibilidad y desea habilitar el acceso público, puede optar por crear una dirección IP elástica para la VPC de Amazon EC2 antes de lanzar su clúster de Amazon Redshift. Si no crea una dirección IP, Amazon Redshift proporciona una dirección IP elástica configurada para utilizarla en la VPC. Amazon Redshift administra esta dirección IP elástica y no está asociada a su cuenta de AWS.

  Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2 para instancias de Linux.

  En algunos casos, es posible que tenga un clúster de acceso público en una VPC al que desee conectarse con la dirección IP privada desde la VPC. Si es el caso, establezca los siguientes parámetros de VPC en `true`:

  - `DNS resolution`
  - `DNS hostnames`

Supongamos que tiene un clúster de acceso público en una VPC pero no establece estos parámetros en `true` en la VPC. En estos casos, las conexiones realizadas desde la VPC se resuelven en la dirección IP elástica del clúster en lugar de la dirección IP privada. Recomendamos que establezca estos parámetros en `true` y utilice la dirección IP privada para un clúster de acceso público cuando se conecte desde la VPC. Para obtener más información, consulte Uso de DNS con su VPC en la Guía del usuario de Amazon VPC.

> **Note**
>
> Si tiene un clúster de acceso público existente en una VPC, las conexiones realizadas desde la VPC seguirán utilizando la dirección IP elástica para conectarse al clúster hasta que cambie el tamaño del clúster. Esto ocurrirá incluso con los anteriores parámetros establecidos. Los clústeres nuevos seguirán el nuevo comportamiento de uso de la dirección IP privada cuando se conecten al clúster de acceso público desde la misma VPC.

La dirección IP elástica es una dirección IP externa para acceder al clúster fuera de la VPC. No está relacionada con las direcciones IP públicas y privadas del nodo del clúster que se muestran en la consola de Amazon Redshift, en Connection details (Detalles de conexión). Las direcciones IP públicas y privadas del nodo del clúster aparecen sin importar que el clúster sea de acceso público o no. Se utilizan únicamente en determinadas circunstancias para configurar reglas de entrada en el host remoto. Estas circunstancias se producen cuando se cargan datos desde una instancia de Amazon EC2 u otro alojamiento remoto utilizando una conexión Secure Shell (SSH). Para obtener más información, consulte Paso 1: Recuperar la clave pública del clúster y las direcciones IP del nodo del clúster en la Guía para desarrolladores de bases de datos de Amazon Redshift.

La opción de asociar un clúster a una dirección IP elástica está disponible cuando se crea el clúster o se restaura el clúster desde una instantánea. En algunos casos, es posible que quiera asociar el clúster con una dirección IP elástica o cambiar una dirección IP elástica que está asociada con el clúster. Para adjuntar una dirección IP elástica después de crear el clúster, primero actualice el clúster para que no sea accesible públicamente, y después haga que sea accesible públicamente y agregue una dirección IP elástica en la misma operación.

- Asocie un grupo de seguridad de VPC.

  Luego, se concede acceso de entrada mediante un grupo de seguridad de VPC. Este grupo de seguridad de VPC debe permitir el acceso al clúster a través del puerto de la base de datos de

modo que pueda conectarse mediante las herramientas de cliente SQL. Puede configurar esto con antelación o agregarle reglas después de lanzar el clúster. Para obtener más información, consulte Configuración de las opciones de comunicación del grupo de seguridad para clústeres de Amazon Redshift, que proporciona orientación sobre la configuración de las reglas de entrada y salida entre un cliente y un clúster aprovisionado o un grupo de trabajo de Amazon Redshift sin servidor. Otro recurso que le ayudará a comprender los grupos de seguridad es Seguridad en la VPC en la Guía del usuario de Amazon VPC. Tenga en cuenta que no puede utilizar los grupos de seguridad del clúster de Amazon Redshift para conceder acceso entrante al clúster.

Para obtener más información acerca del uso de clústeres en una VPC, consulte Creación de un clúster en una VPC.

Restauración de una instantánea de un clúster en VPC

Una instantánea de un clúster en VPC solo se puede restaurar en una VPC, no fuera de esta. Puede restaurarla en la misma VPC o en otra VPC de la cuenta. Para obtener más información acerca de las instantáneas, consulte Instantáneas y copias de seguridad de Amazon Redshift.

Creación de un clúster en una VPC

Los siguientes son los pasos generales sobre cómo puede implementar un clúster en su nube virtual privada (VPC).

Creación de un clúster en una VPC

1. Configure una VPC.

   Puede crear el clúster en la VPC predeterminada para la cuenta, si la cuenta tiene una, o en una VPC que haya creado. Para obtener más información, consulte Usar EC2-VPC al crear el clúster. Para crear una VPC, consulte Crear una VPC en la Guía del usuario de Amazon VPC. Anote el identificador de la VPC, la subred y la zona de disponibilidad de la subred. Necesitará esta información para lanzar el clúster.

   > **Note**
   >
   > Debe tener por lo menos una subred definida en la VPC para que pueda agregarla al grupo de subredes del clúster en el siguiente paso. Para obtener más información

acerca de cómo agregar una subred a su VPC, consulte Agregar una subred a su VPC en la Guía del usuario de Amazon VPC.

2. Cree un grupo de subredes del clúster de Amazon Redshift para determinar qué subred puede utilizar su clúster de Amazon Redshift en la VPC.

   Puede crear un grupo de subredes del clúster mediante la consola de Amazon Redshift o mediante programación. Para obtener más información, consulte Grupos de subredes del clúster de Amazon Redshift.

3. Autorice el acceso para conexiones entrantes en un grupo de seguridad de VPC que vaya a asociar con el clúster.

   Puede habilitar un cliente fuera de la VPC (en Internet público) para conectarse al clúster. Para ello, va a asociar el clúster con un grupo de seguridad de VPC que otorga acceso entrante al puerto que utilizó cuando lanzó el clúster. Si desea obtener ejemplos de las reglas del grupo de seguridad, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon VPC.

4. Siga los pasos de Introducción a Amazon Redshift en la Guía de introducción a Amazon Redshift para crear un clúster. Realice las siguientes modificaciones cuando cree un clúster:

   - Para mostrar la sección Additional configurations (Configuraciones adicionales), deshabilite Use defaults (Usar valores predeterminados).
   - En la sección Network and security (Red y seguridad), especifique la Virtual private cloud (VPC) (Nube virtual privada [VPC]), el Cluster subnet group (Grupo de subredes del clúster) y el VPC security group (Grupo de seguridad de VPC) que haya configurado.

Ahora ya puede utilizar el clúster. Puede seguir los pasos de introducción para probar el clúster mediante la carga de datos de ejemplo y la prueba de consultas de ejemplo.

Administración de grupos de seguridad de VPC para un clúster

Cuando aprovisiona un clúster de Amazon Redshift, se bloquea de forma predeterminada para que nadie pueda obtener acceso a él. Para concederle a otros usuarios acceso de entrada a un clúster de Amazon Redshift, debe asociar el clúster a un grupo de seguridad. Si está en la plataforma de EC2-VPC, puede utilizar un grupo de seguridad de Amazon VPC existente o definir uno nuevo. Luego lo asociará a un clúster como se describe a continuación. Si está en la plataforma EC2-Classic, defina un grupo de seguridad de clúster y asócielo a un clúster. Para obtener más

información acerca del uso de grupos de seguridad de clúster en la plataforma EC2-Classic, consulte Grupos de seguridad del clúster de Amazon Redshift.

Un grupo de seguridad de VPC está formado por un conjunto de reglas que controlan el acceso a una instancia en la VPC, como el clúster. Las reglas individuales establecen el acceso en función de los rangos de direcciones IP o de otros grupos de seguridad de VPC. Cuando asocia un grupo de seguridad de VPC a un clúster, las reglas que están definidas en el grupo de seguridad de VPC controlan el acceso al clúster.

Cada clúster que aprovisione en la plataforma EC2-VPC tiene uno o más grupos de seguridad de Amazon VPC asociados a él. Amazon VPC proporciona un grupo de seguridad de VPC llamado “default” (predeterminado) que se crea automáticamente junto con la VPC. Cada clúster que se lanza en la VPC se asocia automáticamente al grupo de seguridad de VPC predeterminado si no especifica un grupo de seguridad de VPC diferente cuando crea el clúster. Puede asociar un grupo de seguridad de VPC a un clúster cuando crea el clúster o puede asociarlo más adelante mediante la modificación del clúster.

La tabla siguiente describe las reglas predeterminadas para el grupo de seguridad de VPC predeterminado.

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound traffic

Puede cambiar las reglas para el grupo de seguridad de VPC predeterminado según las necesidades del clúster de Amazon Redshift.

Si el grupo de seguridad de VPC predeterminado es suficiente para el usuario, no es necesario que cree más. No obstante, de forma opcional, puede crear grupos de seguridad de VPC adicionales para administrar mejor el acceso de entrada al clúster. Por ejemplo, suponga que está ejecutando un servicio en un clúster de Amazon Redshift y tiene varios niveles de servicio diferentes que proporciona a los clientes. Si no desea proporcionar el mismo acceso a todos los niveles de servicio, es posible que desee crear grupos de seguridad de VPC independientes, uno para cada nivel de servicio. Luego puede asociar estos grupos de seguridad de VPC al clúster.

Puede crear hasta 100 grupos de seguridad de VPC para una VPC y asociar un grupo de seguridad de VPC con muchos clústeres. No obstante, solo puede asociar hasta cinco grupos de seguridad de VPC con un clúster determinado.

Amazon Redshift aplica los cambios a un grupo de seguridad de VPC de inmediato. Por lo que si asoció un grupo de seguridad de VPC a un clúster, las reglas de acceso de entrada al clúster en el grupo de seguridad de VPC actualizado se aplican de inmediato.

Puede crear y modificar grupos de seguridad de VPC en https://console.aws.amazon.com/vpc/. También puede administrar grupos de seguridad de VPC mediante programación con la AWS CLI, la CLI de Amazon EC2 y las AWS Tools for Windows PowerShell. Para obtener más información acerca del uso de grupos de seguridad de VPC, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.

Configuración de las opciones de comunicación del grupo de seguridad para un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor

Este tema lo ayuda a configurar sus grupos de seguridad para enrutar y recibir el tráfico de red adecuadamente. A continuación, se exponen un par de casos de uso habituales:

- Ha activado la accesibilidad pública para un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor, pero no recibe tráfico. Para ello, debe configurar una regla de entrada para permitir que le llegue tráfico desde Internet.
- Su clúster o grupo de trabajo no es de acceso público y utiliza el grupo de seguridad de VPC predeterminado y preconfigurado de Redshift para permitir el tráfico entrante. Pero usted tiene la necesidad de utilizar un grupo de seguridad distinto del predeterminado y este grupo de seguridad personalizado no permite el tráfico entrante. Debe configurarlo para permitir la comunicación.

En las secciones siguientes encontrará ayuda para elegir la respuesta correcta para cada caso de uso y se le mostrará cómo configurar el tráfico de red según sus necesidades. Opcionalmente, puede utilizar los pasos para configurar la comunicación de otros grupos de seguridad privados.

> **Note**
>
> La configuración del tráfico de red en la mayoría de los casos no se hace de forma automática en Amazon Redshift. Esto se debe a que pueden variar en un nivel detallado, en función de si el origen del tráfico es Internet o un grupo de seguridad privado y debido a que los requisitos de seguridad varían.

Accesibilidad pública con configuración de grupo de seguridad predeterminada o personalizada

Si está creando o ya tiene un clúster o grupo de trabajo, realice los siguientes pasos de configuración para que sea accesible públicamente. Esto se aplica tanto cuando elige el grupo de seguridad predeterminado como un grupo de seguridad personalizado:

1. Busque la configuración de red:
   - Para un clúster de Amazon Redshift aprovisionado, elija la pestaña Propiedades y, a continuación, en Configuración de red y seguridad, seleccione la VPC de su clúster.
   - Para un grupo de trabajo de Amazon Redshift sin servidor, elija Configuración del grupo de trabajo. Elija el grupo de trabajo de la lista. A continuación, en Acceso a datos, en el panel Red y seguridad, elija Editar.
2. Configure la puerta de enlace de Internet y la tabla de enrutamiento para su VPC. Elija la VPC por su nombre para iniciar la configuración. Abre el panel de VPC. Para conectarse a un clúster o grupo de trabajo de acceso público desde Internet, se debe adjuntar una puerta de enlace de Internet a la tabla de enrutamiento. Puede configurarlo si elige Tablas de enrutamiento en el panel de VPC. Confirme que la puerta de enlace de Internet objetivo está establecida con la fuente 0.0.0.0/0 o un CIDR de IP público. La tabla de enrutamiento debe estar asociada a VPC en la que se encuentra el clúster. Para obtener más información sobre la configuración del acceso a Internet para una VPC, como lo que se describe aquí, consulte Habilitar el acceso a Internet en la documentación de Amazon VPC. Para obtener más información sobre la configuración de una tabla de enrutamiento, consulte Configurar tablas de enrutamiento.
3. Después de configurar la puerta de enlace de Internet y la tabla de enrutamiento, vuelva a la configuración de red de Redshift. Abra el acceso entrante; para ello, elija el grupo de seguridad y, a continuación, las reglas de entrada. Elija Editar reglas de entrada.
4. Elija el Protocolo y el Puerto para la regla o reglas de entrada, según sus necesidades, para permitir el tráfico de los clientes. Para un clúster RA3, seleccione un puerto en los intervalos 5431-5455 o 8191-8215. Cuando haya terminado, guarde cada regla.
5. Edite la configuración De acceso público para habilitarla. Puede hacerlo desde el menú Acciones de su clúster o grupo de trabajo.

Al activar la configuración de acceso público, Redshift crea una dirección IP elástica. Es una dirección IP estática que está asociada a su cuenta de AWS. Los clientes externos a la VPC pueden utilizarla para conectarse.

Para obtener más información sobre la configuración de su grupo de seguridad, consulte Grupos de seguridad del clúster de Amazon Redshift.

Puede probar sus reglas conectándose con un cliente; realice lo siguiente si se conecta a Amazon Redshift sin servidor. Una vez finalizada la configuración de red, conéctese con su herramienta cliente, como Amazon Redshift RSQL. Si utiliza su dominio de Amazon Redshift Serverless como host, ingrese lo siguiente:

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```

Accesibilidad privada con configuración de grupo de seguridad predeterminada o personalizada

Cuando no se comunica a través de Internet con su clúster o grupo de trabajo, se habla de acceso privado. Si eligió el grupo de seguridad predeterminado cuando lo creó, el grupo de seguridad incluye las siguientes reglas de comunicación predeterminadas:

- Una regla de entrada que permite el tráfico de todos los recursos asignados al grupo de seguridad.
- Una regla de salida que permite todo el tráfico saliente. El destino de esta regla es 0.0.0.0/0. En notación de enrutamiento entre dominios sin clases (CIDR), representa todas las direcciones IP posibles.

Puede ver las reglas en la consola si selecciona el grupo de seguridad de su clúster o grupo de trabajo.

Si tanto su clúster o grupo de trabajo como su cliente utilizan el grupo de seguridad predeterminado, no es necesaria ninguna configuración adicional para permitir el tráfico de red. Pero si elimina o modifica alguna regla del grupo de seguridad predeterminado para Redshift o el cliente, esto ya no será aplicable. En este caso, debe configurar reglas para permitir la comunicación entrante y saliente. Una configuración común del grupo de seguridad es la siguiente:

- Para una instancia de Amazon EC2 cliente:
  - Una regla de entrada que permite la dirección IP del cliente.
  - Una regla de salida que permite el intervalo de direcciones IP (bloque de CIDR) de todas las subredes proporcionadas para el uso de Redshift. O puede especificar 0.0.0.0/0, que son todos los intervalos de direcciones IP.

- Para su clúster o grupo de trabajo de Redshift:
  - Una regla de entrada que permite el grupo de seguridad cliente.
  - Una regla de salida que permite el tráfico a 0.0.0.0/0. Normalmente, la regla de salida permite todo el tráfico saliente. Opcionalmente, puede agregar una regla de salida para permitir el tráfico al grupo de seguridad cliente. En este caso opcional, no siempre es necesaria una regla de salida, ya que se permite que el tráfico de respuesta de cada solicitud llegue a la instancia. Para obtener más detalles sobre el comportamiento de las solicitudes y respuestas, consulte Grupos de seguridad en la guía del usuario de Amazon VPC.

Si cambia la configuración de cualquier subred o grupo de seguridad especificado para el uso de Redshift, es posible que tenga que cambiar las reglas de tráfico en consecuencia para mantener abierta la comunicación. Para obtener más información sobre la creación de reglas de entrada y salida, consulte Bloques CIDR de VPC en la guía del usuario de Amazon VPC. Para obtener más información acerca de cómo conectarse a Amazon Redshift desde un cliente, consulte Configuración de conexiones en Amazon Redshift.

Cómo funciona Amazon Redshift con el uso compartido de VPC para los recursos de AWS

El uso compartido de VPC le permite crear recursos de aplicaciones de AWS, como instancias de Amazon EC2 y otros servicios de AWS, en una nube privada virtual (VPC) administrada de forma centralizada y compartida. La cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes) que pertenecen a la misma organización de AWS. Aquí se describe cómo puede crear y utilizar un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor en una VPC compartida.

Los beneficios del uso compartido de la VPC incluyen que no tiene que administrar tantas VPC y puede ayudarlo a simplificar la red. El beneficio específico para los administradores y usuarios de Amazon Redshift es que los recursos de Redshift pueden funcionar de forma productiva en la VPC compartida. Para obtener más información sobre el uso compartido de la VPC, consulte Compartir la VPC con otras cuentas, que profundiza en los beneficios de compartir VPC y su funcionamiento.

Cómo utilizar los recursos del almacenamiento de datos de Amazon Redshift en una VPC compartida

En primer lugar, es importante entender que los participantes de una subred compartida no pueden ver un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor. Sin

embargo, esto no impide que los participantes trabajen con la base de datos del propietario en una VPC compartida. Esto se detalla en profundidad en los pasos siguientes.

Antes de crear un clúster de Amazon Redshift aprovisionado en una VPC compartida, debe crear un grupo de subredes que desee utilizar para Amazon Redshift. Esto debe incluir las subredes de la VPC compartida que desee utilizar. Al crear el clúster de Amazon Redshift, debe elegir esta subred y especificar también el grupo de seguridad de la VPC compartida. Del mismo modo, debe especificar las subredes compartidas y el grupo de seguridad que creó en la VPC compartida al crear el grupo de trabajo y la base de datos de Amazon Redshift sin servidor. Después de configurar las subredes, lleve a cabo estos pasos para configurar los recursos de Redshift en el entorno compartido:

1. El propietario de la VPC crea un clúster de Amazon Redshift o un grupo de trabajo Amazon Redshift sin servidor mediante una subred de la VPC compartida.
2. El propietario de la VPC hace que el clúster o el grupo de trabajo estén disponibles en un escenario entre VPC. Los pasos se describen en Uso de puntos de conexión de VPC administrados por Redshift en Amazon Redshift para un clúster aprovisionado o en Conexión con Amazon Redshift sin servidor desde un punto de conexión de VPC administrado por Amazon Redshift para Amazon Redshift sin servidor. Al habilitar la disponibilidad entre VPC, pueden poner la base de datos a disposición de los usuarios en la misma cuenta de AWS o en otras cuentas.
3. Por el contrario, mediante el uso compartido de VPC, un propietario puede compartir una subred con un participante y el participante puede crear un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor en la subred. Sin embargo, en este caso, el propietario no puede ver un recurso de Amazon Redshift creado por un participante. El clúster o grupo de trabajo debe estar accesible mediante la habilitación de la disponibilidad entre VPC de la misma manera que se describió en el paso anterior.

Notas de uso para usar los recursos de Amazon Redshift en una VPC compartida

Tenga en cuenta los siguientes comportamientos relacionados con el uso de Amazon Redshift en una subred compartida:

- Como se detalla en la sección anterior, el propietario de la VPC no puede compartir un clúster de Amazon Redshift o un grupo de trabajo Amazon Redshift sin servidor con un participante mediante el uso compartido de VPC. Sin embargo, el participante puede crear un clúster o un grupo de trabajo de Amazon Redshift sin servidor en la subred del propietario. En este caso, Amazon Redshift no está visible mediante el uso compartido de VPC para el propietario.

- El propietario de la VPC no puede ver, actualizar ni eliminar un clúster aprovisionado de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor que el participante cree en la subred compartida.
- No hay permisos disponibles para hacer que otra cuenta de AWS pueda acceder a los recursos de Amazon Redshift que cree en la VPC compartida.

Grupos de subredes del clúster de Amazon Redshift

Información general

Usted crea un grupo de subred de clúster si aprovisiona el clúster en su Virtual Private Cloud (VPC, Nube privada virtual). Para obtener más información acerca de la VPC, consulte la página de detalles del producto de Amazon VPC.

Su VPC puede tener una o más subredes, un subconjunto de direcciones IP dentro de la VPC, que le permite agrupar recursos según las necesidades de seguridad y operación. Un grupo de subred de clúster le permite especificar un conjunto de subredes en su VPC. Cuando aprovisiona un clúster, proporciona un grupo de subredes y Amazon Redshift crea el clúster en una de las subredes del grupo.

Para obtener más información acerca de la creación de una VPC, vaya a la documentación de la Guía del usuario de Amazon VPC.

Después de crear un grupo de subredes, puede quitar las subredes que agregó previamente o agregar más subredes. Amazon Redshift ofrece operaciones de la API para que pueda crear, modificar o eliminar un grupo de subredes del clúster. También puede usar la consola para realizar estas operaciones.

Administración de grupos de subred de clúster mediante la consola

Puede administrar los grupos de subredes del clúster mediante la consola de Amazon Redshift. Puede crear un grupo de subredes del clúster, administrar o eliminar uno existente. Todas estas tareas parten de la lista de grupos de subredes de clúster. Para administrar este tipo de grupo, debe seleccionar un grupo de subredes de clúster.

Puede aprovisionar un clúster en una de las subredes que proporciona al grupo de subred. Un grupo de subred de clúster le permite especificar un conjunto de subredes en su virtual private cloud (VPC).

Creación de un grupo de subredes de clúster

Debe tener al menos un grupo de subred de clúster definido para aprovisionar un clúster en una Virtual Private Cloud (VPC, Nube virtual privada).

Pasos para crear un grupo de subred de clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Subnet groups (Grupos de subredes). Se muestra la lista de grupos de subredes.
3. Seleccione Create cluster subnet group (Crear grupo de subred de clúster) para mostrar la página de creación.
4. Introduzca información para el grupo de subredes, incluidas las subredes que desea añadir.
5. Elija Create cluster subnet group (Crear grupo de subred de clúster) para crear el grupo con las subredes que eligió.

Modificación de un grupo de subredes de clúster

Pasos para modificar un grupo de subredes de clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Subnet groups (Grupos de subredes). Se muestra la lista de grupos de subredes.
3. Elija el grupo de subredes que modificar.
4. Para Actions (Acciones), seleccione Modify (Modificar) para mostrar los detalles del grupo de subredes.
5. Actualice la información para el grupo de subredes.
6. Seleccione Save (Guardar) para modificar el grupo.

Cambiar o eliminar subredes en algunos casos requiere pasos adicionales. Por ejemplo, este artículo del AWS Knowledge Center, ¿Cómo muevo mi clúster de Amazon Redshift aprovisionado a una subred diferente?, describe un caso de uso que cubre el traslado de un clúster.

Eliminación de un grupo de subredes de clúster

No puede eliminar un grupo de subredes de clúster que es utilizado por algún clúster.

Pasos para eliminar un grupo de subredes de clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Subnet groups (Grupos de subredes). Se muestra la lista de grupos de subredes.
3. Elija el grupo de subredes que eliminar, luego seleccione Delete (Eliminar).

Administre los grupos de subredes del clúster mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar los grupos de subredes del clúster.

- create-cluster-subnet-group
- delete-cluster-subnet-group
- describe-cluster-subnet-groups
- modify-cluster-subnet-group

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar los grupos de subredes del clúster.

- CreateClusterSubnetGroup
- DeleteClusterSubnetGroup
- DescribeClusterSubnetGroups
- ModifyClusterSubnetGroup

Historial de versiones del clúster

Amazon Redshift lanza periódicamente nuevas versiones del clúster que se utilizan para actualizarlo.

Important

Para ver la información acerca de las versiones de clúster de Amazon Redshift disponibles y sus características, mejoras y correcciones, consulte Versiones de clúster para Amazon Redshift.

Uso de integraciones sin ETL

Este tema incluye documentación de la versión preliminar de las integraciones sin ETL de Aurora PostgreSQL y RDS para MySQL con Amazon Redshift. Tanto la documentación como las características quedan sujetas a cambios. Se recomienda utilizar las integraciones sin ETL de RDS para MySQL y Aurora PostgreSQL únicamente en entornos de prueba y no de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

La integración sin ETL es una solución totalmente administrada que permite que los datos transaccionales u operativos estén disponibles en Amazon Redshift prácticamente en tiempo real. Con esta solución, puede configurar una integración desde su fuente a un almacenamiento de datos de Amazon Redshift. No es necesario mantener una canalización de extracción, transformación y carga (ETL). Nosotros nos ocupamos de la ETL mediante la automatización de la creación y administración de la replicación de datos del origen de datos al clúster de Amazon Redshift o al espacio de nombres de Redshift sin servidor. Puede seguir actualizando y consultando los datos de origen y, al mismo tiempo, utilizar Amazon Redshift para cargas de trabajo de análisis, como informes y paneles.

Los siguientes orígenes son compatibles actualmente con las integraciones sin ETL:

- Edición de Aurora compatible con MySQL
- Edición de Aurora compatible con PostgreSQL (versión preliminar)
- RDS para MySQL (versión preliminar)

Para crear una integración sin ETL, especifique un origen de integración y un almacenamiento de datos de Amazon Redshift como destino. La integración replica los datos del origen en el almacenamiento de datos de destino. Los datos estarán disponibles en Amazon Redshift en cuestión de segundos. La integración supervisa el estado de la canalización de datos y se recupera de los problemas cuando es posible. Puede crear integraciones a partir de orígenes del mismo tipo en un único almacenamiento de datos de Amazon Redshift para obtener información integral de varias aplicaciones.

Con los datos de Amazon Redshift, puede utilizar los análisis que proporciona Amazon Redshift. Por ejemplo, el machine learning (ML) integrado, las vistas materializadas, el uso compartido de datos y

el acceso directo a varios almacenes y lagos de datos. La integración sin ETL mantiene los recursos de computación aislados de los recursos de datos, de modo que usted utiliza las herramientas más eficientes para procesar datos. Para los ingenieros de datos, la integración sin ETL proporciona acceso a datos urgentes que, de otro modo, pueden verse retrasados por errores intermitentes en canalizaciones de datos complejas. Puede ejecutar consultas analíticas y modelos de ML en los datos transaccionales para obtener información casi en tiempo real sobre eventos y decisiones empresariales urgentes.

Puede crear una suscripción de notificación de eventos de Amazon Redshift para recibir notificaciones cada vez que se produzca un evento para una integración sin ETL determinada. Para ver la lista de notificaciones de eventos relacionadas con la integración, consulte Notificaciones de eventos de integración sin ETL con Amazon EventBridge. La forma más sencilla de crear una suscripción es a través de la consola de Amazon SNS. Para obtener información acerca de cómo crear un tema de Amazon SNS y suscribirse a él, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Cuando empiece a utilizar las integraciones sin ETL, tenga en cuenta los siguientes conceptos:

- Una base de datos de origen es la base de datos en la que se replican los datos en Amazon Redshift.
- Un almacenamiento de datos de destino es el clúster aprovisionado de Amazon Redshift o el grupo de trabajo de Redshift sin servidor en el que se replican los datos.
- Una base de datos de destino es la base de datos que se crea a partir de una integración sin ETL en el almacenamiento de datos de destino.

Puede monitorear las integraciones sin ETL mediante la consulta de determinadas vistas del sistema en Amazon Redshift.

- SVV_INTEGRATION proporciona información sobre los detalles de configuración de las integraciones sin ETL.
- SYS_INTEGRATION_ACTIVITY proporciona información sobre las integraciones sin ETL finalizadas.
- SVV_INTEGRATION_TABLE_STATE proporciona información sobre el estado de la integración.
- SYS_INTEGRATION_TABLE_STATE_CHANGE proporciona información sobre el registro de cambios de estado de la tabla para las integraciones.

Para obtener información sobre los precios de las integraciones sin ETL, consulte la página de precios correspondiente:

- Precios de Amazon Redshift
- Precios de Amazon Aurora
- Precios de Amazon RDS

Para obtener más información acerca de los orígenes de la integración sin ETL, consulte los temas siguientes:

- Para obtener información sobre las integraciones sin ETL de Aurora, consulte los temas Beneficios, Conceptos clave, Limitaciones, Cuotas y Regiones admitidas de las integraciones sin ETL en la Guía del usuario de Amazon Aurora.
- Para obtener información sobre las integraciones sin ETL de RDS, consulte los temas Beneficios, Conceptos clave, Limitaciones, Cuotas y Regiones admitidas de las integraciones sin ETL en la Guía del usuario de Amazon RDS.

Temas

- Consideraciones al utilizar las integraciones sin ETL con Amazon Redshift
- Introducción a las integraciones sin ETL
- Creación de bases de datos de destino en Amazon Redshift
- Consulta y creación de vistas materializadas con datos replicados
- Administración de integraciones sin ETL
- Métricas para integraciones sin ETL
- Solución de problemas de integración sin ETL

Consideraciones al utilizar las integraciones sin ETL con Amazon Redshift

Las siguientes consideraciones se aplican a las integraciones sin ETL con Amazon Redshift.

- El almacenamiento de datos de Amazon Redshift de destino debe cumplir los siguientes requisitos previos:

  - Ejecutar Amazon Redshift sin servidor o un tipo de nodo RA3 (ra3.16xlarge, ra3.4xlarge y ra3.xlplus).
  - Cifrado (si se utiliza un clúster aprovisionado).
  - Distinción entre mayúsculas y minúsculas activada.
- No puedes habilitar la compatibilidad mejorada con VPC en el almacenamiento de datos con las integraciones configuradas.
- Si elimina un origen que sea el origen de la integración autorizada para un almacenamiento de datos de Amazon Redshift, todas las integraciones asociadas pasarán al estado `FAILED`.
- No puede eliminar un almacenamiento de datos de Amazon Redshift que tenga integraciones sin ETL existentes. Primero debe eliminar todas las integraciones asociadas.
- Primero debe eliminar todas las integraciones que estén asociadas a una base de datos de destino antes de eliminar la base de datos de destino.
- La base de datos de destino es de solo lectura. No puede crear tablas, vistas ni vistas materializadas en la base de datos de destino. Sin embargo, puede utilizar vistas materializadas en otras tablas del almacenamiento de datos de destino.
- Las vistas materializadas se admiten cuando se utilizan en consultas entre bases de datos. La actualización de las vistas materializadas con datos replicados a partir de integraciones sin ETL conlleva una actualización completa de la vista. No se admite la actualización incremental, la reescritura automática de consultas, la actualización automática ni las vistas materializadas automatizadas. Para obtener información sobre la creación de vistas materializadas con datos replicados mediante integraciones sin ETL, consulte Creación de vistas materializadas con datos replicados.
- Solo puede consultar las tablas del almacenamiento de datos de destino que tengan el estado `Synced`. Para obtener más información, consulte Métricas para integraciones sin ETL.
- Las integraciones sin ETL no son compatibles con los almacenamientos de datos de destino que se configuran para la implementación multi-AZ.
- Los clústeres aprovisionados con integraciones sin ETL no admiten el cambio de tamaño clásico. Si se ejecuta esta operación, la integración pasará a tener el estado `FAILED`.
- Amazon Redshift solo acepta caracteres UTF-8, por lo que es posible que no respete la intercalación definida en el origen. Las reglas de clasificación y comparación pueden ser diferentes, por lo que, en última instancia, pueden cambiar los resultados de la consulta.
- Las tablas del origen de la integración deben contar con una clave principal. De lo contrario, las tablas no se podrán replicar en el almacenamiento de datos de destino de Amazon Redshift.

- Para las integraciones sin ETL de Aurora PostgreSQL y RDS para MySQL con Amazon Redshift, cree el almacenamiento de datos de destino en Vista previa. Para obtener más información, consulte Creación y configuración de un almacenamiento de datos de Amazon Redshift de destino.

Para las consideraciones que también se aplican al origen de integración, consulte uno de los siguientes temas:

- Para los orígenes de Aurora, consulte Limitaciones en la Guía del usuario de Amazon Aurora.
- Para los orígenes de Amazon RDS, consulte Limitaciones en la Guía del usuario de Amazon Aurora.

Introducción a las integraciones sin ETL

Antes de configurar la integración sin ETL en Amazon Redshift, configure el origen de integración con los parámetros y permisos necesarios. Después, continúe con el resto de la configuración inicial desde la consola de Amazon Redshift y la AWS CLI.

Para crear una integración sin ETL de Aurora con Amazon Redshift

Para crear una integración sin ETL de Aurora con Amazon Redshift, haga lo siguiente:

1. Desde la consola de Amazon RDS, cree un grupo de parámetros del clúster de base de datos personalizado tal como se describe en la Guía del usuario de Amazon Aurora.
2. Desde la consola de Amazon RDS, cree un clúster de base de datos de Amazon Aurora de origen tal como se describe en la Guía del usuario de Amazon Aurora.
3. Desde la consola de Amazon Redshift: Creación y configuración de un almacenamiento de datos de Amazon Redshift de destino.
   - Desde la AWS CLI o la consola de Amazon Redshift: Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos.
   - Desde la consola de Amazon Redshift: Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.
4. Desde la consola de Amazon RDS, cree una integración sin ETL tal y como se describe en la Guía del usuario de Amazon Aurora.
5. Desde la consola de Amazon Redshift o el editor de consultas v2, cree una base de datos de Amazon Redshift a partir de su integración.

A continuación, consulte y cree vistas materializadas con datos replicados.

Para crear una integración sin ETL de RDS con Amazon Redshift

Para crear una integración sin ETL de RDS con Amazon Redshift, haga lo siguiente:

1. Desde la consola de Amazon RDS, cree un grupo de parámetros de base de datos personalizado tal y como se describe en la Guía del usuario de Amazon Aurora.
2. Desde la consola de Amazon RDS, cree una instancia de Amazon RDS de origen tal y como se describe en la Guía del usuario de Amazon RDS.
3. Desde la consola de Amazon Redshift: Creación y configuración de un almacenamiento de datos de Amazon Redshift de destino.
   - Desde la AWS CLI o la consola de Amazon Redshift: Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos.
   - Desde la consola de Amazon Redshift: Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.
4. Desde la consola de Amazon RDS, cree una integración sin ETL tal y como se describe en la Guía del usuario de Amazon RDS.
5. Desde la consola de Amazon Redshift o el editor de consultas v2, cree una base de datos de Amazon Redshift a partir de su integración.

   A continuación, consulte y cree vistas materializadas con datos replicados.

La consola de Amazon RDS ofrece un flujo de creación de la integración paso a paso, en el que se especifica la base de datos de origen y el almacenamiento de datos de Amazon Redshift de destino. Si se producen problemas, puede elegir que Amazon RDS los corrija por usted en lugar de corregirlos manualmente en la consola de Amazon RDS o de Amazon Redshift.

Creación y configuración de un almacenamiento de datos de Amazon Redshift de destino

Antes de este paso, cree el origen de integración y configure los parámetros requeridos por el tipo de origen para las integraciones sin ETL.

En este paso, se crea y configura un almacenamiento de datos de Amazon Redshift de destino, como por ejemplo, un grupo de trabajo de Amazon Redshift sin servidor o un clúster aprovisionado.

El almacenamiento de datos de destino debe tener las siguientes características:

- Ejecución de Amazon Redshift sin servidor o de un clúster aprovisionado de tipo de instancia ra3.16xlarge, ra3.4xlarge o ra3.xlplus.
- Tiene activada la distinción entre mayúsculas y minúsculas (`enable_case_sensitive_identifier`). Para obtener más información, consulte Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos.
- Estar cifrado, si el almacenamiento de datos de destino es un clúster aprovisionado de Amazon Redshift. Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift.
- Haberse creado en la misma región de AWS que el origen de integración.

> **Note**
>
> Para las integraciones sin ETL de Aurora PostgreSQL y RDS para MySQL con Amazon Redshift, tenga en cuenta también lo siguiente para el almacenamiento de datos de destino.
>
> - Debe crear el almacenamiento de datos en Vista previa en la pista `preview_2023`. No puede utilizar características de vista previa ni trasladar el almacenamiento de datos de vista previa a una implementación de producción.
> - Si decide crear un clúster aprovisionado de Amazon Redshift, dicho clúster debe tener al menos dos nodos.
> - Para los orígenes de Aurora PostgreSQL, debe crear su almacenamiento de datos de destino en la región Este de EE. UU. (Ohio) de AWS. Tenga en cuenta que debe crear la base de datos de origen para las integraciones sin ETL de Aurora PostgreSQL en el entorno de vista previa de bases de datos de Amazon RDS.
>
>   En el caso de los orígenes de RDS para MySQL, debe crear su almacenamiento de datos de destino en una región de AWS compatible. Para ver una lista de las regiones de AWS en las que están disponibles las integraciones sin ETL de RDS para MySQL, consulte Supported Regions for zero-ETL integrations with Amazon Redshift en la Guía del usuario de Amazon RDS.
>
> Para crear el almacenamiento de datos de destino en Vista previa para las integraciones sin ETL de Aurora PostgreSQL y RDS para MySQL, consulte uno de los siguientes temas en función del tipo de implementación:

- Para crear una versión preliminar del clúster aprovisionado de Amazon Redshift, consulte Crear un clúster de vista previa. Asegúrese de elegir la pista `preview_2023` para poder utilizar integraciones sin ETL.
- Para crear una versión preliminar de un grupo de trabajo de Amazon Redshift sin servidor, consulte Crear un grupo de trabajo de vista previa.

Para crear el almacenamiento de datos de destino para las integraciones sin ETL de Aurora MySQL, consulte uno de los siguientes temas en función del tipo de implementación:

- Para crear un clúster aprovisionado de Amazon Redshift, consulte Creación de un clúster.
- Para crear un grupo de trabajo de Amazon Redshift sin servidor con un espacio de nombres, consulte Creación de un grupo de trabajo con un espacio de nombres.

Al crear un clúster aprovisionado, Amazon Redshift también crea un grupo de parámetros predeterminados. No puede editar el grupo de parámetros predeterminado. Sin embargo, puede crear un grupo de parámetros personalizado antes de crear un nuevo clúster y, a continuación, asociarlo al clúster. O bien, puede editar el grupo de parámetros que se asociará al clúster creado. También debe activar la distinción entre mayúsculas y minúsculas para el grupo de parámetros al crear el grupo de parámetros personalizado o al editar uno actual para poder utilizar las integraciones sin ETL.

Puede crear un grupo de parámetros personalizados mediante la consola de Amazon Redshift o la AWS CLI como se indica a continuación:

- Con la consola de Amazon Redshift: Administración de grupos de parámetros mediante la consola
- Con la AWS CLI: Administración de grupos de parámetros mediante la AWS CLI y la API de Amazon Redshift

Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos

Puede asociar un grupo de parámetros y habilitar la distinción entre mayúsculas y minúsculas para un clúster aprovisionado durante la creación. Sin embargo, únicamente podrá actualizar un grupo de trabajo sin servidor a través de AWS Command Line Interface (AWS CLI) después de crearlo. Es necesario para admitir la distinción entre mayúsculas y minúsculas de MySQL y

PostgreSQL. `enable_case_sensitive_identifier` es un valor de configuración que determina si en los identificadores de nombres de bases de datos, tablas y columnas se distingue entre mayúsculas y minúsculas. Este parámetro debe estar activado para crear integraciones sin ETL en el almacenamiento de datos. Para obtener más información, consulte enable_case_sensitive_identifier.

Para Amazon Redshift sin servidor: Activación de la distinción entre mayúsculas y minúsculas para Amazon Redshift sin servidor mediante la AWS CLI. Tenga en cuenta que solo puede activar la distinción entre mayúsculas y minúsculas para Amazon Redshift sin servidor desde la AWS CLI.

Para los clústeres aprovisionados de Amazon Redshift, habilite la distinción entre mayúsculas y minúsculas en el clúster de destino mediante uno de los siguientes temas:

- Activación de la distinción entre mayúsculas y minúsculas para los clústeres aprovisionados de Amazon Redshift mediante la consola de Amazon Redshift
- Activación de la distinción entre mayúsculas y minúsculas para los clústeres aprovisionados de Amazon Redshift mediante la AWS CLI

Activación de la distinción entre mayúsculas y minúsculas para Amazon Redshift sin servidor mediante la AWS CLI

Ejecute el siguiente comando AWS CLI para activar la distinción entre mayúsculas y minúsculas en el grupo de trabajo.

```
aws redshift-serverless update-workgroup \
        --workgroup-name target-workgroup \
        --config-parameters
 parameterKey=enable_case_sensitive_identifier,parameterValue=true
```

Espere a que el estado del grupo de trabajo sea `Active` antes de ir al paso siguiente.

Activación de la distinción entre mayúsculas y minúsculas para los clústeres aprovisionados de Amazon Redshift mediante la consola de Amazon Redshift

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el panel de navegación de la izquierda, elija Panel de clústeres aprovisionados.
3. Elija el clúster aprovisionado en el que desea replicar los datos.

4. En el panel de navegación de la izquierda, elija Configuraciones > Administración de cargas de trabajo.
5. En la página de administración de cargas de trabajo, elija el grupo de parámetros.
6. Elija la pestaña Parámetros.
7. Seleccione Editar parámetros y, a continuación, cambie enable_case_sensitive_identifier a true.
8. A continuación, elija Guardar.

Activación de la distinción entre mayúsculas y minúsculas para los clústeres aprovisionados de Amazon Redshift mediante la AWS CLI

1. Como no puede editar el grupo de parámetros predeterminado, desde el programa de terminal, ejecute el siguiente comando de la AWS CLI para crear un grupo de parámetros personalizado. Más adelante, lo asociará al clúster aprovisionado.

```
aws redshift create-cluster-parameter-group \
    --parameter-group-name zero-etl-params \
    --parameter-group-family redshift-1.0 \
    --description "Param group for zero-ETL integrations"
```

2. Ejecute el siguiente comando de la AWS CLI para activar la distinción entre mayúsculas y minúsculas para el grupo de parámetros.

```
aws redshift modify-cluster-parameter-group \
    --parameter-group-name zero-etl-params \
    --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. Ejecute el siguiente comando para asociar el grupo de parámetros con el clúster.

```
aws redshift modify-cluster \
    --cluster-identifier target-cluster \
    --cluster-parameter-group-name zero-etl-params
```

4. Espere a que el clúster aprovisionado esté disponible. Puede comprobar el estado del clúster con el comando `describe-cluster`. A continuación, ejecute el siguiente comando para reiniciar el clúster.

```
aws redshift reboot-cluster \
    --cluster-identifier target-cluster
```

Configuración de la autorización para el almacenamiento de datos de Amazon Redshift

Para replicar datos desde el origen de integración en su almacenamiento de datos de Amazon Redshift, debe agregar inicialmente las dos entidades siguientes:

- Entidad principal autorizada: identifica al usuario o rol que puede crear integraciones sin ETL en el almacenamiento de datos.
- Origen de integración autorizado: identifica la base de datos de origen que puede actualizar el almacenamiento de datos.

Puede configurar las entidades principales autorizadas y los orígenes de integración autorizados desde la pestaña Política de recursos de la consola de Amazon Redshift o mediante la operación de la API de `PutResourcePolicy` Amazon Redshift.

Agregar entidades principales autorizadas

Para crear una integración sin ETL en el grupo de trabajo de Redshift sin servidor o el clúster aprovisionado, autorice el acceso al espacio de nombres asociado o al clúster aprovisionado.

Puede omitir este paso si se cumplen las dos condiciones siguientes:

- La Cuenta de AWS propietaria del grupo de trabajo de Redshift sin servidor o el clúster aprovisionado también son propietarias de la base de datos de origen.
- Esa entidad principal está asociada a una política de IAM basada en identidad con permisos para crear integraciones sin ETL en este espacio de nombres de Redshift sin servidor o clúster aprovisionado.

Agregar entidades principales autorizadas a un espacio de nombres de Amazon Redshift sin servidor

1. En la consola de Amazon Redshift, elija Redshift sin servidor en el panel de navegación de la izquierda.
2. Elija Configuración del espacio de nombres, luego escoja su espacio de nombres y vaya a la pestaña Política de recursos.
3. Elija Agregar entidades principales autorizadas.

4. Para cada entidad principal autorizada que desee agregar, introduzca el ARN del usuario o rol de AWS o el ID de cuenta de Cuenta de AWS al que desee conceder acceso para crear integraciones sin ETL en el espacio de nombres. Un ID de cuenta se almacena como un ARN.
5. Elija Guardar cambios.

Agregar entidades principales autorizadas a un clúster aprovisionado de Amazon Redshift

1. En la consola de Amazon Redshift, en el panel de navegación de la izquierda, elija Panel de clústeres aprovisionados.
2. Elija Clústeres y seleccione el clúster. Vaya a la pestaña Política de recursos.
3. Elija Agregar entidades principales autorizadas.
4. Para cada entidad principal autorizada que desee agregar, introduzca el ARN del usuario o rol de AWS o el ID de cuenta de la Cuenta de AWS al que desee conceder acceso para crear integraciones sin ETL en el clúster. Un ID de cuenta se almacena como un ARN.
5. Elija Guardar cambios.

Agregar orígenes de integración autorizados

Para permitir que el origen actualice el almacenamiento de datos de Amazon Redshift, debe agregarlo como origen de integración autorizado al espacio de nombres.

Agregar un origen de integración autorizado a un espacio de nombres de Amazon Redshift sin servidor

1. En la consola de Amazon Redshift, vaya al Panel sin servidor.
2. Elija el nombre del espacio de nombres.
3. Vaya a la pestaña Política de recursos.
4. Seleccione Agregar un origen de integración autorizado.
5. Especifique el ARN del origen para la integración sin ETL.

> **Note**
>
> La eliminación de un origen de integración autorizado impide que los datos se repliquen en el espacio de nombres. Esta acción desactiva todas las integraciones sin ETL de ese origen en este espacio de nombres.

Agregar un origen de integración autorizado a un clúster aprovisionado de Amazon Redshift

1. En la consola de Amazon Redshift, vaya al Panel de clústeres aprovisionados.
2. Elija el nombre del clúster aprovisionado.
3. Vaya a la pestaña Política de recursos.
4. Seleccione Agregar un origen de integración autorizado.
5. Especifique el ARN del origen que es el origen de datos para la integración sin ETL.

> **Note**
>
> La eliminación de un origen de integración autorizado impide que los datos se repliquen en el clúster aprovisionado. Esta acción desactiva todas las integraciones sin ETL de ese origen en este clúster aprovisionado de Amazon Redshift.

Configuración de la autorización con la API de Amazon Redshift

Puede utilizar las operaciones de la API de Amazon Redshift para configurar políticas de recursos que funcionen con las integraciones sin ETL.

Para controlar el origen que puede crear una integración entrante en el espacio de nombres, cree una política de recursos y asóciela al espacio de nombres. Con la política de recursos, puede especificar el origen que tiene acceso a la integración. La política de recursos se adjunta al espacio de nombres del almacenamiento de datos de destino para permitir que el origen cree una integración entrante para replicar los datos activos del origen en Amazon Redshift.

La siguiente es una política de recursos de ejemplo.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "redshift:AuthorizeInboundIntegration",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "source_arn"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "source_principal"
      },
      "Action": "redshift:CreateInboundIntegration"
    }
  ]
}
```

A continuación, se resumen las operaciones de la API de Amazon Redshift aplicables a la configuración de las políticas de recursos para las integraciones:

- Utilice la operación de la API PutResourcePolicy para conservar la política de recursos. Al proporcionar otra política de recursos, se reemplaza la política de recursos anterior del recurso. Utilice el ejemplo de política de recursos anterior, que concede permisos para las siguientes acciones:
  - `CreateInboundIntegration`: permite a la entidad principal de origen crear una integración entrante para que los datos se repliquen desde el origen en el almacenamiento de datos de destino.
  - `AuthorizeInboundIntegration`: permite a Amazon Redshift validar continuamente que el almacenamiento de datos de destino pueda recibir datos replicados desde el ARN de origen.
- Utilice la operación de la API GetResourcePolicy para ver las políticas de recursos existentes.
- Utilice la operación de la API DeleteResourcePolicy para eliminar una política de recursos del recurso.

Para actualizar una política de recursos, también puede usar el comando put-resource-policy de la AWS CLI.

Siguientes pasos

Ahora que ha configurado la autorización para el almacenamiento de datos de Amazon Redshift de destino, puede crear una integración sin ETL y comenzar a replicar los datos.

Haga lo siguiente en función del origen:

- Para crear integraciones sin ETL de Amazon, consulte Creación de integraciones sin ETL de Amazon Aurora con Amazon Redshift en la Guía del usuario de Amazon Aurora.
- Para crear integraciones sin ETL de RDS, consulte Creating Amazon RDS zero-ETL integrations with Amazon Redshift en la Guía del usuario de Amazon RDS.

Creación de bases de datos de destino en Amazon Redshift

Para replicar datos desde su origen en Amazon Redshift, debe crear una base de datos a partir de su integración en Amazon Redshift.

Conéctese a su grupo de trabajo de Redshift sin servidor o al clúster aprovisionado y cree una base de datos con una referencia a su identificador de integración. Este identificador es el valor que se devuelve para `integration_id` cuando se consulta la vista SVV_INTEGRATION.

> **Important**
>
> Antes de crear una base de datos a partir de la integración, la integración sin ETL debe estar creada y tener el estado `Active` en la consola de Amazon RDS o Amazon Redshift.

Creación de bases de datos de destino en Amazon Redshift

Antes de empezar a replicar datos desde su origen en Amazon Redshift, debe crear una base de datos a partir de la integración en Amazon Redshift. Puede crear la base de datos mediante la consola de Amazon Redshift o el editor de consultas v2.

Creación de una base de datos de destino mediante la consola de Amazon Redshift

1. En el panel de navegación izquierdo, elija Integraciones sin ETL.

2. En la lista de integraciones, seleccione una integración.
3. Si utiliza un clúster aprovisionado, primero deberá conectarse a la base de datos. Seleccione Connect to database (Conectar a base de datos). Puede conectarse mediante una conexión reciente o creando una nueva.
4. Para crear una base de datos a partir de la integración, elija Crear base de datos a partir de integración.
5. Introduzca un nombre de base de datos. El ID de integración y el nombre del almacenamiento de datos se rellenan previamente.

   Para los orígenes de Aurora PostgreSQL, introduzca también la base de datos con nombre que especificó al crear la integración sin ETL.
6. Elija Crear base de datos.

Creación de una base de datos de destino mediante el editor de consultas v2

1. Vaya a la consola de Amazon Redshift y elija Editor de consultas v2.
2. En el panel de la izquierda, elija su grupo de trabajo de Amazon Redshift sin servidor o el clúster aprovisionado de Amazon Redshift y conéctese a él.
3. Para obtener el ID de integración, navegue hasta la lista de integraciones en la consola de Amazon Redshift.

   También puede ejecutar el siguiente comando para obtener el valor de `integration_id`:

   ```
   SELECT integration_id FROM SVV_INTEGRATION;
   ```
4. A continuación, ejecute el siguiente comando para crear la base de datos. Al especificar el ID de integración, se crea una conexión entre la base de datos y el origen.

   Sustituya `integration_id` por el valor que ha devuelto el comando anterior.

   ```
   CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id';
   ```

   En el caso de los orígenes de Aurora PostgreSQL, también debe incluir una referencia a la base de datos designada en el clúster que especificó al crear la integración. Por ejemplo:

```
CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id'
 DATABASE named_db;
```

> **Note**
>
> Solo su origen de integración puede actualizar los datos de la base de datos que cree a partir de la integración. Para cambiar el esquema de una tabla, ejecute los comandos DDL o DML en las tablas del origen. Puede ejecutar comandos DDL y DML en las tablas del origen, pero solo puede ejecutar comandos DDL y consultas de solo lectura en la base de datos de destino.

Para obtener información acerca de la visualización del estado de una base de datos de destino, consulte Administración de integraciones sin ETL.

Adición de datos al origen

Después de crear una base de datos de destino, puede agregar datos a su origen. Para agregar datos al origen, consulte uno de los siguientes temas:

- Para los orígenes de Aurora, consulte Añadir datos al clúster de base datos de origen en la Guía del usuario de Amazon Aurora.
- Para los orígenes de Amazon RDS, consulte Add data to the source DB instance en la Guía del usuario de Amazon RDS.

Consulta y creación de vistas materializadas con datos replicados

Consulta de datos replicados en Amazon Redshift

Una vez añadidos los datos al origen, se replican casi en tiempo real en el almacenamiento de datos de Amazon Redshift y ya se pueden consultar. Para obtener información sobre las métricas de integración y las estadísticas de la tabla, consulte Métricas para integraciones sin ETL.

> **Note**
>
> Como una base de datos es lo mismo que un esquema en MySQL, el nivel de base de datos de MySQL se asigna al nivel de esquema de Amazon Redshift. Tenga en cuenta esta diferencia de asignación cuando consulte datos replicados desde Aurora MySQL o RDS para MySQL.

Para consultar los datos replicados

1. Vaya a la consola de Amazon Redshift y elija Editor de consultas v2.
2. Conéctese a su grupo de trabajo de Amazon Redshift sin servidor o al clúster aprovisionado de Amazon Redshift y elija su base de datos en la lista desplegable.
3. Utilice la instrucción SELECT para seleccionar todos los datos replicados del esquema y la tabla que creó en el origen. Para distinguir entre mayúsculas y minúsculas, utilice comillas dobles (" ") para los nombres de esquemas, tablas y columnas. Por ejemplo:

   ```
   SELECT * FROM "schema_name"."table_name";
   ```

   También puede consultar los datos mediante la CLI de Amazon Redshift.

Creación de vistas materializadas con datos replicados

Puede crear vistas materializadas en su base de datos local de Amazon Redshift para transformar los datos replicados mediante integraciones sin ETL. Conéctese a su base de datos local y utilice consultas entre bases de datos para acceder a las bases de datos de destino. Puede utilizar nombres de objetos totalmente cualificados con la notación de tres partes (destination-database-name.schema-name.table-name) o crear un esquema externo que haga referencia al par de base de datos y esquema de destino y usar la notación de dos partes (external-schema-name.table-name). Para obtener más información sobre las consultas entre bases de datos, consulte Consulta de datos entre bases de datos.

Utilice el siguiente ejemplo para crear e insertar datos de ejemplo en las tablas *sales_zetl* y *event_zetl* desde el origen *tickit_zetl*. Las tablas se replican en la base de datos de Amazon Redshift *zetl_int_db*.

```
CREATE TABLE sales_zetl (
```

```
        salesid integer NOT NULL primary key,
        eventid integer NOT NULL,
        pricepaid decimal(8, 2)
);

CREATE TABLE event_zetl (
        eventid integer NOT NULL PRIMARY KEY,
        eventname varchar(200)
);

INSERT INTO sales_zetl VALUES(1, 1, 3.33);
INSERT INTO sales_zetl VALUES(2, 2, 4.44);
INSERT INTO sales_zetl VALUES(3, 2, 5.55);

INSERT INTO event_zetl VALUES(1, "Event 1");
INSERT INTO event_zetl VALUES(2, "Event 2");
```

Puede crear una vista materializada para obtener las ventas totales por evento mediante la notación de tres partes:

```
--three part notation zetl-database-name.schema-name.table-name
CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_3p as
(SELECT eventname, sum(pricepaid) as total_price
FROM  zetl_int_db.tickit_zetl.sales_zetl S, zetl_int_db.tickit_zetl.event_zetl E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

Puede crear una vista materializada para obtener las ventas totales por evento mediante la notación de dos partes:

```
--two part notation external-schema-name.table-name notation
CREATE EXTERNAL schema ext_tickit_zetl
FROM REDSHIFT
DATABASE zetl_int_db
SCHEMA tickit_zetl;

CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_2p
AS
(
    SELECT eventname, sum(pricepaid) as total_price
    FROM  ext_tickit_zetl.sales_zetl S, ext_tickit_zetl.event_zetl E
    WHERE S.eventid = E.eventid
```

```
    GROUP BY 1
);
```

Para ver las vistas materializadas que ha creado, utilice el siguiente ejemplo.

```
SELECT * FROM mv_transformed_sales_per_event_3p;

+-----------+-------------+
| eventname | total_price |
+-----------+-------------+
| Event 1   | 3.33        |
| Event 2   | 9.99        |
+-----------+-------------+

SELECT * FROM mv_transformed_sales_per_event_2p;

+-----------+-------------+
| eventname | total_price |
+-----------+-------------+
| Event 1   | 3.33        |
| Event 2   | 9.99        |
+-----------+-------------+
```

Administración de integraciones sin ETL

Puede consultar los detalles de una integración sin ETL para ver su información de configuración y su estado en la consola de Amazon Redshift.

Para ver los detalles de una integración sin ETL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el panel de navegación izquierdo, elija el panel Sin servidor o Clústeres aprovisionados. A continuación, elija Integraciones sin ETL.
3. Seleccione la integración sin ETL que desea ver. Para cada intención, debe proporcionar la siguiente información:
   - El ID de integración es el identificador que se devuelve cuando se crea la integración.
   - Estado puede ser uno de los siguientes:

  - `Active`: la integración sin ETL está enviando datos transaccionales al almacenamiento de datos de Amazon Redshift de destino.
  - `Syncing`: la integración sin ETL detectó un error recuperable y vuelve a almacenar los datos. Las tablas afectadas no se podrán consultar en Amazon Redshift hasta que se hayan sincronizado de nuevo.
  - `Failed`: la integración sin ETL detectó un evento o error irrecuperable que no se puede corregir. Debe eliminar y volver a crear la integración sin ETL.
  - `Creating`: la integración sin ETL se está creando.
  - `Deleting`: la integración sin ETL se está eliminando.
  - `Needs attention`: la integración sin ETL detectó un evento o error que requiere la intervención manual para su resolución. Para solucionar el problema, siga los pasos que se indican en el mensaje de error.
- ARN de origen es el ARN de los datos de origen.
- Destino es el ARN del espacio de nombres del almacenamiento de datos de destino.
- Base de datos puede ser una de las siguientes opciones:
  - `No database`: no hay ninguna base de datos de destino para la integración.
  - `Creating`: Amazon Redshift está creando la base de datos de destino para la integración.
  - `Active`: los datos se replican desde el origen de integración en Amazon Redshift.
  - `Error`: se ha producido un error en la integración.
  - `Recovering`: la integración se está recuperando después de que se haya reiniciado el almacenamiento de datos.
  - `Resyncing`: Amazon Redshift está volviendo a sincronizar las tablas de la integración.
- Tipo de destino es el tipo de almacenamiento de datos de Amazon Redshift.
- Fecha de creación es la fecha y hora (UTC) de creación de la integración.

> **Note**
>
> Para ver los detalles de la integración de un almacenamiento de datos, elija la página de detalles del clúster aprovisionado o del espacio de nombres sin servidor y, a continuación, elija la pestaña Integraciones sin ETL.

En la lista de integraciones sin ETL, puede elegir Datos de consulta para ir al editor de consultas v2 de Amazon Redshift. La base de datos de destino de Amazon Redshift tiene activado el parámetro enable_case_sensitive_identifier. Al escribir SQL, es posible que tenga que escribir los esquemas, las tablas y los nombres de las columnas entre comillas dobles ("<nombre>"). Para obtener más información sobre la consulta de datos en su almacenamiento de datos de Amazon Redshift, consulte Consulta de una base de datos mediante el editor de consultas v2 de Amazon Redshift.

En la lista de integraciones sin ETL, puede elegir Compartir datos para crear un recurso compartido de datos. Para crear un recurso compartido de datos para la base de datos de Amazon Redshift, siga las instrucciones de la página Crear un recurso compartido de datos. Para poder compartir datos en su base de datos de Amazon Redshift, primero debe crear una base de datos de destino. Para obtener más información sobre cómo compartir datos, consulte Conceptos sobre el uso compartido de datos para Amazon Redshift.

Para actualizar la integración, puede usar el comando ALTER DATABASE. Al hacerlo, se replican todos los datos del origen de integración en la base de datos de destino. En el siguiente ejemplo se actualizan todas las tablas sincronizadas y con errores de la integración sin ETL.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

Uso compartido de datos en Amazon Redshift

Después de agregar datos en el origen, estos se replican inmediatamente en Amazon Redshift y ya se pueden compartir mediante la creación de recursos compartidos de datos.

Para compartir datos, primero debe crear una base de datos de destino.

> **Important**
>
> Para compartir datos de un almacenamiento de datos de vista previa de Amazon Redshift con un almacenamiento de datos del consumidor de Amazon Redshift, su almacenamiento de datos del consumidor debe estar en la pista `preview_2023`. Para obtener más información sobre el uso compartido de datos, consulte ¿Qué es un recurso compartido de datos? en la Guía para desarrolladores de bases de datos de Amazon Redshift.
> Para crear un almacenamiento de datos de destino en vista previa, consulte uno de los siguientes temas en función de su tipo de implementación:
>
> - Clúster aprovisionado de Amazon Redshift: Crear un clúster de vista previa

- Grupo de trabajo de Redshift sin servidor: Crear un grupo de trabajo de vista previa

Uso compartido de datos en Amazon Redshift sin servidor mediante la consola de Amazon Redshift

1. En la consola de Amazon Redshift, en el panel de navegación de la izquierda, elija Amazon Redshift sin servidor > Panel sin servidor.
2. Elija Integraciones sin ETL en el panel de navegación.
3. Elija Share data (Compartir datos).
4. En la página de creación de un recurso compartido de datos, siga los pasos que se indican en Creación de recursos compartidos de datos.

Uso compartido de datos para clústeres aprovisionados de Amazon Redshift mediante la consola de Amazon Redshift

1. En la consola de Amazon Redshift, en el panel de navegación de la izquierda, elija Panel de clústeres aprovisionados.
2. Elija Integraciones sin ETL en el panel de navegación.
3. En la lista de integraciones, seleccione una integración.
4. En la página de detalles de la integración, elija Conectarse a la base de datos.
5. En la página Conexión a la base de datos, puede crear una conexión nueva o utilizar una reciente. Asegúrese de que la conexión esté hecha con la base de datos de destino.
6. Si crea una conexión nueva, introduzca un Nombre de base de datos para la base de datos. A continuación, haga clic en Conectar.
7. En la página de detalles de la integración, elija Compartir datos.
8. En la página de creación de un recurso compartido de datos, siga los pasos que se indican en Creación de recursos compartidos de datos.

Métricas para integraciones sin ETL

También puede utilizar las métricas de la consola de Amazon Redshift y Amazon CloudWatch para obtener información sobre el estado y el rendimiento de sus integraciones sin ETL. Puede

ajustar las métricas para que muestren datos de menor o mayor duración, o elegir ver las métricas en CloudWatch. Para ver las métricas de su integración en la consola de Amazon Redshift, elija Integraciones sin ETL en el panel de navegación de la izquierda y seleccione su ID de integración.

Para las integraciones sin ETL de Aurora y Amazon RDS, Amazon Redshift proporciona dos tipos de métricas en la página de detalles de la integración de una integración. Los tipos de métricas son las siguientes:

- En la pestaña Métricas de integración, estos son los gráficos disponibles:

Métrica	Descripción
`Lag`	Retardo desde el momento en que los datos se confirman en su origen hasta el momento en que están disponibles para las consultas en Amazon Redshift. Unidades: segundo Dimensiones: `IntegrationLag`
`Tables replicated`	Número de tablas que se han replicado desde su base de datos de origen en Amazon Redshift. Unidades: recuento Dimensiones: `IntegrationNumTablesReplicated`
`Tables failed`	Número de tablas que no se han replicado. Unidades: recuento Dimensiones: `IntegrationNumTablesFailedReplication`

- En la pestaña Estadísticas de la tabla, puede ver la lista de tablas activas o con errores. Las estadísticas de esta pestaña son las siguientes:
  - Nombre del esquema: nombre del esquema en el que se encuentra la tabla.
  - Nombre de la tabla: nombre de la tabla en la base de datos de origen.
  - Estado: estado de la tabla. Entre los valores posibles se incluyen `Synced`, `Failed`, `Deleted`, `Resync Required` y `Resync Initiated`.

- Base de datos: la base de datos de Amazon Redshift en la que se encuentra la tabla.
- Última actualización: fecha y hora (UTC) en que se ha actualizado la tabla por última vez.

Solución de problemas de integración sin ETL

Solución de problemas de integraciones sin ETL con Aurora MySQL

Utilice la siguiente información para solucionar problemas habituales relacionados con las integraciones sin ETL con Aurora MySQL.

Temas

- Error en la creación de la integración
- Las tablas no tienen claves principales
- Tipos de datos no admitidos en las tablas
- Error en los comandos del lenguaje de manipulación de datos
- Los cambios de los que se hecho el seguimiento entre orígenes de datos no coinciden
- Error de autorización
- El número de tablas es superior a 100 000 o el número de esquemas es superior a 4950
- Amazon Redshift no puede cargar datos
- La configuración de los parámetros del grupo de trabajo es incorrecta
- No se ha creado una base de datos para activar una integración sin ETL
- La tabla tiene el estado Resincronización requerida o Resincronización iniciada

Error en la creación de la integración

Si se ha producido un error en la creación de la integración sin ETL, el estado de la integración es `Inactive`. Asegúrese de que lo siguiente sea correcto para su clúster de base de datos de Aurora de origen:

- Ha creado el clúster en la consola de Amazon RDS.
- El clúster de base de datos de Aurora de origen ejecuta la versión 3.05 o superior de MySQL. Para validarlo, vaya a la pestaña Configuración del clúster y compruebe la Versión del motor.
- Ha establecido correctamente la configuración de los parámetros de binlog para el clúster. Si los parámetros de su binlog de Aurora MySQL están establecidos de forma incorrecta o no están

asociados con el clúster de base de datos de Aurora de origen, se produce un error en la creación. Consulte Configuración de los parámetros del clúster de base de datos.

Además, asegúrese de que lo siguiente sea correcto para su almacenamiento de datos de Amazon Redshift:

- Está activada la distinción entre mayúsculas y minúsculas. Consulte Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos.
- Ha agregado la entidad principal autorizada y el origen de integración correctos para su espacio de nombres. Consulte Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.

Las tablas no tienen claves principales

En la base de datos de destino, una o varias de las tablas no tienen clave principal y no se pueden sincronizar.

Para resolver este problema, vaya a la pestaña Estadísticas de la tabla en la página de detalles de integración o utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. También puede agregar claves principales a las tablas y Amazon Redshift volverá a sincronizarlas. Como alternativa, aunque no se recomienda, puede eliminar estas tablas en Aurora y crear tablas con una clave principal. Para obtener más información, consulte Prácticas recomendadas de Amazon Redshift para el diseño de tablas.

Tipos de datos no admitidos en las tablas

En la base de datos que ha creado a partir de la integración en Amazon Redshift y en la que se replican datos desde el clúster de base de datos de Aurora, una o varias de las tablas tienen tipos de datos no compatibles y no se pueden sincronizar.

Para resolver este problema, vaya a la pestaña Estadísticas de la tabla en la página de detalles de integración o utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. A continuación, elimine estas tablas y vuelva a crear tablas nuevas en Amazon RDS. Para obtener más información sobre los tipos de datos no compatibles, consulte Diferencias de tipos de datos entre las bases de datos de Aurora y Amazon Redshift en la Guía del usuario de Amazon Aurora.

Error en los comandos del lenguaje de manipulación de datos

Amazon Redshift no ha podido ejecutar comandos DML en las tablas de Redshift. Para resolver este problema, utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. Amazon Redshift vuelve a sincronizar automáticamente las tablas para resolver este error.

Los cambios de los que se hecho el seguimiento entre orígenes de datos no coinciden

Este error se produce cuando los cambios entre Amazon Aurora y Amazon Redshift no coinciden, lo que provoca que la integración cambie a un estado `Failed`.

Para solucionarlo, elimine la integración sin ETL y vuelva a crearla en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

Error de autorización

Se ha producido un error en la autorización porque el clúster de base de datos de Aurora de origen se ha eliminado como origen de integración autorizado para el almacenamiento de datos de Amazon Redshift.

Para solucionar este problema, elimine la integración sin ETL y vuelva a crearla en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

El número de tablas es superior a 100 000 o el número de esquemas es superior a 4950

Para un almacenamiento de datos de destino, el número de tablas es superior a 100 000 o el número de esquemas es superior a 4950. Amazon Aurora no puede enviar datos a Amazon Redshift. El número de tablas y esquemas supera el límite establecido. Para solucionar este problema, elimine los esquemas o las tablas innecesarios de la base de datos de origen.

Amazon Redshift no puede cargar datos

Amazon Redshift no puede cargar datos en la integración sin ETL.

Para resolver este problema, elimine la integración sin ETL en Amazon RDS y vuelva a crearla. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

La configuración de los parámetros del grupo de trabajo es incorrecta

Su grupo de trabajo no tiene activada la distinción entre mayúsculas y minúsculas.

Para resolver este problema, vaya a la pestaña Propiedades en la página de detalles de integración, elija el grupo de parámetros y active el identificador de distinción entre mayúsculas y minúsculas en la pestaña Propiedades. Si no tiene un grupo de parámetros existente, cree uno con el identificador de distinción entre mayúsculas y minúsculas activado. A continuación, cree una nueva integración sin ETL en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL.

No se ha creado una base de datos para activar una integración sin ETL

No hay una base de datos creada para la integración sin ETL a fin de activarla.

Para resolver este problema, cree una base de datos para la integración. Para obtener más información, consulte Creación de bases de datos de destino en Amazon Redshift.

La tabla tiene el estado Resincronización requerida o Resincronización iniciada

Su tabla tiene el estado Resincronización requerida o Resincronización iniciada.

Para recopilar información de error más detallada sobre por qué la tabla tiene ese estado, utilice la vista de sistema SYS_LOAD_ERROR_DETAIL.

Solución de problemas de integraciones sin ETL con Aurora PostgreSQL

Utilice la siguiente información para solucionar problemas habituales relacionados con las integraciones sin ETL con Aurora PostgreSQL.

Temas

- Error en la creación de la integración
- Las tablas no tienen claves principales
- Tipos de datos no admitidos en las tablas
- Error en los comandos del lenguaje de manipulación de datos
- Los cambios de los que se hecho el seguimiento entre orígenes de datos no coinciden
- Error de autorización
- El número de tablas es superior a 100 000 o el número de esquemas es superior a 4950
- Amazon Redshift no puede cargar datos
- La configuración de los parámetros del grupo de trabajo es incorrecta
- No se ha creado una base de datos para activar una integración sin ETL

- La tabla tiene el estado Resincronización requerida o Resincronización iniciada

Error en la creación de la integración

Si se ha producido un error en la creación de la integración sin ETL, el estado de la integración es `Inactive`. Asegúrese de que lo siguiente sea correcto para su clúster de base de datos de Aurora de origen:

- Ha creado el clúster en la consola de Amazon RDS.
- Su clúster de base de datos de Aurora de origen está ejecutando Aurora PostgreSQL versión 15.4.99 o superior. Para validarlo, vaya a la pestaña Configuración del clúster y compruebe la Versión del motor.
- Ha establecido correctamente la configuración de los parámetros de binlog para el clúster. Si los parámetros de su binlog de Aurora PostgreSQL están establecidos de forma incorrecta o no están asociados con el clúster de base de datos de Aurora de origen, se produce un error en la creación. Consulte Configuración de los parámetros del clúster de base de datos.

Además, asegúrese de que lo siguiente sea correcto para su almacenamiento de datos de Amazon Redshift:

- Está activada la distinción entre mayúsculas y minúsculas. Consulte Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos.
- Ha agregado la entidad principal autorizada y el origen de integración correctos para su espacio de nombres. Consulte Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.

Las tablas no tienen claves principales

En la base de datos de destino, una o varias de las tablas no tienen clave principal y no se pueden sincronizar.

Para resolver este problema, vaya a la pestaña Estadísticas de la tabla en la página de detalles de integración o utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. También puede agregar claves principales a las tablas y Amazon Redshift volverá a sincronizarlas. Como alternativa, aunque no se recomienda, puede eliminar estas tablas en Aurora y crear tablas con una clave principal. Para obtener más información, consulte Prácticas recomendadas de Amazon Redshift para el diseño de tablas.

Tipos de datos no admitidos en las tablas

En la base de datos que ha creado a partir de la integración en Amazon Redshift y en la que se replican datos desde el clúster de base de datos de Aurora, una o varias de las tablas tienen tipos de datos no compatibles y no se pueden sincronizar.

Para resolver este problema, vaya a la pestaña Estadísticas de la tabla en la página de detalles de integración o utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. A continuación, elimine estas tablas y vuelva a crear tablas nuevas en Amazon RDS. Para obtener más información sobre los tipos de datos no compatibles, consulte Diferencias de tipos de datos entre las bases de datos de Aurora y Amazon Redshift en la Guía del usuario de Amazon Aurora.

Error en los comandos del lenguaje de manipulación de datos

Amazon Redshift no ha podido ejecutar comandos DML en las tablas de Redshift. Para resolver este problema, utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. Amazon Redshift vuelve a sincronizar automáticamente las tablas para resolver este error.

Los cambios de los que se hecho el seguimiento entre orígenes de datos no coinciden

Este error se produce cuando los cambios entre Amazon Aurora y Amazon Redshift no coinciden, lo que provoca que la integración cambie a un estado `Failed`.

Para solucionarlo, elimine la integración sin ETL y vuelva a crearla en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

Error de autorización

Se ha producido un error en la autorización porque el clúster de base de datos de Aurora de origen se ha eliminado como origen de integración autorizado para el almacenamiento de datos de Amazon Redshift.

Para solucionar este problema, elimine la integración sin ETL y vuelva a crearla en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

El número de tablas es superior a 100 000 o el número de esquemas es superior a 4950

Para un almacenamiento de datos de destino, el número de tablas es superior a 100 000 o el número de esquemas es superior a 4950. Amazon Aurora no puede enviar datos a Amazon Redshift. El

número de tablas y esquemas supera el límite establecido. Para solucionar este problema, elimine los esquemas o las tablas innecesarios de la base de datos de origen.

Amazon Redshift no puede cargar datos

Amazon Redshift no puede cargar datos en la integración sin ETL.

Para resolver este problema, elimine la integración sin ETL en Amazon RDS y vuelva a crearla. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

La configuración de los parámetros del grupo de trabajo es incorrecta

Su grupo de trabajo no tiene activada la distinción entre mayúsculas y minúsculas.

Para resolver este problema, vaya a la pestaña Propiedades en la página de detalles de integración, elija el grupo de parámetros y active el identificador de distinción entre mayúsculas y minúsculas en la pestaña Propiedades. Si no tiene un grupo de parámetros existente, cree uno con el identificador de distinción entre mayúsculas y minúsculas activado. A continuación, cree una nueva integración sin ETL en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL.

No se ha creado una base de datos para activar una integración sin ETL

No hay una base de datos creada para la integración sin ETL a fin de activarla.

Para resolver este problema, cree una base de datos para la integración. Para obtener más información, consulte Creación de bases de datos de destino en Amazon Redshift.

La tabla tiene el estado Resincronización requerida o Resincronización iniciada

Su tabla tiene el estado Resincronización requerida o Resincronización iniciada.

Para recopilar información de error más detallada sobre por qué la tabla tiene ese estado, utilice la vista de sistema SYS_LOAD_ERROR_DETAIL.

Solución de problemas de integraciones sin ETL con RDS para MySQL

Utilice la siguiente información para solucionar problemas habituales relacionados con las integraciones sin ETL con RDS para MySQL.

Temas

- Error en la creación de la integración

- Las tablas no tienen claves principales
- Tipos de datos no admitidos en las tablas
- Error en los comandos del lenguaje de manipulación de datos
- Los cambios de los que se hecho el seguimiento entre orígenes de datos no coinciden
- Error de autorización
- El número de tablas es superior a 100 000 o el número de esquemas es superior a 4950
- Amazon Redshift no puede cargar datos
- La configuración de los parámetros del grupo de trabajo es incorrecta
- No se ha creado una base de datos para activar una integración sin ETL
- La tabla tiene el estado Resincronización requerida o Resincronización iniciada

Error en la creación de la integración

Si se ha producido un error en la creación de la integración sin ETL, el estado de la integración es `Inactive`. Asegúrese de que lo siguiente sea correcto para su instancia de base de datos de RDS de origen:

- Ha creado la instancia en la consola de Amazon RDS.
- La instancia de base de datos de origen de RDS debe utilizar la versión 8.0.28 de RDS para MySQL o superior. Para validarlo, vaya a la pestaña Configuración de la instancia y compruebe la Versión del motor.
- Ha configurado correctamente los parámetros de binlog para la instancia. Si los parámetros de su binlog de RDS para MySQL están establecidos de forma incorrecta o no están asociados con la instancia de base de datos de RDS de origen, se produce un error en la creación. Consulte Configurar los parámetros de la instancia de base de datos.

Además, asegúrese de que lo siguiente sea correcto para su almacenamiento de datos de Amazon Redshift:

- Está activada la distinción entre mayúsculas y minúsculas. Consulte Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos.
- Ha agregado la entidad principal autorizada y el origen de integración correctos para su espacio de nombres. Consulte Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.

Las tablas no tienen claves principales

En la base de datos de destino, una o varias de las tablas no tienen clave principal y no se pueden sincronizar.

Para resolver este problema, vaya a la pestaña Estadísticas de la tabla en la página de detalles de integración o utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. También puede agregar claves principales a las tablas y Amazon Redshift volverá a sincronizarlas. Como alternativa, aunque no se recomienda, puede eliminar estas tablas en RDS y crear tablas con una clave principal. Para obtener más información, consulte Prácticas recomendadas de Amazon Redshift para el diseño de tablas.

Tipos de datos no admitidos en las tablas

En la base de datos que ha creado a partir de la integración en Amazon Redshift y en la que se replican datos desde la instancia de base de datos de RDS, una o varias de las tablas tienen tipos de datos no compatibles y no se pueden sincronizar.

Para resolver este problema, vaya a la pestaña Estadísticas de la tabla en la página de detalles de integración o utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. A continuación, elimine estas tablas y vuelva a crear tablas nuevas en Amazon RDS. Para obtener más información sobre los tipos de datos no compatibles, consulte Diferencias de tipos de datos entre las bases de datos de RDS y Amazon Redshift en la Guía del usuario de Amazon Aurora.

Error en los comandos del lenguaje de manipulación de datos

Amazon Redshift no ha podido ejecutar comandos DML en las tablas de Redshift. Para resolver este problema, utilice SVV_INTEGRATION_TABLE_STATE para ver las tablas con errores. Amazon Redshift vuelve a sincronizar automáticamente las tablas para resolver este error.

Los cambios de los que se hecho el seguimiento entre orígenes de datos no coinciden

Este error se produce cuando los cambios entre Amazon Aurora y Amazon Redshift no coinciden, lo que provoca que la integración cambie a un estado `Failed`.

Para solucionarlo, elimine la integración sin ETL y vuelva a crearla en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

Error de autorización

Se ha producido un error en la autorización porque la instancia de base de datos de RDS de origen se ha eliminado como origen de integración autorizado para el almacenamiento de datos de Amazon Redshift.

Para solucionar este problema, elimine la integración sin ETL y vuelva a crearla en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

El número de tablas es superior a 100 000 o el número de esquemas es superior a 4950

Para un almacenamiento de datos de destino, el número de tablas es superior a 100 000 o el número de esquemas es superior a 4950. Amazon Aurora no puede enviar datos a Amazon Redshift. El número de tablas y esquemas supera el límite establecido. Para solucionar este problema, elimine los esquemas o las tablas innecesarios de la base de datos de origen.

Amazon Redshift no puede cargar datos

Amazon Redshift no puede cargar datos en la integración sin ETL.

Para resolver este problema, elimine la integración sin ETL en Amazon RDS y vuelva a crearla. Para obtener más información, consulte Creación de integraciones sin ETL y Eliminación de las integraciones sin ETL.

La configuración de los parámetros del grupo de trabajo es incorrecta

Su grupo de trabajo no tiene activada la distinción entre mayúsculas y minúsculas.

Para resolver este problema, vaya a la pestaña Propiedades en la página de detalles de integración, elija el grupo de parámetros y active el identificador de distinción entre mayúsculas y minúsculas en la pestaña Propiedades. Si no tiene un grupo de parámetros existente, cree uno con el identificador de distinción entre mayúsculas y minúsculas activado. A continuación, cree una nueva integración sin ETL en Amazon RDS. Para obtener más información, consulte Creación de integraciones sin ETL.

No se ha creado una base de datos para activar una integración sin ETL

No hay una base de datos creada para la integración sin ETL a fin de activarla.

Para resolver este problema, cree una base de datos para la integración. Para obtener más información, consulte Creación de bases de datos de destino en Amazon Redshift.

La tabla tiene el estado Resincronización requerida o Resincronización iniciada

Su tabla tiene el estado Resincronización requerida o Resincronización iniciada.

Para recopilar información de error más detallada sobre por qué la tabla tiene ese estado, utilice la vista de sistema SYS_LOAD_ERROR_DETAIL.

Consulta a una base de datos

Para consultar las bases de datos alojadas en el clúster de Amazon Redshift, tiene dos opciones:

- Conéctese a su clúster y ejecute consultas en la AWS Management Console con el editor de consultas.

  Si utiliza el editor de consultas en la consola de Amazon Redshift, no tiene que descargar ni configurar una aplicación de cliente SQL.
- Conéctese a su clúster a través de una herramienta de cliente SQL, como SQL Workbench/J.

  Amazon Redshift admite herramientas de cliente SQL que se conectan a través de Java Database Connectivity (JDBC) y Open Database Connectivity (ODBC). Amazon Redshift no proporciona ni instala ninguna biblioteca o herramienta de cliente SQL; por lo tanto, debe instalarlas en su equipo cliente o su instancia de Amazon EC2 para utilizarlas. Puede utilizar la mayoría de las herramientas de cliente SQL compatibles con los controladores JDBC u ODBC.

> **Note**
>
> Al escribir procedimientos almacenados, sugerimos una práctica recomendada para proteger los valores confidenciales:
> No codifique ninguna información confidencial en la lógica de procedimientos almacenada. Por ejemplo, no asigne una contraseña de usuario en una instrucción CREATE USER del cuerpo de un procedimiento almacenado. Esto supone un riesgo de seguridad, porque los valores codificados de forma rígida se pueden registrar como metadatos de esquema en las tablas del catálogo. En cambio, pase valores confidenciales, como las contraseñas, como argumentos al procedimiento almacenado, mediante parámetros.
> Para obtener más información acerca de los procedimientos almacenados, consultePROCEDIMIENTO DE CREACIÓNyCreación de procedimientos almacenados en Amazon Redshift. Para obtener más información acerca de las tablas de catálogos, consulte Tablas de catálogos de sistema.

Temas

- Consulta de una base de datos mediante el editor de consultas v2 de Amazon Redshift
- Consulta de una base de datos mediante el editor de consultas

- Conexión a un almacenamiento de datos de Amazon Redshift mediante herramientas de cliente SQL
- Uso de la API de datos de Amazon Redshift

Consulta de una base de datos mediante el editor de consultas v2 de Amazon Redshift

El editor de consultas v2 es una aplicación de cliente SQL independiente basada en web que se utiliza para crear y ejecutar consultas en el almacenamiento de datos de Amazon Redshift. Puede visualizar los resultados en gráficos y colaborar si comparte sus consultas con otros miembros del equipo. El editor de consultas v2 sustituye al editor de consultas anterior.

> **Note**
>
> El editor de consultas v2 está disponible en Regiones de AWS comerciales. Para obtener una lista de Regiones de AWS en las que está disponible el editor de consultas v2, consulte los puntos de conexión mostrados para Editor de consultas v2 de Redshift en la Referencia general de Amazon Web Services.

Para obtener una demostración del editor de consultas v2, vea el siguiente video. Editor de consultas de Amazon Redshift V2.

Para obtener una demostración del análisis de datos, vea el siguiente video. Análisis de datos mediante el editor de consultas de Amazon Redshift V2.

Para obtener una demostración del uso del editor de consultas v2 a la hora de ejecutar varias consultas con una conexión aislada o compartida, vea el siguiente video. Ejecución de consultas simultáneas con el editor de consultas v2.

El editor de consultas v2 tiene un amplio conjunto de características para administrar y ejecutar las instrucciones SQL. Los temas de las siguientes secciones sirven de introducción para muchas de estas características. Explore el editor de consultas v2 por su cuenta para familiarizarse con sus capacidades.

Temas

- Configuración de su Cuenta de AWS

- Trabajo con el editor de consultas v2
- Interacción con el SQL generativo del editor de consultas v2 (versión preliminar)
- Descarga de datos en una base de datos
- Creación y ejecución de consultas
- Creación y ejecución de cuadernos
- Consulta de AWS Glue Data Catalog
- Consulta de un lago de datos
- Uso de recursos compartidos de datos
- Programación de consultas con el editor de consultas versión 2
- Visualización de resultados de las consultas
- Colaboración y uso compartido en equipo

Configuración de su Cuenta de AWS

Cuando elige el editor de consultas v2 desde la consola de Amazon Redshift, se abre una pestaña nueva en el navegador con la interfaz del editor de consultas v2. Con los permisos adecuados, puede acceder a los datos de un clúster o grupo de trabajo de Amazon Redshift propiedad de su Cuenta de AWS en la Región de AWS actual.

La primera vez que un administrador configura el editor de consultas v2 para su Cuenta de AWS, este elige la AWS KMS key que se utiliza para cifrar los recursos del editor de consultas v2. De manera predeterminada, se utiliza una clave propia de AWS para cifrar los recursos. O bien, un administrador puede utilizar una clave administrada por el cliente seleccionando el nombre de recurso de Amazon (ARN) para la clave en la página de configuración. Luego de configurar una cuenta, la configuración de cifrado AWS KMS no se puede cambiar. Para obtener más información sobre cómo crear y utilizar una clave administrada por el cliente con el editor de consultas v2, consulte Creación de una clave AWS KMS administrada por el cliente para usar con el editor de consultas v2. El administrador también puede elegir opcionalmente un S3 bucket (Bucket de S3) y una ruta que se utilice para algunas características, como carga de datos de un archivo. Para obtener más información, consulte Configuración y flujo de trabajo de la carga de datos desde un archivo local.

El editor de consultas v2 de Amazon Redshift admite la autenticación, el cifrado, el aislamiento y la conformidad para mantener los datos en reposo y los datos en tránsito protegidos. Para obtener más información sobre la seguridad de datos y el editor de consultas v2, consulte lo siguiente:

- Cifrado en reposo
- Cifrado en tránsito
- Configuración y análisis de vulnerabilidades en Amazon Redshift

AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o que se realizan en nombre de esta. Además, entrega los archivos de registro a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que estas se realizaron. Para obtener más información sobre cómo se ejecuta el editor de consultas v2 en AWS CloudTrail, consulte Registro con CloudTrail. Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

El editor de consultas v2 tiene cuotas ajustables para algunos de sus recursos. Para obtener más información, consulte Cuotas para objetos de Amazon Redshift.

Recursos creados con el editor de consultas v2

En el editor de consultas v2, puede crear recursos como consultas y gráficos guardados. Todos los recursos del editor de consultas v2 están asociados a un rol de IAM o a un usuario. Recomendamos adjuntar políticas a un rol de IAM y asignar el rol a un usuario.

En el editor de consultas v2, puede agregar y eliminar etiquetas para consultas y gráficos guardados. Puede utilizar estas etiquetas al momento de configurar políticas de IAM personalizadas o para buscar recursos. También puede administrar las etiquetas mediante el editor de etiquetas de AWS Resource Groups.

Puede configurar roles de IAM con políticas de IAM para compartir consultas con otros usuarios en la misma Cuenta de AWS en la Región de AWS.

Creación de una clave AWS KMS administrada por el cliente para usar con el editor de consultas v2

Para crear una clave de cifrado simétrica administrada por el cliente:

Puede crear una clave de cifrado simétrica administrada por el cliente para cifrar los recursos del editor de consultas v2 mediante la consola de AWS KMS o las operaciones de la API de AWS KMS. Para obtener instrucciones sobre cómo crear una clave, consulte Creación de una clave de AWS KMS de cifrado simétrica en la Guía para desarrolladores de AWS Key Management Service.

Política de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administración del acceso a las claves AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Para utilizar la clave administrada por el cliente con el editor de consultas v2 de Amazon Redshift, se deben permitir las siguientes operaciones de API en la política de clave:

- `kms:GenerateDataKey`: genera una clave de datos simétrica única para cifrar los datos.
- `kms:Decrypt`: descifra los datos cifrados con la clave administrada por el cliente.
- `kms:DescribeKey`: proporciona los detalles de la clave administrada por el cliente para permitir que el servicio valide la clave.

La siguiente es una política de AWS KMS de ejemplo para la Cuenta de AWS `111122223333`. En la primera sección, `kms:ViaService` limita el uso de la clave al servicio del editor de consultas v2 (que se denomina `sqlworkbench.`*`region`*`.amazonaws.com` en la política). La Cuenta de AWS que utiliza la clave de debe ser `111122223333`. En la segunda sección, el usuario raíz y los administradores de clave de la Cuenta de AWS `111122223333` pueden acceder a la clave.

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy",
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon Redshift Query
 Editor V2",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "sqlworkbench.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:*"
            ],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        }
    ]
}
```

Los siguientes recursos proporcionan más información sobre claves AWS KMS:

- Para obtener más información sobre las políticas de AWS KMS, consulte Especificación de permisos en una política en la Guía para desarrolladores de AWS Key Management Service.
- Para obtener información sobre las políticas de solución de problemas de AWS KMS, consulte Solución de problemas de acceso a las claves en la Guía para desarrolladores de AWS Key Management Service.
- Para obtener más información sobre las claves, consulte Claves KMS de AWS en la Guía para desarrolladores de AWS Key Management Service.

Acceso al editor de consultas v2

Para obtener acceso al editor de consultas v2, necesita permiso. Un administrador puede adjuntar una de las siguientes políticas administradas de AWS al rol para conceder el permiso. (Recomendamos adjuntar políticas a un rol de IAM y asignar el rol a un usuario). Estas políticas administradas de AWS se escriben con diferentes opciones que controlan cómo los recursos de etiquetado permiten compartir consultas. Puede utilizar la consola de IAM (https://console.aws.amazon.com/iam/) para adjuntar políticas de IAM.

- AmazonRedshiftQueryEditorV2FullAccess: concede acceso completo a todos los recursos y las operaciones del editor de consultas v2 de Amazon Redshift. Esta política también concede acceso a otros servicios requeridos.
- AmazonRedshiftQueryEditorV2NoSharing: permite trabajar con el editor de consultas v2 de Amazon Redshift sin compartir recursos. Esta política también concede acceso a otros servicios requeridos.
- AmazonRedshiftQueryEditorV2ReadSharing: permite trabajar con el editor de consultas v2 de Amazon Redshift con uso compartido limitado de los recursos. La entidad principal concedida puede leer los recursos compartidos con su equipo, pero no puede actualizarlos. Esta política también concede acceso a otros servicios requeridos.
- AmazonRedshiftQueryEditorV2ReadWriteSharing: permite trabajar con el editor de consultas v2 de Amazon Redshift con uso compartido de recursos. La entidad principal concedida puede leer y actualizar los recursos compartidos con su equipo. Esta política también concede acceso a otros servicios requeridos.

También puede crear su propia política en función de los permisos permitidos y denegados en las políticas administradas proporcionadas. Si utiliza el editor de políticas de la consola de IAM para crear su propia política, elija SQL Workbench como servicio para el que crea la política en el editor visual. El editor de consultas v2 utiliza el nombre del servicio AWS SQL Workbench en el editor visual y el Simulador de políticas de IAM.

Para que una entidad principal (un usuario con un rol de IAM asignado) se conecte a un clúster de Amazon Redshift, necesita los permisos de una de las políticas administradas del editor de consultas v2. También necesitan el permiso `redshift:GetClusterCredentials` para el clúster. Para obtener este permiso, alguien con permiso administrativo puede adjuntar una política a los roles de IAM usados para conectarse al clúster mediante credenciales temporales. Puede delimitar el alcance de la política a clústeres específicos o hacerlo más general. Para obtener más información sobre los

permisos para usar credenciales temporales, consulte Crear un rol o usuario de IAM con permisos para llamar a GetClusterCredentials.

Para que una entidad principal (normalmente un usuario con un rol de IAM asignado) active la capacidad en la página Configuración de cuenta para que otras personas de la cuenta puedan Exportar conjunto de resultados, necesita el permiso `sqlworkbench:UpdateAcountExportSettings` asociado al rol. Este permiso está presente en la política administrada por AWS `AmazonRedshiftQueryEditorV2FullAccess`.

A medida que se agregan nuevas características al editor de consultas v2, las políticas administradas de AWS se actualizan según sea necesario. Si crea su propia política basándose en los permisos permitidos y denegados en las políticas administradas proporcionadas, edite sus políticas para mantenerlas actualizadas con los cambios en las políticas administradas. Para obtener más información sobre las políticas administradas en Amazon Redshift, consulte Políticas administradas por AWS para Amazon Redshift.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

> **Note**
>
> Si un administrador de AWS IAM Identity Center elimina todas las asociaciones de conjuntos de permisos de un conjunto de permisos concreto en toda la cuenta, ya no se podrá acceder a los recursos del editor de consultas asociados originalmente al conjunto de permisos

eliminado. Si más adelante se vuelven a crear los mismos permisos, se crea un nuevo identificador interno. Como el identificador interno ha cambiado, no se puede acceder a los recursos del editor de consultas que anteriormente eran propiedad de un usuario. Se recomienda que, antes de que los administradores eliminen un conjunto de permisos, los usuarios de ese conjunto de permisos realicen copias de seguridad de los recursos del editor de consultas, como los cuadernos y las consultas.

Configuración de etiquetas de entidad principal para conectar un clúster o grupo de trabajo desde el editor de consultas v2

Para conectarse al clúster o grupo de trabajo mediante la opción de usuario federado, configure el rol o usuario de IAM con etiquetas de entidades principales. O bien, configure el proveedor de identidades (IdP) para que pase `RedshiftDbUser` y (opcionalmente) `RedshiftDbGroups`. Para obtener más información acerca del uso de IAM para administrar etiquetas, consulte Transferencia de etiquetas de sesión en AWS Security Token Service en la Guía del usuario de IAM. Para configurar el acceso mediante AWS Identity and Access Management, un administrador puede agregar etiquetas mediante la consola de IAM (https://console.aws.amazon.com/iam/).

Para agregar etiquetas de entidades principales a un rol de IAM

1. Inicie sesión en AWS Management Console y abra la consola IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija el rol que necesita acceso al editor de consultas v2 mediante un usuario federado.
4. Elija la pestaña Tags (Etiquetas).
5. Elija Manage tags (Administrar etiquetas).
6. Elija Add tag (Agregar etiqueta) e ingrese la Key (Clave) como `RedshiftDbUser` e ingrese un Value (Valor) del nombre de usuario federado.
7. Si lo desea, elija Add tag (Agregar etiqueta) e ingrese la Key (Clave) como `RedshiftDbGroups` e ingrese un Value (Valor) del nombre de grupo que se va a asociar al usuario.
8. Elija Save changes (Guardar cambios) para ver la lista de etiquetas asociadas al rol de IAM elegido. Es posible que la propagación de los cambios tarde varios segundos.
9. Para utilizar el usuario federado, actualice la página del editor de consultas v2 después de que se hayan propagado los cambios.

Configure el proveedor de identidades (IdP) para pasar etiquetas de entidades principales

El procedimiento para configurar etiquetas mediante un proveedor de identidades (IdP) varía según el IdP. Consulte la documentación del IdP para obtener instrucciones sobre cómo transferir información de usuario y grupo a los atributos de SAML. Cuando se configura correctamente, aparecen los siguientes atributos en la respuesta de SAML que utiliza AWS Security Token Service para rellenar las etiquetas de entidades principales para `RedshiftDbUser` y `RedshiftDbGroups`.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbUser">
    <AttributeValue>db-user-name</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbGroups">
    <AttributeValue>db-groups</AttributeValue>
</Attribute>
```

El *db_groups* opcional debe ser una lista separada por dos puntos, como `group1:group2:group3`.

Además, puede configurar el atributo `TransitiveTagKeys` para conservar las etiquetas durante el encadenamiento de roles.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

Para obtener más información sobre la configuración del editor de consultas v2, consulte Permisos necesarios para usar del editor de consultas v2 .

> **Note**
>
> Cuando se conecta a su clúster o grupo de trabajo mediante la opción de conexión Usuario federado del editor de consultas v2, el proveedor de identidades (IdP) puede proporcionar etiquetas de entidades principales personalizadas para `RedshiftDbUser` y `RedshiftDbGroups`. Actualmente, AWS IAM Identity Center no admite pasar etiquetas de entidades principales personalizadas directamente al editor de consultas v2.

Trabajo con el editor de consultas v2

El editor de consultas v2 se utiliza principalmente para editar y ejecutar consultas, visualizar resultados y compartir su trabajo con su equipo. Con el editor de consultas v2, puede crear bases de datos, esquemas, tablas y funciones definidas por el usuario (UDF). En un panel de vista de árbol, para cada una de las bases de datos, puede ver sus esquemas. Para cada esquema, puede ver sus tablas, vistas, UDF y procedimientos almacenados.

Temas

- Apertura del editor de consultas v2
- Conexión a una base de datos de Amazon Redshift
- Exploración de una base de datos de Amazon Redshift
- Creación de objetos de base de datos
- Visualización del historial de consultas y pestañas
- Consideraciones al trabajar con el editor de consultas v2
- Modificación de la configuración de la cuenta

Apertura del editor de consultas v2

Para abrir el editor de consultas v2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú del navegador, elija Editor (Editor) y luego Query editor v2 (Editor de consultas v2). El editor de consultas v2 se abre en una pestaña nueva del navegador.

La página del editor de consultas contiene un menú de navegación que permite elegir una vista de la siguiente manera:

Editor

Administre y consulte los datos organizados como tablas y contenidos en una base de datos. La base de datos puede contener datos almacenados o una referencia a los datos almacenados en

otro lugar, como Amazon S3. Se conecta a una base de datos contenida en un clúster o en un grupo de trabajo sin servidor.

Cuando se trabaja en la vista Editor, tiene los siguientes controles:

- En el campo Cluster (Clúster) o Workgroup (Grupo de trabajo), se muestra el nombre al que está conectado actualmente. En el campo Database (Base de datos) se muestran las bases de datos del clúster o grupo de trabajo. Las acciones que realiza en la vista Database (Base de datos) actúan de manera predeterminada en la base de datos que seleccionó.
- Una vista jerárquica de vista de árbol de los clústeres o grupos de trabajo, bases de datos y esquemas. En la sección de esquemas, puede trabajar con tablas, vistas, funciones y procedimientos almacenados. Cada objeto de la vista de árbol admite un menú contextual para realizar acciones asociadas para el objeto, como Refresh (Actualizar) o Drop (Eliminar).
- Una acción

  Create (Crear) para crear bases de datos, esquemas, tablas y funciones.
- Una acción

  Cargar datos para cargar datos desde Amazon S3 o desde un archivo local en la base de datos.
- Un icono

  Save (Guardar) para guardar la consulta.
- Un icono

  Shortcuts (Atajos) para mostrar atajos de teclado para el editor.
- Un icono

  Más para mostrar más acciones en el editor. Por ejemplo:
  - Compartir con mi equipo: compartir un cuaderno con su equipo. Para obtener más información, consulte Colaboración y uso compartido en equipo.
  - Atajos para mostrar atajos de teclado para el editor.
  - Historial de pestañas para mostrar el historial de pestañas de una pestaña en el editor.
  - Actualizar autocompletar para actualizar las sugerencias mostradas al crear SQL.

- Un área del Editor de

  en la que puede introducir y ejecutar la consulta.

  Después de ejecutar una consulta, aparece una pestaña denominada Result (Resultado) con los resultados. Aquí es donde puede activar Chart (Gráfico) para visualizar los resultados. También puede exportar sus resultados mediante Export (Exportar).

- Un área del Notebook

  en la que puede agregar secciones para introducir y ejecutar SQL o agregar Markdown.

  Después de ejecutar una consulta, aparece una pestaña denominada Result (Resultado) con los resultados. Es aquí donde puede exportar sus resultados mediante Export (Exportar).

Consultas

Una consulta contiene los comandos SQL para administrar y consultar los datos de una base de datos. Cuando utiliza el editor de consultas v2 para cargar datos de ejemplo, también crea y guarda consultas de ejemplo para usted.

Cuando elige una consulta guardada, puede abrirla, cambiarle el nombre y eliminarla mediante el menú contextual (haga clic con el botón derecho). Para ver atributos como el ARN de la consulta de una consulta guardada, elija Detalles de la consulta. También puede ver su historial de versiones, editar las etiquetas adjuntadas a la consulta y compartirla con su equipo.

Notebooks

Un SQL Notebook contiene celdas SQL y Markdown. Puede utilizar SQL Notebooks para organizar, anotar y compartir varios comandos SQL en un solo documento.

Cuando elige un cuaderno guardado, puede abrirlo, cambiarle el nombre y eliminarlo mediante el menú contextual (haga clic con el botón derecho). Para ver atributos como el ARN del cuaderno de un cuaderno guardado, elija Detalles del bloc de notas. También puede ver su historial de versiones, editar las etiquetas adjuntadas al cuaderno, exportarlo y compartirlo con su equipo. Para obtener más información, consulte Creación y ejecución de cuadernos.

Gráficos

Un gráfico es una representación visual de sus datos. El editor de consultas v2 proporciona herramientas para crear muchos tipos de gráficos y guardarlos.

Cuando elige un gráfico guardado, puede abrirlo, cambiarle el nombre y eliminarlo mediante el menú contextual (haga clic con el botón derecho). Para ver atributos como el ARN del gráfico de un gráfico guardado, elija Detalles del gráfico. También puede editar las etiquetas adjuntadas al gráfico y exportarlo. Para obtener más información, consulte Visualización de resultados de las consultas.

Historial

El historial de consultas es una lista de consultas a la hora de ejecutar mediante el editor de consultas v2 de Amazon Redshift. Estas consultas se ejecutaron como consultas individuales o como parte de un SQL notebook. Para obtener más información, consulte Visualización del historial de consultas y pestañas.

Consultas programadas

Una consulta programada es una consulta que se configura para que se inicie en momentos específicos.

En todas las vistas del editor de consultas v2 están presentes los siguientes iconos:

- Un icono Visual mode (Modo visual)

  , para alternar entre el modo claro y el modo oscuro.
- Un icono Settings (Configuración)

  , para abrir un menú de las diferentes pantallas de configuración.

- Un icono Editor preferences (Preferencias del editor)

  ,
  para editar las preferencias al utilizar el editor de consultas v2. Aquí puede Editar la configuración del espacio de trabajo para cambiar el tamaño de la fuente, el tamaño de las pestañas y otras configuraciones de visualización. También puede activar (o desactivar) Autocompletar para que le muestre sugerencias a medida que introduce su código SQL.
- Un icono Connections (Conexiones)

  ,
  para ver las conexiones utilizadas por las pestañas del editor.

  Se utiliza una conexión para recuperar datos de una base de datos. Se crea una conexión para una base de datos específica. Con una conexión aislada, los resultados de un comando SQL que cambia la base de datos (por medio de, por ejemplo, la creación de una tabla temporal) en una pestaña del editor no son visibles en otra pestaña del editor. Al abrir una pestaña del editor en el editor de consultas v2, el valor predeterminado es una conexión aislada. Al crear una conexión compartida, es decir, cuando se desactiva el conmutador Isolated session (Sesión aislada), los resultados de otras conexiones compartidas con la misma base de datos son visibles entre sí. Sin embargo, las pestañas del editor que utilizan una conexión compartida en una base de datos no se ejecutan en paralelo. Las consultas que utilizan una misma conexión deben esperar hasta que dicha conexión esté disponible. Una conexión con una base de datos no se puede compartir con otra base de datos. En consecuencia, los resultados de SQL no son visibles en diferentes conexiones de base de datos.

  Un administrador del editor de consultas v2 controla el número de conexiones que cualquier usuario de la cuenta puede tener activas.
- Un icono Account settings (Configuración de cuenta)

  ,
  por medio del cual un administrador puede cambiar ciertos ajustes de todos los usuarios de la cuenta. Para obtener más información, consulte Modificación de la configuración de la cuenta.

Conexión a una base de datos de Amazon Redshift

Para conectarse a una base de datos, elija el nombre del clúster o grupo de trabajo en el panel de vista de árbol. Si se le solicita, ingrese los parámetros de conexión.

Cuando se conecta a un clúster o grupo de trabajo y sus bases de datos, normalmente debe proporcionar un nombre de Database (Base de datos). También debe proporcionar los parámetros necesarios para uno de los siguientes métodos de autenticación:

IAM Identity Center

Con este método, conéctese a su almacenamiento de datos de Amazon Redshift con las credenciales de inicio de sesión único de su proveedor de identidades (IdP). Su clúster o grupo de trabajo debe estar habilitado para el Centro de identidades de IAM en la consola de Amazon Redshift.

Usuario federado

Con este método, las etiquetas de entidades principales del rol o usuario de IAM deben proporcionar los detalles de la conexión. Estas etiquetas se configuran en AWS Identity and Access Management o el proveedor de identidades (IdP). El editor de consultas v2 se basa en las siguientes etiquetas.

- `RedshiftDbUser`: esta etiqueta define el usuario de base de datos que utiliza el editor de consultas v2. Esta etiqueta es necesaria.
- `RedshiftDbGroups`: esta etiqueta define los grupos de bases de datos que se unen al conectarse al editor de consultas v2. Esta etiqueta es opcional y su valor debe ser una lista separada por dos puntos, como `group1:group2:group3`. Los valores vacíos se ignoran, es decir, `group1:::group2` se interpreta como `group1:group2`.

Estas etiquetas se reenvían a la API `redshift:GetClusterCredentials` para obtener credenciales para el clúster. Para obtener más información, consulte Configuración de etiquetas de entidad principal para conectar un clúster o grupo de trabajo desde el editor de consultas v2.

Credenciales temporales con un nombre de usuario de base de datos

Esta opción solo está disponible cuando se conecta a un clúster. Con este método, el editor de consultas v2, proporcione un User name (Nombre de usuario) para la base de datos. El editor de consultas v2 genera una contraseña temporal para conectarse a la base de datos con su nombre de usuario de la base de datos. Un usuario que utilice este método para conectarse debe tener permiso de IAM para `redshift:GetClusterCredentials`. Para evitar que los usuarios utilicen este método, modifique su usuario o rol de IAM para denegar este permiso.

Credenciales temporales mediante su identidad de IAM

Esta opción solo está disponible cuando se conecta a un clúster. Con este método, el editor de consultas v2 asigna un nombre de usuario a su identidad de IAM y genera

una contraseña temporal para conectarse a la base de datos como su identidad de IAM. Un usuario que utilice este método para conectarse debe tener permiso de IAM para `redshift:GetClusterCredentialsWithIAM`. Para evitar que los usuarios utilicen este método, modifique su usuario o rol de IAM para denegar este permiso.

Nombre de usuario y contraseña de la base de datos

Con este método, también debe proporcionar un User name (Nombre de usuario) y una Password (Contraseña) para la base de datos a la que se está conectando. El editor de consultas v2 crea un secreto en su nombre almacenado en AWS Secrets Manager. Este secreto contiene las credenciales para conectarse a la base de datos.

AWS Secrets Manager

Con este método, en lugar de un nombre de base de datos, debe proporcionar un Secret (Secreto) almacenado en Secrets Manager que contenga su base de datos y sus credenciales de inicio de sesión. Para obtener información sobre cómo crear un secreto, consulte Creación de un secreto para las credenciales de conexión a la base de datos.

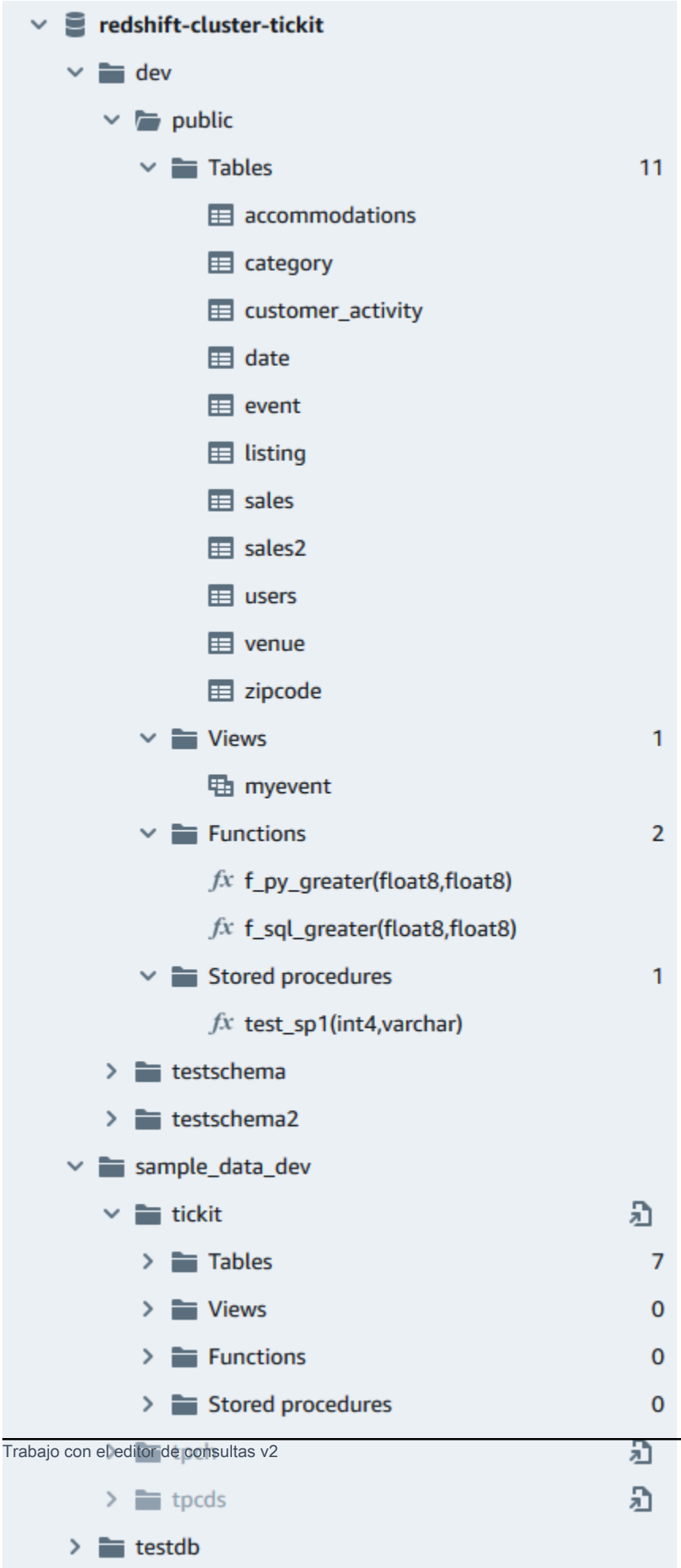
Cuando selecciona un clúster o grupo de trabajo con el editor de consultas v2, según el contexto, puede crear, editar y eliminar conexiones mediante el menú contextual (clic derecho). Para ver atributos como el ARN de conexión de la conexión, elija Detalles de la conexión. También puede editar las etiquetas adjuntadas a la conexión.

Exploración de una base de datos de Amazon Redshift

Dentro de una base de datos, puede administrar esquemas, tablas, vistas, funciones y procedimientos almacenados en el panel de vista de árbol. Cada objeto de la vista tiene acciones asociadas a él en un menú contextual (clic derecho).

El panel jerárquico de vista de árbol muestra los objetos de base de datos. Para actualizar el panel de vista de árbol para mostrar los objetos de la base de datos que es posible que se hayan creado después de la última visualización de la vista de árbol, elija el icono .

Abra el menú contextual (clic derecho) de un objeto para ver qué acciones puede realizar.


redshift-cluster-tickit
dev
public
Tables 11
accommodations
category
customer_activity
date
event
listing
sales
sales2
users
venue
zipcode
Views 1
myevent
Functions 2
f_py_greater(float8,float8)
f_sql_greater(float8,float8)
Stored procedures 1
test_sp1(int4,varchar)
testschema
testschema2
sample_data_dev
tickit
Tables 7
Views 0
Functions 0
Stored procedures 0
tpch
tpcds
testdb

Una vez que elige una tabla, puede hacer lo siguiente:

- Para iniciar una consulta en el editor con una instrucción SELECT que consulta todas las columnas de la tabla, utilice Select table (Seleccionar tabla).
- Para ver los atributos o una tabla, utilice Show table definition (Mostrar definición de tabla). Utilice esta opción para ver los nombres de columnas, los tipos de columnas, la codificación, las claves de distribución, las claves de ordenación y si una columna puede contener valores nulos. Para obtener más información sobre los atributos de las tablas, consulte CREATE TABLE en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Para eliminar una tabla, utilice Delete (Eliminar). Puede usar Truncate table (Truncar tabla) para eliminar todas las filas de la tabla o Drop table (Eliminar tabla) para eliminar la tabla de la base de datos. Para obtener más información, consulte TRUNCATE y DROP TABLE en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Elija un esquema para Refresh (Actualizar) o Drop schema (Eliminar esquema).

Elija una vista para Show view definition (Mostrar definición de vista) o Drop view (Eliminar vista).

Elija una función para Show function definition (Mostrar definición de la función) o Drop function (Eliminar función).

Elija un procedimiento almacenado para Show procedure definition (Mostrar definición de procedimiento) o Drop procedure (Eliminar procedimiento).

Creación de objetos de base de datos

Puede crear objetos de base de datos, incluidas bases de datos, esquemas, tablas y funciones definidas por el usuario (UDF). Para crear objetos de base de datos, es necesario que se conecte a un clúster o grupo de trabajo y a una base de datos.

Creación de bases de datos

Puede usar el editor de consultas v2 para crear bases de datos en su clúster o grupo de trabajo.

Para crear una base de datos

Para obtener más información sobre las bases de datos, consulte CREATE DATABASE en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Elija Create (Crear) y luego elija Database (Base de datos).
2. Ingrese un Database name (Nombre de base de datos).
3. (Opcional) Seleccione Users and groups (Usuarios y grupos), y elija un Database user (Usuario de base de datos).
4. (Opcional) Puede crear la base de datos a partir de un recurso compartido de datos o de AWS Glue Data Catalog. Para obtener más información sobre AWS Glue, consulte ¿Qué es AWS Glue? en la Guía para desarrolladores de AWS Glue.
   - (Opcional) Seleccione Crear mediante un recurso compartido de datos y elija Seleccionar un recurso compartido de datos. La lista incluye recursos compartidos de datos de productor que pueden utilizarse para crear un recurso compartido de datos de consumidor en el clúster o grupo de trabajo actual.
   - (Opcional) Seleccione Crear mediante AWS Glue Data Catalog y Elija una base de datos de AWS Glue. En Esquema del catálogo de datos, introduzca el nombre que se utilizará para el esquema cuando se haga referencia a los datos en un nombre de tres partes (database.schema.table).
5. Elija Crear base de datos.

   La nueva base de datos se muestra en el panel de vista de árbol.

   Cuando elija el paso opcional para consultar una base de datos creada a partir de un recurso compartido de datos, conéctese a una base de datos de Amazon Redshift del clúster o grupo de trabajo (por ejemplo, la base de datos predeterminada `dev`) y utilice la notación de tres partes (database.schema.table) que hace referencia al nombre de base de datos que creó al seleccionar Crear mediante un recurso compartido de datos. La base de datos para compartir datos aparece en la pestaña del editor de consultas v2, pero no está habilitada para la conexión directa.

   Cuando elija el paso opcional para consultar una base de datos creada a partir de AWS Glue Data Catalog, conéctese a la base de datos de Amazon Redshift en el clúster o grupo de trabajo (por ejemplo, la base de datos predeterminada `dev`) y utilice la notación de tres partes (database.schema.table) que hace referencia al nombre de la base de datos que creó al seleccionar Crear mediante AWS Glue Data Catalog, al esquema al que asignó un nombre en Esquema del catálogo de datos y la tabla de AWS Glue Data Catalog. Similar a:

```
SELECT * FROM glue-database.glue-schema.glue-table
```

> **Note**
>
> Confirme que se ha conectado a la base de datos predeterminada mediante el método de conexión Credenciales temporales con su identidad de IAM y que se han concedido a sus credenciales de IAM privilegios de uso en la base de datos AWS Glue.
>
> ```
> GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
> ```

La base de datos AWS Glue para compartir datos aparece en la pestaña del editor de consultas v2, pero no está habilitada para la conexión directa.

Para obtener más información sobre la consulta de AWS Glue Data Catalog, consulte Uso de recursos compartidos de datos administrados por Lake Formation como consumidor y Uso de recursos compartidos de datos administrados por Lake Formation como productor en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Ejemplo de creación de una base de datos como consumidor de recursos compartidos de datos

En el siguiente ejemplo se describe un escenario específico que se utilizó para crear una base de datos a partir de un recurso compartido de datos mediante el editor de consultas v2. Consulte este escenario para aprender a crear una base de datos a partir de un recurso compartido de datos en su entorno. Este escenario utiliza dos clústeres, `cluster-base` (el clúster productor) y `cluster-view` (el clúster consumidor).

1. Utilice la consola de Amazon Redshift para crear un recurso compartido de datos para la tabla `category2` en el clúster `cluster-base`. El recurso compartido de datos de productor se denomina `datashare_base`.

   Para obtener información sobre la creación de recursos compartidos de datos, consulte Uso compartido de datos entre clústeres en Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

2. Utilice la consola de Amazon Redshift para aceptar el recurso compartido de datos `datashare_base` como consumidor de la tabla `category2` en el clúster `cluster-view`.
3. Consulte el panel de vista de árbol en el editor de consultas v2 que muestra la jerarquía de `cluster-base` como:

   - Clúster: `cluster-base`
     - Base de datos: `dev`
       - Esquema: `public`
         - Tablas: `category2`
4. Elija Create (Crear) y luego elija Database (Base de datos).
5. Introduzca `see_datashare_base` en Nombre de base de datos.
6. Seleccione Crear mediante un recurso compartido de datos y elija Seleccionar un recurso compartido de datos. Elija `datashare_base` para utilizarlo como origen de la base de datos que está creando.

   El panel de vista de árbol en el editor de consultas v2 muestra la jerarquía de `cluster-view` como:

   - Clúster: `cluster-view`
     - Base de datos: `see_datashare_base`
       - Esquema: `public`
         - Tablas: `category2`
7. Cuando consulte los datos, conéctese a la base de datos predeterminada del clúster `cluster-view` (normalmente se denomina `dev`), pero haga referencia a la base de datos de recursos compartidos de datos `see_datashare_base` en su código SQL.

   > **Note**
   >
   > En la vista del editor de consultas v2, el clúster seleccionado es `cluster-view`. La base de datos seleccionada es `dev`. La base de datos `see_datashare_base` aparece

en la lista, pero no está habilitada para la conexión directa. Elija la base de datos `dev` y la referencia `see_datashare_base` en el código SQL que ejecute.

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

La consulta recupera datos del recurso compartido de datos `datashare_base` del clúster `cluster_base`.

Ejemplo de creación de una base de datos a partir de un AWS Glue Data Catalog

En el siguiente ejemplo se describe un escenario específico que se utilizó para crear una base de datos a partir de un AWS Glue Data Catalog mediante el editor de consultas v2. Consulte este escenario para aprender a crear una base de datos a partir de un AWS Glue Data Catalog en su entorno. Este escenario utiliza el clúster `cluster-view` para que contenga la base de datos que cree.

1. Elija Create (Crear) y luego elija Database (Base de datos).
2. Introduzca `data_catalog_database` en Nombre de base de datos.
3. Seleccione Crear mediante un AWS Glue Data Catalog y Elija una base de datos de AWS Glue. Elija `glue_db` para utilizarlo como origen de la base de datos que está creando.

   Elija Esquema del catálogo de datos e introduzca `myschema` como nombre del esquema a utilizar en la notación de tres partes.

   El panel de vista de árbol en el editor de consultas v2 muestra la jerarquía de `cluster-view` como:

   - Clúster: `cluster-view`
     - Base de datos: `data_catalog_database`
       - Esquema: `myschema`
         - Tablas: `category3`

4. Cuando consulte los datos, conéctese a la base de datos predeterminada del clúster `cluster-view` (normalmente se denomina `dev`), pero haga referencia a la base de datos `data_catalog_database` en su código SQL.

   > **Note**
   >
   > En la vista del editor de consultas v2, el clúster seleccionado es `cluster-view`. La base de datos seleccionada es `dev`. La base de datos `data_catalog_database` aparece en la lista, pero no está habilitada para la conexión directa. Elija la base de datos `dev` y la referencia `data_catalog_database` en el código SQL que ejecute.

   ```
   SELECT * FROM "data_catalog_database"."myschema"."category3";
   ```

   La consulta recupera los datos catalogados por AWS Glue Data Catalog.

Creación de esquemas

Puede usar el editor de consultas v2 para crear esquemas en su clúster o grupo de trabajo.

Para crear un esquema

Para obtener más información sobre los esquemas, consulte Esquemas en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Elija (Crear) y luego elija Schema (Esquema).
2. Ingrese un Schema name (Nombre de esquema).
3. Elija Local (Local) o External (Externo) en Schema type (Tipo de esquema).

   Para obtener más información sobre los esquemas locales, consulte CREATE SCHEMA en la Guía para desarrolladores de bases de datos de Amazon Redshift. Para obtener más información sobre los esquemas externos, consulte CREATE EXTERNAL SCHEMA en la Guía para desarrolladores de bases de datos de Amazon Redshift.
4. Si elige External (Externo), dispondrá de las siguientes opciones de un esquema externo.

- Glue Data Catalog (Catálogo de datos de Glue): para crear un esquema externo en Amazon Redshift que haga referencia a tablas en AWS Glue. Además de elegir la base de datos de AWS Glue, seleccione el rol de IAM asociado al clúster y el rol de IAM asociado al catálogo de datos.
- PostgreSQL: para crear un esquema externo en Amazon Redshift que haga referencia a una base de datos de Amazon RDS para PostgreSQL o de Amazon Aurora PostgreSQL-Compatible Edition. Proporcione la información de conexión a la base de datos. Para obtener más información sobre las consultas federadas, lea Consulta de datos con consultas federadas en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- MySQL: para crear un esquema externo en Amazon Redshift que haga referencia a una base de datos de Amazon RDS para MySQL o de Amazon Aurora MySQL-Compatible Edition. Proporcione la información de conexión a la base de datos. Para obtener más información sobre las consultas federadas, lea Consulta de datos con consultas federadas en la Guía para desarrolladores de bases de datos de Amazon Redshift.

5. Elija Create schema (Crear esquema).

   El nuevo esquema aparece en el panel de vista de árbol.

Creación de tablas

Puede usar el editor de consultas v2 para crear tablas en su clúster o grupo de trabajo.

Para crear una tabla de

Puede crear una tabla basada en un archivo de valores separados por comas (CSV) que especifique o definir cada columna de la tabla. Para obtener más información sobre las tablas, consulte Diseño de tablas y CREATE TABLE en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Elija Open query in editor (Abrir consulta en el editor) para ver y editar la instrucción CREATE TABLE antes de ejecutar la consulta para crear la tabla.

1. Elija

   Create (Crear) y, luego, Table (Tabla).
2. Elija un esquema.
3. Ingrese un nombre para la tabla.

4. Elija

   Add field (Agregar campo) para agregar una columna.
5. Utilice un archivo CSV como plantilla para la definición de la tabla:

   a. Elija Load from CSV (Cargar desde CSV).

   b. Desplácese hasta la ubicación del archivo.

      Si utiliza un archivo CSV, asegúrese de que la primera fila del archivo contenga los encabezados de columna.

   c. Elija el archivo y, a continuación, elija Open (Abrir). Confirme que los nombres de columnas y los tipos de datos son lo que desea.
6. Para cada columna, elija la columna y las opciones que desee:

   - Elija un valor para Encoding (Codificación).
   - Elija un Default value (Valor predeterminado).
   - Active Automatically increment (Incrementar automáticamente) si desea que los valores de columna incrementen. A continuación, especifique un valor para Auto increment seed (Incrementar automáticamente el valor de inicialización) y Auto increment step (Incrementar automáticamente el paso).
   - Active Not NULL (Sin valores nulos) si la columna debe contener siempre un valor.
   - Ingrese un valor de Size (Tamaño) para la columna.
   - Active Primary key (Clave principal) si desea que la columna sea una clave principal.
   - Active Unique key (Clave única) si desea que la columna sea una clave única.
7. (Opcional) Elija Table details (Detalles de la tabla) y elija cualquiera de las siguientes opciones:

   - Columna y estilo de clave de distribución
   - Columna de clave de ordenación y tipo de ordenación
   - Active Backup (Copia de seguridad) para incluir la tabla en instantáneas.
   - Active Temporary table (Tabla temporal) para crear la tabla como una tabla temporal.
8. Elija Open query in editor (Abrir consulta en el editor) para seguir especificando opciones con objeto de definir la tabla o elija Create table (Crear tabla) para crear la tabla.

Creación de funciones

Puede usar el editor de consultas v2 para crear funciones en su clúster o grupo de trabajo.

Para crear una función

1. Elija Create (Crear) y elija Function (Función).
2. Para Type (Tipo), elija SQL o Python.
3. Elija un valor para Schema (Esquema).
4. Ingrese un valor en Name (Nombre) para la función.
5. Ingrese un valor en Volatility (Volatilidad) para la función.
6. Elija Parameters (Parámetros) por sus tipos de datos según el orden de los parámetros de entrada.
7. En Returns (Devoluciones), elija un tipo de datos.
8. Ingrese el código del programa SQL o programa de Python para la función.
9. Seleccione Create (Crear).

Para obtener más información sobre las funciones definidas por el usuario (UDF), consulte Creación de funciones definidas por el usuario en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Visualización del historial de consultas y pestañas

Puede ver el historial de consultas con el editor de consultas v2. Solo las consultas que ejecutó con el editor de consultas v2 aparecen en el historial de consultas. Se muestran las dos consultas que se ejecutaron desde una pestaña Editor o una pestaña Notebook (Bloc de notas). Puede filtrar la lista que se muestra por un periodo de tiempo, por ejemplo `This week`, en el que una semana se define de lunes a domingo. La lista de consultas muestra 25 filas de consultas que coinciden con el filtro a la vez. Elija Load more (Cargar más) para ver el siguiente conjunto. Elija una consulta y desde el menú Actions (Acciones). Las acciones disponibles dependen de si la consulta elegida se ha guardado. Puede elegir las siguientes operaciones:

- View query details (Ver detalles de la consulta): muestra una página de detalles de la consulta con más información sobre la consulta que se ejecutó.

- Open query in a new tab (Abrir consulta en una pestaña nueva): abre una pestaña del editor nueva y la prepara con la consulta elegida. Si sigue conectado, el clúster o el grupo de trabajo y la base de datos se seleccionan automáticamente. Para ejecutar la consulta, primero confirme que se han elegido el clúster o el grupo de trabajo y la base de datos correctos.
- Open source tab (Pestaña de código abierto): si sigue abierta, navega hasta la pestaña del editor o del bloc de notas que contenía la consulta cuando se ejecutó. Es posible que el contenido del editor o del bloc de notas haya cambiado después de ejecutarse la consulta.
- Open saved query (Abrir consulta guardada): navega hasta la pestaña del editor o del bloc de notas y abre la consulta.

También puede ver el historial de consultas ejecutadas en una pestaña Editor o el historial de consultas ejecutadas en una pestaña Notebook (Bloc de notas). Para ver un historial de consultas en una pestaña, elija Tab history (Historial de una pestaña). En el historial de pestañas, puede llevar a cabo las operaciones siguientes:

- Copy query (Copiar consulta): copia el contenido SQL de la versión de la consulta en el portapapeles.
- Open query in a new tab (Abrir consulta en una pestaña nueva): abre una pestaña del editor nueva y la prepara con la consulta elegida. Para ejecutar la consulta, debe elegir el clúster o el grupo de trabajo y la base de datos.
- View query details (Ver detalles de la consulta): muestra una página de detalles de la consulta con más información sobre la consulta que se ejecutó.

Consideraciones al trabajar con el editor de consultas v2

Tenga en cuenta lo siguiente cuando trabaje con el editor de consultas v2.

- El tamaño máximo del resultado de la consulta es el menor de 5 MB o 100 000 filas.
- Puede ejecutar una consulta con un tamaño máximo de 300 000 caracteres.
- Puede guardar una consulta con un tamaño máximo de 30 000 caracteres.
- De forma predeterminada, el editor de consultas v2 confirma automáticamente cada comando SQL que ejecuta. Cuando se proporciona una instrucción BEGIN, las instrucciones en un bloque BEGIN-COMMIT o BEGIN-ROLLBACK se ejecutan como una única transacción. Para obtener más información acerca de las transacciones, consulte BEGIN en la Guía para desarrolladores de bases de datos de Amazon Redshift.

- El número máximo de advertencias que muestra el editor de consultas v2 al ejecutar una sentencia SQL es `10`. Por ejemplo, cuando se ejecuta un procedimiento almacenado, no se muestran más de 10 instrucciones RAISE.
- El editor de consultas v2 no admite un `RoleSessionName` de IAM que contenga comas (,). Es posible que aparezca un error similar al siguiente: Mensaje de error: «“AROA123456789EXAMPLE:mytext,yourtext” no es un valor válido para TagValue, contiene caracteres no válidos». Este problema surge cuando se define un `RoleSessionName` de IAM que incluye una coma y, a continuación, se utiliza el editor de consultas v2 con ese rol de IAM.

  Para obtener más información sobre un IAM `RoleSessionName`, consulte el atributo RoleSessionName de SAML en la Guía del usuario de IAM.

Modificación de la configuración de la cuenta

Un usuario con los permisos de IAM adecuados puede ver y cambiar los parámetros de Account settings (Configuración de cuenta) para otros usuarios en la misma Cuenta de AWS. Este administrador puede ver o configurar lo siguiente:

- El número máximo de conexiones simultáneas a bases de datos por usuario en la cuenta. Quedan incluidas las conexiones para Isolated sessions (Sesiones aisladas). Cuando se cambia este valor, pueden pasar 10 minutos hasta que el cambio surta efecto.
- Permite a los usuarios de la cuenta exportar un conjunto completo de resultados desde un comando SQL a un archivo.
- Cargue y vea bases de datos de ejemplo con algunas consultas guardadas que tengan relación.
- Especifique una ruta de Amazon S3 utilizada por los usuarios de la cuenta para cargar datos desde un archivo local.
- Visualice el ARN de clave de KMS que se utiliza para cifrar los recursos del editor de consultas v2.

Interacción con el SQL generativo del editor de consultas v2 (versión preliminar)

Esta es la documentación de la versión preliminar del SQL generativo del editor de consultas v2. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para obtener

una vista previa de los términos y las condiciones, consulte Participación de la versión beta del servicio en Términos del servicio de AWS.

> **Note**
>
> En la actualidad, el soporte del SQL generativo solo está disponible en las siguientes Regiones de AWS:
>
> - Región Este de EE. UU. (Norte de Virginia) (us-east-1)
> - Región Oeste de EE. UU. (Oregón) (us-west-2)

Puede interactuar con la funcionalidad del SQL generativo de Amazon Q en el editor de consultas v2 de Amazon Redshift. Se trata de un asistente de codificación que genera instrucciones SQL en función de sus indicaciones y del esquema de la base de datos. Este asistente de codificación está disponible mientras se crea un cuaderno en el editor de consultas v2.

Cuando interactúe con el SQL generativo, realice preguntas específicas, repita cuando tenga solicitudes complejas y verifique la precisión de las respuestas.

Cuando envíe solicitudes de análisis en lenguaje natural, sea lo más específico posible para ayudar al asistente de codificación a entender exactamente lo que necesita. En lugar de preguntar “busca los principales eventos que han vendido más entradas”, proporciona más detalles, por ejemplo “busca nombres o ID de los tres eventos que hayan vendido más entradas en 2008”. Utilice nombres coherentes de objetos de la base de datos, como los nombres de esquemas, tablas y columnas, tal como se han definido en la base de datos, en lugar de hacer referencia al mismo objeto de manera diferente, cosa que puede confundir al asistente.

Divida las solicitudes complejas en varias instrucciones simples que sean más fáciles de interpretar para el asistente. Haga preguntas de seguimiento de forma iterativa para obtener un análisis más detallado del asistente. Por ejemplo, primero pregunte “¿qué estado tiene más eventos?”. Luego, según la respuesta, pregunte “¿cuál es el evento más popular de este estado?”.

Revise la consulta SQL generada antes de ejecutarla para garantizar que sea precisa. Si la consulta SQL generada contiene errores o no coincide con su intención, proporcione instrucciones al asistente sobre cómo corregirla en lugar de reformular toda la solicitud. Por ejemplo, si a la consulta le falta una cláusula predicativa sobre el año, pregunte “Indícame eventos del año 2008”.

Consideraciones a la hora de interactuar con el SQL generativo

Tenga en cuenta lo siguiente cuando trabaje en el panel de chat.

- El administrador del editor de consultas v2 de su cuenta debe haber activado la función de chat en la página Configuración del SQL generativo.
- Para utilizar el SQL generativo del editor de consultas v2, necesita un permiso `sqlworkbench:GetQSqlRecommendations` en su política de IAM, además de los demás permisos especificados en la política administrada de AWS del editor de consultas v2. Para obtener más información sobre las políticas administradas por AWS, consulte Acceso al editor de consultas v2.
- Las preguntas deben escribirse en inglés.
- Las preguntas deben hacer referencia a la base de datos conectada de su clúster o grupo de trabajo. Para evitar errores de estado vacío, debe haber al menos una tabla y algunos datos en la base de datos.
- Las preguntas deben hacer referencia a los datos almacenados en la base de datos conectada. No puede hacer referencia a un esquema externo. Para obtener más información sobre los esquemas admitidos, consulte Crear esquema en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Cualquier pregunta que dé como resultado SQL que cambie la base de datos conectada puede generar una advertencia.
- La tecnología de IA generativa es nueva y puede haber errores (a veces denominados alucinaciones) en las respuestas. Pruebe y revise todo el código para detectar errores y vulnerabilidades antes de usarlo en su entorno o carga de trabajo.
- Para mejorar las recomendaciones, comparta las consultas SQL ejecutadas por otros usuarios de su cuenta. El administrador de su cuenta puede ejecutar los siguientes comandos SQL para permitir el acceso al historial de consultas de la cuenta.

  ```
  GRANT ROLE SYS:MONITOR to "IAMR:role-name";
  GRANT ROLE SYS:MONITOR to "IAM:user-name";
  GRANT ROLE SYS:MONITOR to "database-username";
  ```

  Para obtener información sobre `SYS:MONITOR`, consulte Roles definidos por el sistema de Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Sus datos están seguros y son privados. Sus datos no se comparten entre cuentas. Sus consultas, datos y esquemas de bases de datos no se utilizan para entrenar un modelo fundacional (FM) de

IA generativa. Los datos introducidos se utilizan como indicaciones contextuales para que el FM responda únicamente a sus consultas.

Uso del SQL generativo

Después de configurar los permisos correctos, al trabajar con un cuaderno en el editor de consultas v2, puede elegir un icono para iniciar una conversación.

Para interactuar con el chat del SQL generativo del editor de consultas v2 para generar SQL

1. En la pestaña Editor del editor de consultas v2, abra un cuaderno.
2. Elija el icono del SQL generativo

   y, a continuación, siga las instrucciones para hacer sus preguntas sobre el SQL generativo del editor de consultas v2 de Amazon Redshift en el panel de chat.

   Las preguntas se escriben en un campo y el editor de consultas v2 responde con una sugerencia de SQL. Si surjen errores, aparecerán en el panel de chat.
3. Seleccione Añadir al cuaderno para añadir al cuaderno una celda de marcado con su pregunta y una celda SQL con el SQL sugerido.
4. (Opcional) Seleccione Regenerar SQL para generar otra respuesta para la misma pregunta. Puede elegir Regenerar SQL una vez para la pregunta actual.
5. (Opcional) En el panel de chat del SQL generativo, seleccione el icono

   de más y, a continuación, elija Actualizar base de datos para actualizar los metadatos que describen la base de datos conectada. Estos metadatos incluyen las definiciones de los esquemas, tablas y columnas de la base de datos.

Actualización de la configuración del SQL generativo en calidad de administrador

Un usuario con los permisos de IAM adecuados puede ver y cambiar los parámetros de Configuración del SQL generativo para otros usuarios de la misma Cuenta de AWS. Este administrador debe tener el permiso `sqlworkbench:UpdateAccountQSqlSettings` en su política de IAM, además de otros permisos especificados en la política administrada por AWS para el editor de consultas v2. Para obtener más información sobre las políticas administradas, consulte Permisos necesarios para usar del editor de consultas v2 .

Para que un administrador active el chat del SQL generativo para todos los usuarios de la cuenta

1. Elija el icono

   de Configuración para ver un menú de las diferentes pantallas de configuración.
2. A continuación, seleccione el icono de configuración del SQL generativo

   para mostrar la página Configuración del SQL generativo.
3. Seleccione SQL generativo para activar la funcionalidad de SQL generativo para los usuarios de la cuenta.

Ejemplo de uso de la capacidad del SQL generativo de Amazon Q con los datos de TICKIT

Para crear preguntas eficaces para generar SQL, debe conocer el esquema de su base de datos y sus datos. Los datos TICKIT constan de siete tablas: dos de hechos y cinco de dimensiones. Los datos de ejemplo contienen registros sobre las ventas a los asistentes a eventos de entretenimiento que tuvieron lugar en 2008. Para obtener más información sobre el esquema de datos TICKIT, consulte Bases de datos de muestra en la Guía para desarrolladores de bases de datos de Amazon Redshift. Puede cargar los datos TICKIT en una base de datos mediante varios métodos tanto en la consola de Amazon Redshift como en el editor de consultas v2. El editor de consultas v2 proporciona un método para cargar los datos TICKIT en la base de datos `sample_data_dev`. Para obtener más información, consulte Carga de datos de ejemplo. El editor de consultas v2 también proporciona preguntas de ejemplo para los datos TICKIT. El siguiente escenario describe una conversación con SQL generativo para generar SQL sobre los datos TICKIT de ejemplo. En este escenario, los datos TICKIT de ejemplo ya están creados en una base de datos `dev` de un clúster de Amazon Redshift.

> **Note**
>
> Este ejemplo sirve para ilustrar una conversación. Es posible que las respuestas del SQL generativo no coincidan con los resultados si se utilizan las mismas preguntas.

Ejemplo de conversación con el generativo SQL del editor de consultas v2

1. En el Editor, conéctese a un clúster o grupo de trabajo que contenga los datos TICKIT de ejemplo.
2. Cree un cuaderno vacío y elija el icono de SQL generativo

   para abrir el panel de chat.
3. Introduzca la siguiente pregunta para generar SQL y comprobar el número de registros de la tabla VENUE:

   ```
   How many venues are there?
   ```

   ```
   SELECT
     COUNT(*) AS num_venues
   FROM
     tickit.venue
   ```

   Seleccione Añadir al cuaderno para añadir dos celdas al cuaderno abierto. Una celda de marcado ¿Cuántos eventos hay? y otra que contenga el SQL generado.

   En la celda SQL, elija Ejecutar para recibir el resultado:

   ```
   count
   ------
   202
   ```
4. Para solicitar otra versión del SQL, elija Regenerar SQL y recibirá la siguiente respuesta:

   ```
   SELECT
     venuestate,
     COUNT(*) AS num_venues
   FROM
     tickit.venue
   GROUP BY
     venuestate
   ```

Seleccione Añadir al cuaderno para añadir más celdas al cuaderno abierto. Una celda de marcado ¿Cuántos eventos hay? y otra que contenga el SQL generado.

En la celda SQL, elija Ejecutar para recibir el resultado en forma de lista de número de evento por estado:

```
venuestate num_venues
----------------------
MA         4
OH         8
MI         5
...
```

5. El asistente del SQL generativo puede hacer suposiciones sobre lo que está preguntando. Aunque no haya widgets en la base de datos, puede seguir preguntando. En este caso, muestra un mensaje que indica que no ha podido generar el SQL.

```
How many widgets are there?
```

```
I was not able to generate any SQL
```

6. A medida que obtenga más información sobre la base de datos, podrá hacer preguntas más específicas para generar el SQL. Por ejemplo, sabe que la base de datos contiene datos de ventas de varios meses de 2008. Introduzca la siguiente pregunta para generar SQL y saber el número de ventas en noviembre de 2008:

```
How many sales were there in November 2008?
```

```
SELECT
  COUNT(*) AS num_sales
FROM
  tickit.sales s
  JOIN tickit.date d ON s.dateid = d.dateid
WHERE
  d.month = 'November'
  AND d.year = 2008
```

Seleccione Añadir al cuaderno para añadir dos celdas al cuaderno abierto. Una celda de marcado ¿Cuántas ventas hubo en noviembre de 2008? y otra que contenga el SQL generado.

En la celda SQL, elija Ejecutar para recibir el resultado:

```
num_sales
-----
0
```

Se da cuenta de que este no es el resultado que esperaba.

7. Observa que el predicado `date.month='November'` espera que el mes de la tabla DATE se represente con una abreviatura del nombre del mes. Cambia el predicado por `d.month='NOV'` y vuelve a ejecutar el SQL.

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
  date.month = 'NOV'
  AND date.year = 2008
```

En la celda SQL, elija Ejecutar para obtener nuevos resultados.

```
count
-----
14261
```

8. Si hace una pregunta que intenta cambiar la base de datos conectada, aparecerá un mensaje de advertencia junto con cualquier SQL recomendado. Introduzca la siguiente pregunta para generar SQL e insertar datos en una tabla:

```
Insert 1 into the venue table.
```

```
INSERT
,
UPDATE
```

```
  OR delete data
FROM
  the database AS that could potentially change the data.Please provide a query
 that ONLY selects data
```

```
I was not able to generate the correct SQL code. I generated SQL, but you'll have
 to edit it to work with your database.
```

Si selecciona Añadir al cuaderno para añadir dos celdas al cuaderno abierto y ejecutar el SQL, el SQL fallará.

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
 1-6546764a-011df2691778846219ce6ec2]
```

Este escenario solo ilustra algunas formas básicas de interactuar con el SQL generativo del editor de consultas v2. Puede experimentar aún más con esta tecnología de IA generativa que le ayudará a empezar a crear SQL para realizar consultas a su base de datos.

Descarga de datos en una base de datos

Puede utilizar el editor de consultas v2 para cargar datos en una base de datos en un clúster o grupo de trabajo de Amazon Redshift.

Carga de datos de ejemplo

El editor de consultas v2 incluye datos y cuadernos de muestra disponibles para cargarlos en una base de datos de muestra y en el esquema correspondiente.

Para cargar datos de ejemplo, elija el icono

asociado a los datos de ejemplo que desea cargar. A continuación, el editor de consultas v2 carga los datos en un esquema en la base de datos `sample_data_dev` y crea una carpeta de cuadernos guardados en su carpeta Notebooks (Cuadernos).

Están disponibles los siguientes conjuntos de datos de ejemplo.

tickit

En la mayoría de los ejemplos de la documentación de Amazon Redshift, se usan datos de ejemplo denominados `tickit`. Estos datos constan de siete tablas: dos de hechos y cinco de dimensiones. Al cargar estos datos, el esquema `tickit` se actualiza con datos de ejemplo. Para obtener más información sobre los datos `tickit`, consulte Bases de datos de muestra en la Guía para desarrolladores de bases de datos de Amazon Redshift.

tpch

Estos datos se utilizan para un punto de referencia de apoyo para la toma de decisiones. Al cargar estos datos, el esquema `tpch` se actualiza con datos de ejemplo. Para obtener más información acerca de los datos de `tpch`, consulte TPC-H.

tpcds

Estos datos se utilizan para un punto de referencia de apoyo para la toma de decisiones. Al cargar estos datos, el esquema `tpcds` se actualiza con datos de ejemplo. Para obtener más información acerca del tipo de datos de `tpcds`, consulte TPC-DS.

Carga de datos desde Amazon S3

Puede cargar datos de Amazon S3 en una tabla existente o nueva.

Para cargar datos en una tabla existente

El editor de consultas v2 utiliza el comando COPY para cargar datos desde Amazon S3. El comando COPY generado y utilizado en el asistente de carga de datos del editor de consultas v2 admite muchos de los parámetros disponibles para la sintaxis del comando COPY para copiar desde Amazon S3. Para obtener información sobre el comando COPY y sus opciones utilizadas para cargar datos desde Amazon S3, consulte COPY desde Amazon Simple Storage Service en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Confirme que la tabla ya esté creada en la base de datos en la que desea cargar datos.
2. Confirme que está conectado a la base de datos de destino en el panel de vista de árbol del editor de consultas v2 antes de continuar. Puede crear una conexión con el menú de contexto (botón derecho) al clúster o grupo de trabajo en el que se cargarán los datos.

Elija Load data (Cargar datos).

3. En Origen de datos, elija Cargar desde bucket de S3.
4. En S3 URIs (URI de S3), elija Browse S3 (Navegar en S3) para buscar el bucket de Amazon S3 que contiene los datos que se van a cargar.
5. Si el bucket de Amazon S3 especificado no está en la misma Región de AWS que la tabla de destino, elija la S3 file location (Ubicación del archivo de S3) para la Región de AWS donde se encuentran los datos.
6. Elija This file is a manifest file (Este archivo es un archivo de manifiesto) si el archivo de Amazon S3 es en realidad un manifiesto que contiene varios URI de bucket de Amazon S3.
7. Elija el File format (Formato de archivo) para el archivo que se va a cargar. Los formatos de datos admitidos son CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET y ORC. En función del formato de archivo especificado, puede elegir las File options (Opciones de archivo) correspondientes. También puede seleccionar Data is encrypted (Los datos están cifrados) si los datos están cifrados e ingresar el nombre de recurso de Amazon (ARN) de la clave KMS utilizada para cifrar los datos.

   Si elige CSV o DELIMITER, también puede seleccionar el Carácter delimitador y si desea Ignorar filas del encabezado en caso de que el número especificado de filas sean en realidad nombres de columnas y no datos para cargar.
8. Elija un método de compresión para comprimir el archivo. El valor predeterminado es no compresión.
9. (Opcional) En Advanced settings (Configuración avanzada) se admiten varios Data conversion parameters (Parámetros de conversión de datos) y Load operations (Operaciones de carga). Ingrese esta información según sea necesario para su archivo.

   Para obtener más información sobre los parámetros de conversión de datos y carga de datos, consulte Parámetros de conversión de datos y Operaciones de carga de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
10. Elija Next (Siguiente).
11. Seleccione Cargar tabla existente.

12. Confirme o elija la ubicación de la Target table (Tabla de destino) incluido el nombre de Cluster or workgroup (Clúster o grupo de trabajo), la Database (Base de datos), el Schema (Esquema) y la Table (Tabla) donde se cargan los datos.
13. Elija un IAM role (Rol de IAM) que tenga los permisos necesarios para cargar datos desde Amazon S3.
14. (Opcional) Elija los nombres de las columnas para ingresarlos en el Column mapping (Mapeo de columnas) para mapear las columnas en el orden del archivo de datos de entrada.
15. Elija Load data (Cargar datos) para iniciar la carga de datos.

    Cuando se completa la carga, el editor de consultas se muestra con el comando COPY generado que se utilizó para cargar los datos. Se muestra el Result (Resultado) de COPY. Si tiene éxito, podrá utilizar SQL para seleccionar datos de la tabla cargada. Si hay un error, consulte la vista de sistema STL_LOAD_ERRORS para obtener más detalles. Para obtener más información sobre los errores del comando COPY, consulte STL_LOAD_ERRORS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Al cargar datos en una tabla nueva, el editor de consultas v2 crea primero la tabla en la base de datos y, después, carga los datos como acciones independientes en el mismo flujo de trabajo.

Para cargar datos en una tabla nueva

El editor de consultas v2 utiliza el comando COPY para cargar datos desde Amazon S3. El comando COPY generado y utilizado en el asistente de carga de datos del editor de consultas v2 admite muchos de los parámetros disponibles para la sintaxis del comando COPY para copiar desde Amazon S3. Para obtener información sobre el comando COPY y sus opciones utilizadas para cargar datos desde Amazon S3, consulte COPY desde Amazon Simple Storage Service en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Confirme que está conectado a la base de datos de destino en el panel de vista de árbol del editor de consultas v2 antes de continuar. Puede crear una conexión con el menú de contexto (botón derecho) al clúster o grupo de trabajo en el que se cargarán los datos.

   Elija Load data (Cargar datos).
2. En Origen de datos, elija Cargar desde bucket de S3.

3. En S3 URIs (URI de S3), elija Browse S3 (Navegar en S3) para buscar el bucket de Amazon S3 que contiene los datos que se van a cargar.
4. Si el bucket de Amazon S3 especificado no está en la misma Región de AWS que la tabla de destino, elija la S3 file location (Ubicación del archivo de S3) para la Región de AWS donde se encuentran los datos.
5. Elija This file is a manifest file (Este archivo es un archivo de manifiesto) si el archivo de Amazon S3 es en realidad un manifiesto que contiene varios URI de bucket de Amazon S3.
6. Elija el File format (Formato de archivo) para el archivo que se va a cargar. Los formatos de datos admitidos son CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET y ORC. En función del formato de archivo especificado, puede elegir las File options (Opciones de archivo) correspondientes. También puede seleccionar Data is encrypted (Los datos están cifrados) si los datos están cifrados e ingresar el nombre de recurso de Amazon (ARN) de la clave KMS utilizada para cifrar los datos.

   Si elige CSV o DELIMITER, también puede seleccionar el Carácter delimitador y si desea Ignorar filas del encabezado en caso de que el número especificado de filas sean en realidad nombres de columnas y no datos para cargar.
7. Elija un método de compresión para comprimir el archivo. El valor predeterminado es no compresión.
8. (Opcional) En Advanced settings (Configuración avanzada) se admiten varios Data conversion parameters (Parámetros de conversión de datos) y Load operations (Operaciones de carga). Ingrese esta información según sea necesario para su archivo.

   Para obtener más información sobre los parámetros de conversión de datos y carga de datos, consulte Parámetros de conversión de datos y Operaciones de carga de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
9. Elija Next (Siguiente).
10. Seleccione Cargar nueva tabla.

    Las columnas de la tabla se deducen de los datos de entrada. Puede modificar la definición del esquema de la tabla si agrega columnas y detalles de tabla. Para volver al esquema de tablas inferidas del editor de consultas v2, elija Restaurar a los valores predeterminados.
11. Confirme o elija la ubicación de la Tabla de destino incluido el Clúster o grupo de trabajo, la Base de datos, el Esquema y la Tabla donde se cargan los datos. Introduzca el nombre de la Tabla que se va a crear.

12. Elija un IAM role (Rol de IAM) que tenga los permisos necesarios para cargar datos desde Amazon S3.
13. Elija Crear tabla para crear la tabla con la definición mostrada.

    Se muestra un resumen de la definición de la tabla. La tabla se crea en la base de datos. Para eliminar la tabla más adelante, ejecute el comando SQL DROP TABLE. Para obtener más información, consulte DROP TABLE en la Guía para desarrolladores de bases de datos de Amazon Redshift.
14. Elija Load data (Cargar datos) para iniciar la carga de datos.

    Cuando se completa la carga, el editor de consultas se muestra con el comando COPY generado que se utilizó para cargar los datos. Se muestra el Result (Resultado) de COPY. Si tiene éxito, podrá utilizar SQL para seleccionar datos de la tabla cargada. Si hay un error, consulte la vista de sistema STL_LOAD_ERRORS para obtener más detalles. Para obtener más información sobre los errores del comando COPY, consulte STL_LOAD_ERRORS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Configuración y flujo de trabajo de la carga de datos desde un archivo local

Puede cargar datos de un archivo local en una tabla existente o nueva.

Configuración del administrador para cargar datos desde un archivo local

El administrador del editor de consultas v2 debe especificar el bucket común de Amazon S3 en la ventana de Account settings (Configuración de la cuenta). Los usuarios de la cuenta deben estar configurados con los permisos adecuados.

- Permisos de IAM requeridos: los usuarios de carga desde archivo local deben tener los permisos `s3:ListBucket`, `s3:GetBucketLocation`, `s3:putObject`, `s3:getObject` y `s3:deleteObject`. El *`optional-prefix`* se puede especificar para limitar el uso de este bucket relacionado con el editor de consultas v2 a los objetos con este prefijo. Puede utilizar esta opción cuando utilice este mismo bucket de Amazon S3 para usos distintos del editor de consultas v2. Para obtener más información sobre los buckets y los prefijos, consulte Administración del acceso de los usuarios a carpetas específicas en la Guía del usuario de Amazon Simple Storage Service. Para asegurarse de que no se permita el acceso a los datos entre usuarios, recomendamos que el administrador del editor de consultas v2 utilice una política de bucket de Amazon S3 para restringir el acceso a los objetos en función de `aws:userid`. El siguiente

ejemplo permite los permisos de Amazon S3 a un *<staging-bucket-name>* con acceso de lectura o escritura solo a los objetos de Amazon S3 con `aws:userid` como prefijo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket-name>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
${aws:userid}/*"
            ]
        }
    ]
}
```

- Separación de datos: recomendamos que los usuarios no tengan acceso a los datos de los demás (ni siquiera de forma breve). La carga desde un archivo local utiliza el bucket de Amazon S3 transitorio configurado por el administrador del editor de consultas v2. Configure la política de bucket para el bucket transitorio a fin de proporcionar una separación de datos entre los usuarios. El siguiente ejemplo muestra una política de bucket que separa los datos entre los usuarios del *<staging-bucket-name>*.

```
{
 "Version": "2012-10-17",
    "Statement": [
        {"Sid": "userIdPolicy",
```

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": ["s3:PutObject",
                       "s3:GetObject",
                       "s3:DeleteObject"],
            "NotResource": [
                "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
${aws:userid}/*"
            ]
        }
    ]
}
```

Carga de datos desde un archivo local

Para cargar datos de archivo local en una tabla existente

El administrador del editor de consultas v2 debe especificar el bucket de Amazon S3 común en la ventana Configuración de la cuenta. El editor de consultas v2 carga automáticamente el archivo local en un bucket de Amazon S3 común utilizado por la cuenta y, a continuación, utiliza el comando COPY para cargar los datos. El comando COPY generado y ejecutado por la ventana de archivo local de carga del editor de consultas v2 admite mucho parámetros disponibles para la sintaxis del comando COPY para copiar desde Amazon S3. Para obtener información sobre el comando COPY y sus opciones utilizadas para cargar datos desde Amazon S3, consulte COPY desde Amazon S3 en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Confirme que la tabla ya esté creada en la base de datos en la que desea cargar datos.
2. Confirme que está conectado a la base de datos de destino en el panel de vista de árbol del editor de consultas v2. Puede crear una conexión con el menú de contexto (botón derecho) al clúster o grupo de trabajo en el que se cargarán los datos.
3. Elija Load data (Cargar datos).
4. Para Data source (Origen de datos), elija Load from local file (Cargar desde archivo local).
5. Elija Examinar para encontrar el archivo que contiene los datos para Cargar el archivo CSV. De forma predeterminada, se muestran los archivos con la extensión `.csv`, `.avro`, `.parquet` y `.orc`, pero puede elegir otros tipos de archivo. El tamaño de archivo máximo es de 5 MB.

6. Elija el File format (Formato de archivo) para el archivo que se va a cargar. Los formatos de datos admitidos son CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET y ORC. En función del formato de archivo especificado, puede elegir las File options (Opciones de archivo) correspondientes. También puede seleccionar Data is encrypted (Los datos están cifrados) si los datos están cifrados e ingresar el nombre de recurso de Amazon (ARN) de la clave KMS utilizada para cifrar los datos.

   Si elige CSV o DELIMITER, también puede seleccionar el Carácter delimitador y si desea Ignorar filas del encabezado en caso de que el número especificado de filas sean en realidad nombres de columnas y no datos para cargar.
7. (Opcional) En Advanced settings (Configuración avanzada) se admiten varios Data conversion parameters (Parámetros de conversión de datos) y Load operations (Operaciones de carga). Ingrese esta información según sea necesario para su archivo.

   Para obtener más información sobre los parámetros de conversión de datos y carga de datos, consulte Parámetros de conversión de datos y Operaciones de carga de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
8. Elija Next (Siguiente).
9. Seleccione Cargar tabla existente.
10. Confirme o elija la ubicación de la Target table (Tabla de destino) incluido el nombre de Cluster or workgroup (Clúster o grupo de trabajo), la Database (Base de datos), el Schema (Esquema) y la Table (Tabla) donde se cargan los datos.
11. (Opcional) Puede elegir los nombres de las columnas para ingresar en el Column mapping (Mapeo de columnas) para mapear las columnas en el orden del archivo de datos de entrada.
12. Elija Load data (Cargar datos) para iniciar la carga de datos.

    Cuando se complete la carga, aparecerá un mensaje si la carga se ha realizado correctamente o no. Si tiene éxito, podrá utilizar SQL para seleccionar datos de la tabla cargada. Si hay un error, consulte la vista de sistema STL_LOAD_ERRORS para obtener más detalles. Para obtener más información sobre los errores del comando COPY, consulte STL_LOAD_ERRORS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

    La plantilla de comandos COPY que se usó para cargar datos aparece en el Query history (Historial de consultas). Esta plantilla de comandos COPY muestra algunos de los parámetros utilizados, pero no se puede ejecutar directamente en una pestaña del editor. Para obtener más información acerca del historial de consultas, consulte Visualización del historial de consultas y pestañas.

Al cargar datos en una tabla nueva, el editor de consultas v2 crea primero la tabla en la base de datos y, después, carga los datos como acciones independientes en el mismo flujo de trabajo.

Para cargar datos de archivo local en una tabla nueva

El administrador del editor de consultas v2 debe especificar el bucket común de Amazon S3 en la ventana de Account settings (Configuración de la cuenta). El archivo local se carga automáticamente en un bucket de Amazon S3 común utilizado por la cuenta y, a continuación, el editor de consultas v2 utiliza el comando COPY para cargar datos. El comando COPY generado y ejecutado por la ventana de archivo local de carga del editor de consultas v2 admite mucho parámetros disponibles para la sintaxis del comando COPY para copiar desde Amazon S3. Para obtener información sobre el comando COPY y sus opciones utilizadas para cargar datos desde Amazon S3, consulte COPY desde Amazon S3 en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Confirme que está conectado a la base de datos de destino en el panel de vista de árbol del editor de consultas v2. Puede crear una conexión con el menú de contexto (botón derecho) al clúster o grupo de trabajo en el que se cargarán los datos.
2. Elija

   Load data (Cargar datos).
3. Para Data source (Origen de datos), elija Load from local file (Cargar desde archivo local).
4. Elija Examinar para encontrar el archivo que contiene los datos para Cargar el archivo CSV. De forma predeterminada, se muestran los archivos con la extensión `.csv`, `.avro`, `.parquet` y `.orc`, pero puede elegir otros tipos de archivo. El tamaño de archivo máximo es de 5 MB.
5. Elija el File format (Formato de archivo) para el archivo que se va a cargar. Los formatos de datos admitidos son CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET y ORC. En función del formato de archivo especificado, puede elegir las File options (Opciones de archivo) correspondientes. También puede seleccionar Data is encrypted (Los datos están cifrados) si los datos están cifrados e ingresar el nombre de recurso de Amazon (ARN) de la clave KMS utilizada para cifrar los datos.

   Si elige CSV o DELIMITER, también puede seleccionar el Carácter delimitador y si desea Ignorar filas del encabezado en caso de que el número especificado de filas sean en realidad nombres de columnas y no datos para cargar.
6. (Opcional) En Advanced settings (Configuración avanzada) se admiten varios Data conversion parameters (Parámetros de conversión de datos) y Load operations (Operaciones de carga). Ingrese esta información según sea necesario para su archivo.

Para obtener más información sobre los parámetros de conversión de datos y carga de datos, consulte Parámetros de conversión de datos y Operaciones de carga de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.

7. Elija Next (Siguiente).
8. Seleccione Cargar nueva tabla.
9. Confirme o elija la ubicación de la Tabla de destino incluido el Clúster o grupo de trabajo, la Base de datos, el Esquema y la Tabla donde se cargan los datos. Introduzca el nombre de la Tabla que se va a crear.
10. Elija Crear tabla para crear la tabla con la definición mostrada.

    Se muestra un resumen de la definición de la tabla. La tabla se crea en la base de datos. Para eliminar la tabla más adelante, ejecute el comando SQL DROP TABLE. Para obtener más información, consulte DROP TABLE en la Guía para desarrolladores de bases de datos de Amazon Redshift.
11. Elija Load data (Cargar datos) para iniciar la carga de datos.

    Cuando se complete la carga, aparecerá un mensaje que indica si la carga se realizó correctamente o no. Si tiene éxito, podrá utilizar SQL para seleccionar datos de la tabla cargada. Si hay un error, consulte la vista de sistema STL_LOAD_ERRORS para obtener más detalles. Para obtener más información sobre los errores del comando COPY, consulte STL_LOAD_ERRORS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

    La plantilla de comandos COPY que se usó para cargar datos aparece en el Query history (Historial de consultas). Esta plantilla de comandos COPY muestra algunos de los parámetros utilizados, pero no se puede ejecutar directamente en una pestaña del editor. Para obtener más información acerca del historial de consultas, consulte Visualización del historial de consultas y pestañas.

Creación y ejecución de consultas

Puede ingresar una consulta en el editor o seleccionar una consulta guardada en la lista de Queries (Consultas) y elegir Run (Ejecutar).

De manera predeterminada, Limit 100 (Límite de 100) está configurado para limitar los resultados a 100 filas. Puede desactivar esta opción para devolver un conjunto de resultados más grande. Si desactiva esta opción, puede incluir la opción LIMIT en la instrucción SQL si desea evitar conjuntos

de resultados muy grandes. Para obtener más información, consulte Cláusula ORDER BY en la Guía para desarrolladores de bases de datos de Amazon Redshift..

Para mostrar un plan de consultas en el área de resultados, active Explain (Explicar). Active Explain graph (Explicar gráfico) para que en los resultados también se muestre una representación gráfica del plan de explicación.

Para guardar una consulta en la carpeta Queries (Consultas), elija Save (Guardar).

Si una consulta es correcta, aparece un mensaje de éxito. Si la consulta devuelve información, los resultados se muestran en la sección Results (Resultados). Si el número de resultados excede el área de visualización, los números aparecen en la parte superior del área de resultados. Puede elegir los números para mostrar páginas sucesivas de resultados.

Puede filtrar y ordenar Result (Resultado) para cada columna. Para ingresar criterios de filtro en el encabezado de la columna de resultados, desplácese sobre la columna para ver un menú (☰) donde puede ingresar criterios para filtrar la columna.

Si la consulta contiene un error, el editor de consultas v2 muestra un mensaje de error en el área de resultados. El mensaje proporciona información sobre cómo corregir la consulta.

Puede exportar o copiar los resultados de la consulta mediante el menú contextual (clic derecho) en el área de resultados de la siguiente manera:

- Elija Export result set (Exportar conjunto de resultados) y JSON o CSV para descargar todo el conjunto de resultados de fila en un archivo. El número de filas del conjunto de resultados puede estar limitado por la opción Limit (Límite) o la cláusula `limit` de SQL de la consulta. El tamaño máximo del conjunto de resultados descargado es de 5 MB.
- Si no hay ninguna fila seleccionada, elija Export current page (Exportar página actual) y JSON o CSV para descargar las filas de la página actual en un archivo.
- Si se seleccionan filas, elija Export selected rows (Exportar filas seleccionadas) y JSON o CSV para descargar las filas seleccionadas en un archivo.
- Si se seleccionan filas, elija Copy rows (Copiar filas) para copiar las filas seleccionadas en el portapapeles.
- Si se seleccionan filas, elija Copy rows with headers (Copiar filas con encabezados) para copiar las filas seleccionadas con los encabezados de las columnas en el portapapeles.

También puede utilizar el acceso directo Ctrl+C en Windows o Cmd+C en macOS para copiar los datos de la página de resultados actual al portapapeles. Si no se selecciona ninguna fila, la celda con enfoque se copia en el portapapeles. Si se seleccionan filas, las filas seleccionadas se copian en el portapapeles.

Para agregar una nueva pestaña de consulta, elija el icono

y luego el Editor, que aparece en la fila con las pestañas de consulta. La pestaña de consulta utiliza una `Isolated session` o no. Con una sesión aislada, los resultados de un comando SQL, como la creación de una tabla temporal en una pestaña del editor, no son visibles en otra pestaña del editor. Al abrir una pestaña del editor en el editor de consultas v2, el valor predeterminado es una sesión aislada.

Para ejecutar una consulta

1. En el área de consulta, realice una de las siguientes acciones:

   - Ingrese una consulta.
   - Pegue una consulta que haya copiado.
   - Elija la carpeta Queries (Consultas), abra el menú contextual (clic derecho), seleccione una consulta guardada y elija Open query (Abrir consulta).

2. Confirme que eligió el valor de Cluster (Clúster), Workgroup (Grupo de trabajo) y Database (Base de datos) correctos para el SQL que va a ejecutar.

   Inicialmente, puede elegir el Cluster (Clúster) o Workgroup (Grupo de trabajo) en vista de árbol. Elija la Database (Base de datos) en vista de árbol también.

   Puede cambiar Cluster (Clúster) o Workgroup (Grupo de trabajo) y Database (Base de datos) en cada pestaña del editor con el control desplegable ubicado cerca del encabezado Isolated session (Sesión aislada) de cada una.

   Decida en cada pestaña del editor si desea ejecutar el SQL en una Isolated session (Sesión aislada). Una sesión aislada tiene su propia conexión a una base de datos. Se usa para ejecutar SQL que está aislado de otras sesiones del editor de consultas. Para obtener más información acerca de las conexiones, consulte Apertura del editor de consultas v2.

3. Elija Ejecutar.

   El área Result (Resultado) se abre y muestra los resultados de la consulta.

Para mostrar el plan de explicación de una consulta

1. Seleccione la consulta.
2. Active Explain (Explicación).

   De manera predeterminada, el Explain graph (Gráfico de explicación) también está activado.
3. Elija Ejecutar.

   La consulta se ejecuta y se muestra el plan de explicación en el área Result (Resultado) de la consulta.

El editor de consultas v2 es compatible con las siguientes características.

- Puede crear consultas con varias instrucciones SQL en una pestaña de consulta. Las consultas se ejecutan en serie y se abren varias pestañas de resultados para cada consulta.
- Puede crear consultas con variables de sesión y tablas temporales.
- Puede crear consultas con parámetros reemplazables designados por `${parameter}`. Puede crear la consulta SQL con varios parámetros reemplazables y utilizar el mismo parámetro en varios lugares de la instrucción SQL.

  Cuando se ejecuta la consulta, se presenta una ventana para ingresar el valor del parámetro. Cada vez que ejecuta la consulta, se presenta la ventana para ingresar los valores de los parámetros.

  Para ver un ejemplo, consulte Ejemplo: Ventas superiores a un parámetro específico.
- Las consultas se versionan automáticamente. Puede elegir una versión anterior de una consulta que desea ejecutar.
- No tiene que esperar a que se complete una consulta para continuar con su flujo de trabajo. Las consultas se siguen ejecutando incluso si cierra el editor de consultas.
- Cuando se crean consultas, se admite la finalización automática de nombres de esquemas, tablas y columnas.

El editor SQL es compatible con las siguientes características:

- Los corchetes iniciales y finales utilizados en SQL tienen colores coincidentes. Las líneas verticales se muestran en el editor para ayudarle a hacer coincidir los corchetes.
- Puede contraer y expandir secciones del SQL.

- Puede buscar y sustituir texto en el SQL.
- Puede utilizar las teclas de acceso directo para varias tareas de edición habituales.
- Los errores de SQL se resaltan en el editor para la ubicación adecuada de las áreas problemáticas.

Para obtener una demostración de las características de edición, vea el siguiente video: Experiencia de edición nueva y mejorada en el editor de consultas v2 de Amazon Redshift.

Consultas de ejemplo

A continuación, encontrará descripciones de los distintos tipos de consultas que puede ejecutar.

Los datos utilizados en estas consultas proceden del esquema de ejemplo de `tickit`. Para obtener más información acerca de cómo cargar datos de `tickit` de ejemplo, consulte Carga de datos de ejemplo. Para obtener más información sobre los datos de ejemplo de `tickit`, consulte Bases de datos de ejemplo en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Cuando ejecute estas consultas de ejemplo, confirme que eligió la base de datos correcta en el editor, como `sample_data_dev`.

Temas

- Ejemplo: Configuración de variables de sesión
- Ejemplo: Evento principal por ventas totales
- Ejemplo: Ventas superiores a un parámetro específico
- Ejemplo: Creación de una tabla temporal
- Ejemplo: Selección de una tabla temporal

Ejemplo: Configuración de variables de sesión

El siguiente comando establece el parámetro de configuración de servidor `search_path` en public (público) para la sesión. Para obtener más información, consulte SET y search_path en la Guía para desarrolladores de bases de datos de Amazon Redshift.

```
set search_path to public;
```

Ejemplo: Evento principal por ventas totales

En la siguiente consulta se encuentra el evento con mayor cantidad de ventas.

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

A continuación, se presenta una lista parcial de los resultados.

```
eventname           totalorders       totalsales
White Christmas         20              9352
Joshua Radin            38             23469
Beach Boys              58             30383
Linda Ronstadt          56             35043
Rascal Flatts           76             38214
Billy Idol              67             40101
Stephenie Meyer         72             41509
Indigo Girls            57             45399
...
```

Ejemplo: Ventas superiores a un parámetro específico

En la siguiente consulta se encuentran las ventas en las que la cantidad vendida es mayor que el parámetro especificado por `${numberoforders}`. Cuando el valor del parámetro es 7, el resultado es 60 filas. Cuando ejecuta la consulta, el editor de consultas v2 muestra una ventana que dice Run query form (Ejecutar formulario de consulta) para recopilar el valor de los parámetros de la instrucción SQL.

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
order by 2;
```

A continuación, se presenta una lista parcial de los resultados.

```
salesid qtysold
20005 8
21279 8
130232 8
42737 8
74681 8
67103 8
```

```
105533 8
91620 8
121552 8
...
```

Ejemplo: Creación de una tabla temporal

La siguiente instrucción crea la tabla temporal eventsalestemp seleccionando información de las tablas sales y event.

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

Ejemplo: Selección de una tabla temporal

En la siguiente instrucción se seleccionan los eventos, el total de pedidos y las ventas totales de la tabla temporal eventsalestemp, ordenados por total de pedidos.

```
select eventname,  totalorders,  totalsales
from eventsalestemp
order by 2;
```

A continuación, se presenta una lista parcial de resultados.

```
eventname          totalorders   totalsales
White Christmas         20          9352
Joshua Radin            38         23469
Martina McBride         50         52932
Linda Ronstadt          56         35043
Indigo Girls            57         45399
Beach Boys              58         30383
...
```

Creación y ejecución de cuadernos

Puede utilizar cuadernos para organizar, anotar y compartir varias consultas SQL en un solo documento. Puede agregar varias celdas de consulta SQL y marcado a un cuaderno. Los cuadernos

proporcionan una forma de agrupar consultas y explicaciones asociadas a un análisis de datos en un solo documento mediante varias celdas de consulta y Markdown. Puede agregar texto y dar formato a la apariencia mediante la sintaxis de Markdown para proporcionar contexto e información adicional para las tareas de análisis de datos. Puede compartir sus cuadernos con los miembros del equipo.

Para utilizar cuadernos, debe agregar el permiso para cuadernos a su entidad principal de IAM (un usuario o rol de IAM). Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift. Puede agregar el permiso a una de las políticas administradas del editor de consultas v2. Para obtener más información, consulte Acceso al editor de consultas v2.

Puede ejecutar todas las celdas de un cuaderno de forma secuencial. La celda de consulta SQL de un cuaderno tiene la mayoría de las mismas funciones que una pestaña del editor de consultas. Para obtener más información, consulte Creación y ejecución de consultas. A continuación, se indican las diferencias entre una pestaña del editor de consultas y una celda SQL de un cuaderno.

- No existe ningún control para ejecutar `Explain` en una instrucción SQL en un cuaderno.
- Solo puede crear un gráfico por cada celda SQL de un cuaderno.

Puede exportar e importar cuadernos a archivos creados con el editor de consultas v2. La extensión del archivo es `.ipynb` y el tamaño de archivo puede ser de un máximo de 5 MB. Las celdas SQL y Markdown se almacenan en el archivo. Un clúster o grupo de trabajo y la base de datos no están almacenados en el cuaderno exportado. Cuando abra un cuaderno importado, elija el clúster o grupo de trabajo y la base de datos donde ejecutarlo. Después de ejecutar las celdas SQL, puede elegir en la pestaña de resultados si desea mostrar la página actual de resultados como un gráfico. El conjunto de resultados de una consulta no se almacena en el cuaderno.

Si ejecuta un cuaderno, ya sea con Ejecutar todo o Ejecutar, aparecerá un panel Estado de ejecución. Seleccione el icono

para abrir el panel. Este panel contiene un resumen del estado más reciente de las celdas SQL Ejecutar todo o Ejecutar del cuaderno. Si ejecuta varias celdas SQL, puede ver de un vistazo el estado, el tiempo transcurrido y algunos detalles sobre la ejecución. Puede filtrar las celdas que se muestran en función del estado: `All`, `Succeeded`, `Error`, `In progress` o `Canceled`. También puede usar este panel para navegar hasta una celda SQL del editor.

Para crear un cuaderno

1. En el menú del navegador, elija Editor de

.
2. Elija

y, a continuación, elija Notebook (Bloc de notas).

   De manera predeterminada, aparece una celda de consulta SQL en el cuaderno.
3. En la celda de consulta SQL, realice una de las siguientes acciones:
   - Ingrese una consulta.
   - Pegue una consulta que haya copiado.
4. (Opcional) Elija el icono

y, a continuación, Markdown para agregar una celda de Markdown en la que puede proporcionar texto descriptivo o explicativo mediante la sintaxis de Markdown estándar.
5. (Opcional) Elija el icono

y, a continuación, elija SQL para insertar una celda SQL.

Puede cambiar el nombre de los cuadernos mediante el icono

(lápiz).

En el menú

(más) también puede realizar las siguientes operaciones en un cuaderno:

-
  Share with my team (Compartir con mi equipo): compartir el cuaderno con su equipo definido por etiquetas. Para obtener más información, consulte Compartir una consulta

-

  Export (Exportar): exportar el cuaderno a un archivo local con la extensión `.ipynb`.

-

  Save version (Guardar versión): crear una versión del cuaderno. Para ver las versiones de un cuaderno, vaya a sus cuadernos guardados y abra Version history (Historial de versiones).

-

  Duplicate (Duplicar): crear una copia del cuaderno y abrirla en una nueva pestaña de cuaderno.

-

  Shortcuts (Accesos directos): mostrar los accesos directos disponibles al crear un cuaderno.

Para abrir un cuaderno guardado

1. En el menú del navegador, elija

   Notebooks (Cuadernos). Se muestran sus cuadernos y carpetas de cuadernos guardados.
2. Elija el cuaderno que desea abrir y haga doble clic en él.

Puede mostrar My notebooks (Mis cuadernos), los cuadernos Shared by me (Compartidos por mí) y los cuadernos Shared to my team (Compartidos con mi equipo) en la pestaña de cuadernos.

Para importar un cuaderno desde un archivo local a My notebooks (Mis cuadernos), elija

Import (Importar) y navegue hasta el archivo `.ipynb` que contiene su cuaderno. El cuaderno se importa a la carpeta de cuadernos abierta en ese momento. A continuación, podrá abrir el cuaderno en el editor de cuadernos.

En el menú contextual (botón derecho del ratón) de un cuaderno puede realizar las siguientes operaciones:

- Open notebook (Abrir cuaderno): abrir el cuaderno en el editor.
- Save version (Guardar versión): guardar una versión del cuaderno.

- Version history (Historial de versiones): mostrar las versiones de un cuaderno. En la ventana Version history (Historial de versiones) puede eliminar y revertir versiones. También puede crear un cuaderno a partir de la versión seleccionada en ese momento.
- Edit tags (Editar etiquetas): crear y editar etiquetas en un cuaderno.
- Share with my team (Compartir con mi equipo): compartir un cuaderno con su equipo.

  Para compartir un cuaderno con su equipo, asegúrese de que tiene la etiqueta de entidad principal `sqlworkbench-team` establecida al mismo valor que el resto de los miembros de su equipo en su cuenta. Por ejemplo, un administrador podría establecer el valor en `accounting-team` para todos los miembros del departamento de contabilidad. Para ver un ejemplo, consulte Permisos necesarios para usar del editor de consultas v2 .
- Export (Exportar): exportar un cuaderno a un archivo local.
- Rename (Cambiar nombre): cambiar el nombre de un cuaderno.
- Duplicate (Duplicar): hacer una copia de un cuaderno.
- Delete (Eliminar): eliminar un cuaderno.

Para ver una demostración de los cuadernos, vea el siguiente vídeo: Amazon Redshift SQL Notebooks in query editor v2 (Cuadernos SQL de Amazon Redshift en el editor de consultas v2).

Consulta de AWS Glue Data Catalog

Puede utilizar el editor de consultas v2 para consultar datos catalogados en AWS Glue Data Catalog. De forma predeterminada, AWS Glue Data Catalog aparece como una base de datos del editor de consultas v2 denominada `awsdatacatalog`. La consulta de AWS Glue Data Catalog no está disponible en todas las Regiones de AWS de Amazon Redshift . Use el comando SHOW para determinar si esta capacidad está disponible. Para obtener más información sobre AWS Glue, consulte ¿Qué es AWS Glue? en la Guía para desarrolladores de AWS Glue.

> **Note**
>
> La consulta de AWS Glue Data Catalog solo se admite en clústeres de tipo de nodo RA3 de Amazon Redshift y en Amazon Redshift sin servidor.

Puede configurar su almacenamiento de datos y ver los objetos de la base de datos AWS Glue catalogados con los siguientes comandos SQL:

- SHOW: para mostrar si `awsdatacatalog` se ha montado para el almacenamiento de datos conectado actualmente. Por ejemplo, para mostrar el valor del parámetro `data_catalog_auto_mount`, ejecute:

  ```
  SHOW data_catalog_auto_mount;
  ```

  Para obtener más información, consulte SHOW en la Guía para desarrolladores de bases de datos de Amazon Redshift.

- ALTER SYSTEM: para cambiar la configuración en el sistema de `data_catalog_auto_mount`. Por ejemplo, para cambiar el valor del parámetro `data_catalog_auto_mount` por on, ejecute:

  ```
  ALTER SYSTEM SET data_catalog_auto_mount = on;
  ```

  El cambio surte efecto cuando se reinicia un clúster aprovisionado o se pausa y reanuda automáticamente un grupo de trabajo sin servidor. Para obtener más información, consulte ALTER SYSTEM en la Guía para desarrolladores de bases de datos de Amazon Redshift.

- SHOW SCHEMAS: muestra una lista de esquemas. Los esquemas de la base de datos denominada `awsdatacatalog` representan las bases de datos de AWS Glue catalogadas en AWS Glue Data Catalog. Por ejemplo, para mostrar estos esquemas, ejecute:

  ```
  SHOW SCHEMAS FROM DATABASE awsdatacatalog;
  ```

  Para obtener más información, consulte SHOW SCHEMAS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

- SHOW TABLES:: muestra una lista de las tablas de un esquema. Por ejemplo, para mostrar las tablas de la base de datos de AWS Glue Data Catalog denominada `awsdatacatalog` que se encuentran en el esquema `myglue`, ejecute:

  ```
  SHOW TABLES FROM SCHEMA awsdatacatalog.myschema;
  ```

  Para obtener más información, consulte SHOW TABLES en la Guía para desarrolladores de bases de datos de Amazon Redshift.

- SHOW COLUMNS: muestra la lista de columnas de una tabla. Por ejemplo, para mostrar las columnas de la base de datos de AWS Glue Data Catalog denominada `awsdatacatalog` que se encuentran en el esquema `myglue` y la tabla `mytable`, ejecute:

```
SHOW COLUMNS FROM TABLE awsdatacatalog.myglue.mytable;
```

Para obtener más información, consulte SHOW COLUMNS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para conceder permiso al usuario o rol de IAM para consultar AWS Glue Data Catalog, siga estos pasos

1. En el panel de vista de árbol, conéctese a la base de datos inicial en el clúster aprovisionado o el grupo de trabajo sin servidor mediante el método de autenticación con Nombre de usuario y contraseña de la base de datos. Por ejemplo, conéctese a la base de datos `dev` con el usuario administrador y la contraseña que utilizó al crear el clúster o el grupo de trabajo.
2. En una pestaña del editor, ejecute la siguiente instrucción SQL para conceder acceso a un usuario de IAM a AWS Glue Data Catalog.

   ```
   GRANT USAGE ON DATABASE awsdatacatalog to "IAM:myIAMUser"
   ```

   Donde *`IAM:myIAMUser`* es un usuario de IAM al que desea conceder privilegio de uso a AWS Glue Data Catalog. Como alternativa, puede conceder privilegio de uso a *`IAMR:myIAMRole`* para un rol de IAM.
3. En el panel de vista de árbol, edite o elimine la conexión al clúster o grupo de trabajo que creó anteriormente. Conéctese al clúster o grupo de trabajo de una de las siguientes maneras:
   - Para acceder a la base de datos `awsdatacatalog` desde un clúster, debe utilizar el método de autenticación Credenciales temporales con su identidad de IAM. Para obtener más información acerca de este método de autenticación, consulte Conexión a una base de datos de Amazon Redshift. Es posible que el administrador del editor de consultas v2 necesite configurar la Configuración de cuenta para mostrar este método de autenticación en la ventana de conexión.
   - Para acceder a la base de datos `awsdatacatalog` desde un grupo de trabajo, debe utilizar el método de autenticación Usuario federado. Para obtener más información acerca de este método de autenticación, consulte Conexión a una base de datos de Amazon Redshift.
4. Con el privilegio adjudicado, puede usar su identidad de IAM para ejecutar SQL con AWS Glue Data Catalog.

Después de la conexión, puede utilizar el editor de consultas v2 para consultar datos catalogados en AWS Glue Data Catalog. En el panel de vista de árbol del editor de consultas v2, elija el clúster o grupo de trabajo y la base de datos `awsdatacatalog`. En el panel del editor o del bloc de notas, confirme que se ha elegido el clúster o grupo de trabajo correcto. La base de datos elegida debe ser la base de datos inicial de Amazon Redshift, por ejemplo `dev`. Para obtener información sobre la creación de consultas, consulte Creación y ejecución de consultas y Creación y ejecución de cuadernos. La base de datos denominada `awsdatacatalog` está reservada para hacer referencia a la base de datos externa del catálogo de datos en la cuenta. Las consultas a la base de datos `awsdatacatalog` solo pueden ser de solo lectura. Utilice la notación de tres partes para hacer referencia a la tabla de la instrucción SELECT. Donde la primera parte es el nombre de la base de datos, la segunda parte es el nombre de la base de datos AWS Glue y la tercera parte es el nombre de la tabla AWS Glue.

```
SELECT * FROM awsdatacatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

Puede realizar varios escenarios que leen los datos AWS Glue Data Catalog y rellenan las tablas de Amazon Redshift.

En el siguiente ejemplo, SQL une dos tablas que se definen en AWS Glue.

```
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

En el siguiente ejemplo, SQL crea una tabla de Amazon Redshift y la rellena con datos de una combinación de dos tablas AWS Glue.

```
CREATE TABLE dev.public.glue AS
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

Consulta de un lago de datos

Puede consultar datos en un lago de datos de Amazon S3. En primer lugar, cree un esquema externo para hacer referencia a la base de datos externa en el elemento AWS Glue Data Catalog. A continuación, puede consultar datos en el lago de datos de Amazon S3.

Demostración: consulta de un lago de datos

Para obtener una demostración sobre cómo consultar un lago de datos, vea el siguiente video. Consulta del lago de datos desde el editor de consultas de Amazon Redshift V2.

Requisitos previos

Antes de trabajar con su lago de datos en el editor de consultas v2, confirme que se configuró lo siguiente en su entorno de Amazon Redshift:

- Rastree sus datos de Amazon S3 con AWS Glue y habilite su catálogo de datos para AWS Lake Formation.
- Cree un rol de IAM para Amazon Redshift mediante el catálogo de datos habilitado para AWS Glue para AWS Lake Formation. Para obtener más información sobre este procedimiento, consulte Para crear un rol de IAM para Amazon Redshift mediante un AWS Glue Data Catalog habilitado para AWS Lake Formation. Para obtener más información sobre el uso de Redshift Spectrum y Lake Formation, consulte Uso de Redshift Spectrum con AWS Lake Formation.
- Conceda permisos SELECT en la tabla para realizar consultas en la base de datos de Lake Formation. Para obtener detalles sobre este procedimiento, consulte Para otorgar permisos SELECT en la tabla para realizar consultas en la base de datos de Lake Formation.

  Puede verificar en la consola de Lake Formation (https://console.aws.amazon.com/lakeformation/), en la sección Permisos, página Permisos del lago de datos, que el rol de IAM, la base de datos de AWS Glue y las tablas de IAM tengan los permisos adecuados.
- Confirme que el usuario conectado tiene permiso para crear esquemas en la base de datos de Amazon Redshift y acceder a los datos de su lago de datos. Cuando se conecta a una base de datos en el editor de consultas v2, elige un método de autenticación que incluye credenciales, que pueden ser un usuario de la base de datos o un usuario de IAM. El usuario conectado debe tener los permisos y los privilegios de base de datos adecuados, como un `superuser`. El usuario `admin` de Amazon Redshift que creó el clúster o grupo de trabajo tiene privilegios de `superuser` y puede crear esquemas y administrar la base de datos de Redshift. Para obtener más información sobre la conexión a una base de datos con el editor de consultas v2, consulte Conexión a una base de datos de Amazon Redshift.

Creación de un esquema externo

Para consultar datos en un lago de datos de Amazon S3, cree primero un esquema externo. El esquema externo hace referencia a la base de datos externa en AWS Glue Data Catalog.

1. En la vista Editor del editor de consultas v2, elija Crear y, a continuación, Esquema.
2. Ingrese un Schema name (Nombre de esquema).
3. Para Tipo de esquema, elija Externo.
4. En los detalles de Catálogo de datos, la Región está predeterminada a la Región de AWS donde se encuentra su base de datos de Redshift.
5. Elija la Base de datos de AWS Glue a la que se asignará el esquema externo y que contiene referencias a las tablas de AWS Glue.
6. Elija un Rol de IAM para Amazon Redshift que tenga los permisos necesarios para consultar datos en Amazon S3.
7. Si lo desea, elija un Rol de IAM que tenga permiso en el catálogo de datos.
8. Elija Create schema (Crear esquema).

   El esquema aparece debajo de la base de datos en el panel de vista de árbol.

Al crear el esquema, si recibe un error de denegación de permiso para la base de datos, compruebe si el usuario conectado tiene el privilegio de base de datos para crear un esquema.

Consulta de datos en el lago de datos de Amazon S3

Utilice el esquema que creó en el procedimiento anterior.

1. En el panel de vista de árbol, elija el esquema.
2. Para ver una definición de tabla, elija una tabla. Se muestran las columnas de tabla y los tipos de datos.
3. Para consultar una tabla, elíjala y, en el menú contextual (clic con el botón derecho), elija Seleccionar tabla para generar una consulta.
4. Ejecute la consulta en el Editor.

   El editor de consultas v2 generó el siguiente ejemplo de SQL para consultar todas las filas de la tabla de AWS Glue denominada `flightscsv`. Para simplificar, se han truncado las columnas y las filas que se muestran en el resultado.

```
SELECT * FROM "dev"."mydatalake_schema"."flightscsv";
```

```
year    quarter   month   dom  day_of_week   fl_date    unique_carrier  airline_id
  carrier   tail_num   fl_num
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N753SK    3086
2016    4         10      19   3             10/19/16   OO              20304
  OO         N778SK    3087
2016 4          10      19   3             10/19/16   OO              20304
 OO         N778SK    3087
...
```

Uso de recursos compartidos de datos

Se puede crear un recurso compartido de datos para que los usuarios de otro clúster puedan consultar los datos. El clúster que contiene los datos que se desean compartir se denomina clúster productor. Se debe crear un recurso compartido de datos en el clúster productor para los objetos de base de datos que se deseen compartir. Se pueden compartir esquemas, tablas, vistas y funciones definidas por el usuario (UDF) de SQL. El clúster con el que se desean compartir los datos se denomina clúster consumidor. En el clúster consumidor, se debe crear una base de datos a partir del recurso compartido de datos. Después, los usuarios del clúster consumidor pueden consultar los datos. Para obtener más información, consulte Introducción al uso compartido de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Creación de recursos compartidos de datos

Se debe crear un recurso compartido de datos en el clúster que se desee utilizar como clúster productor. Para obtener más información sobre los recursos compartidos de datos, consulte Consideraciones sobre el uso compartido de datos en Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1. Elija la base de datos del clúster productor que desea utilizar.
2. Cree el recurso compartido de datos. Por ejemplo:

```
create datashare mysource;
```

3. Establezca permisos en el recurso compartido de datos. Por ejemplo:

```
grant alter, share on datashare mysource to admin;
```

4. Establezca permisos en los objetos de base de datos que desea compartir. Por ejemplo:

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. Establezca permisos en el espacio de nombres del clúster consumidor para acceder al recurso compartido de datos. Por ejemplo:

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-
bb1234567890';
```

Exhibición de recursos compartidos de datos

Se pueden mostrar los recursos compartidos de datos que se hayan creado en el clúster productor.

1. Elija el clúster productor.
2. Muestre los recursos compartidos de datos. Por ejemplo:

```
show datashares;
```

```
share_name share_owner source_database  consumer_database share_type createdate
 is_publicaccessible share_acl producer_account producer_namespace
test_datashare 100  db_producer  NULL   OUTBOUND 2/15/2022  FALSE  admin
 123456789012  p1234567-8765-4321-p10987654321
```

Creación de la base de datos consumidora

En el clúster consumidor, se debe crear una base de datos a partir del recurso compartido de datos. Estos pasos describen cómo compartir datos entre dos clústeres de una misma cuenta. Para obtener más información acerca de cómo compartir datos entre cuentas de AWS, consulte Uso compartido de datos entre cuentas de AWS en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Se pueden utilizar comandos SQL o el panel de vista de árbol del editor de consultas v2 para crear la base de datos.

Para utilizar SQL

1. Cree una base de datos a partir del recurso compartido de datos de la cuenta y del espacio de nombres del clúster productor. Por ejemplo:

```
create database share_db from datashare mysource of account '123456789012'
 namespace 'p1234567-8765-4321-p10987654321';
```

2. Establezca permisos para que los usuarios puedan acceder a la base de datos y al esquema. Por ejemplo:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Para utilizar el panel de vista de árbol del editor de consultas v2

1. Elija

Create (Crear) y luego elija Database (Base de datos).
2. Ingrese un Database name (Nombre de base de datos).
3. (Opcional) Seleccione Users and groups (Usuarios y grupos), y elija un Database user (Usuario de base de datos).
4. Elija Create using a datashare (Crear utilizando un recurso compartido de datos).
5. Elija el recurso compartido de datos.
6. Elija Crear base de datos.

   La nueva base de datos

datash (recurso compartido de datos) se muestra en el panel de vista de árbol del editor de consultas v2.

7. Establezca permisos para que los usuarios puedan acceder a la base de datos y al esquema. Por ejemplo:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Consulta de objetos de recursos compartidos de datos

En el clúster consumidor, se pueden consultar objetos de recursos compartidos de datos utilizando nombres de objetos completos expresados con la notación de tres partes: base de datos, esquema y nombre del objeto.

1. En el panel de vista de árbol del editor de consultas v2, elija el esquema.
2. Para ver una definición de tabla, elija una tabla.

   Se muestran las columnas de tabla y los tipos de datos.
3. Para consultar una tabla, elija la tabla y utilice el menú contextual (clic con el botón derecho) con objeto de elegir Select table (Seleccionar tabla).
4. Consulte las tablas mediante comandos SELECT. Por ejemplo:

```
select top 10 * from test_db.public.event;
```

Programación de consultas con el editor de consultas versión 2

Puede crear una programación que ejecute una instrucción SQL con el editor de consultas de Amazon Redshift versión 2. Puede crear una programación para ejecutar la instrucción SQL en los intervalos de tiempo que coincidan con las necesidades de su empresa. Cuando llega el momento de ejecutar la consulta programada, Amazon EventBridge inicia la consulta y utiliza la API de datos de Amazon Redshift.

Para crear una programación que ejecute una instrucción SQL

1. Elija la vista Editor

y elija

Programación para crear una programación que ejecute una instrucción SQL.

2. Al definir la programación, se proporciona la siguiente información:

   - El rol de IAM que asume los permisos necesarios para ejecutar la consulta. Este rol de IAM también está asociado a su clúster o grupo de trabajo.
   - Los valores de autenticación para AWS Secrets Manager o las credenciales temporales para autorizar el acceso al clúster o grupo de trabajo. La API de datos admite estos métodos de autenticación. Para obtener más información, consulte Autenticación de una consulta programada.
   - El clúster o grupo de trabajo donde reside la base de datos.
   - El nombre de la tabla de base datos que contiene los datos que se van a consultar.
   - Nombre de la consulta programada y su descripción. El editor de consultas v2 antepone el prefijo "QS2-" al nombre de la consulta programada que usted proporcione. El editor de consultas versión 1 añade el prefijo «QS-» a los nombres de las consultas programadas.
   - La instrucción SQL que se ejecutará según la programación.
   - La frecuencia de la programación y las opciones de repetición o un valor con formato cron que define la programación. Para obtener más información, consulte Cron Expressions (Expresiones cron) en la Guía del usuario de Eventos de Amazon CloudWatch.
   - Si lo desea, puede habilitar las notificaciones de Amazon SNS estándar para supervisar la consulta programada. Puede que tenga que confirmar la dirección de correo electrónico que proporcionó en la notificación de Amazon SNS. Consulte en el correo electrónico si hay un enlace para confirmar la dirección de correo electrónico para las notificaciones de Amazon SNS. Para obtener más información, consulte Notificaciones por correo electrónico en la Guía para desarrolladores de Amazon Simple Notification Service. Si su consulta se está ejecutando, pero no ve mensajes publicados en el tema de SNS, consulte Mi regla se activa pero no veo ningún mensaje publicado en mi tema de Amazon SNS en la Guía del usuario de Amazon EventBridge.

3. Seleccione Programar consulta para guardar y activar la programación y añadir la programación a la lista de consultas de la vista Consultas programadas.

La vista Consultas programadas

muestra todas las consultas programadas para sus clústeres y grupos de trabajo. En esta vista puede ver los detalles de la programación de la consulta, activar o desactivar la programación, editar la programación y eliminar la consulta programada. Al consultar los detalles de la consulta, también puede ver el historial de ejecución de la consulta con la programación.

> **Note**
>
> Una ejecución de consulta de programación solo está disponible en la lista Historial de programación durante 24 horas. Las consultas que se ejecutan de forma programada no aparecen en la vista Historial de consultas del editor de consultas v2.

Configuración de permisos para programar una consulta

Para programar consultas, el usuario de AWS Identity and Access Management (IAM) que define la programación y el rol de IAM asociado a la programación se deben configurar con los permisos de IAM para poder utilizar Amazon EventBridge y la API de datos de Amazon Redshift. Para recibir correos electrónicos de consultas programadas, también debe configurarse la notificación de Amazon SNS que especifique de forma opcional.

A continuación se describen las tareas para utilizar las políticas administradas de AWS para conceder permisos, pero según el entorno, es posible que prefiera reducir el alcance de los permisos concedidos.

Para el usuario de IAM que haya iniciado sesión en el editor de consultas versión 2, edite el usuario de IAM mediante la consola de IAM (https://console.aws.amazon.com/iam/).

- Además de los permisos para ejecutar las operaciones de Amazon Redshift y del editor de consultas versión 2, adjunte las políticas administradas `AmazonEventBridgeFullAccess` y `AmazonRedshiftDataFullAccess` AWS a un usuario de IAM.
- Como alternativa, asigne los permisos a un rol y asigne el rol al usuario.

  Adjunte una política con el permiso `sts:AssumeRole` al ARN del recurso del rol de IAM que especifique cuando defina la consulta programada. Para obtener más información sobre cómo asumir roles, consulte Conceder permisos de usuario para cambiar de rol en la Guía del usuario de IAM.

En el siguiente ejemplo, se muestra una política de permisos que asume el rol de IAM `myRedshiftRole` en la cuenta `123456789012`. El rol de IAM `myRedshiftRole` también es el rol de IAM que se adjunta al clúster o grupo de trabajo en el que se ejecuta la consulta programada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AssumeIAMRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/myRedshiftRole"
            ]
        }
    ]
}
```

Actualice la política de confianza del rol de IAM utilizado para programar la consulta a fin de permitir que el usuario de IAM la asuma.

```
{
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/myIAMusername"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Para el rol de IAM que especifique para permitir la ejecución de la consulta programada, edite el rol de IAM mediante la consola de IAM (https://console.aws.amazon.com/iam/).

- Adjunte las políticas administradas `AmazonRedshiftDataFullAccess` y `AmazonEventBridgeFullAccess` de AWS al rol de IAM. La política administrada `AmazonRedshiftDataFullAccess` solo permite el permiso `redshift-`

`serverless:GetCredentials` para los grupos de trabajo Redshift sin servidor que estén etiquetados con la clave `RedshiftDataFullAccess`.

Autenticación de una consulta programada

Cuando programa una consulta, utiliza uno de los siguientes métodos de autenticación cuando se ejecuta el código SQL. Cada método requiere una combinación diferente de entrada en el editor de consultas versión 2. Estos métodos de autenticación son compatibles con la API de datos que se utiliza para ejecutar sus instrucciones SQL.

El usuario o rol de base de datos que se utiliza para ejecutar la consulta debe tener los privilegios de base de datos necesarios. Por ejemplo, para conceder privilegios `IAMR:MyRedshiftQEv2Scheduler` a la tabla `mytable`, ejecute el siguiente comando SQL.

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

Para ver la lista de usuarios de la base de datos en su clúster o grupo de trabajo, consulte la vista del sistema `PG_USER_INFO`.

> **Note**
>
> Cualquier grupo de trabajo de Redshift sin servidor para el que programe consultas se debe etiquetar con la clave `RedshiftDataFullAccess`. Para obtener más información, consulte Autorización del acceso a la API de datos de Amazon Redshift.
> Como alternativa al etiquetado del grupo de trabajo, puede agregar una política insertada al rol de IAM (que se especifica con la programación) que permita `redshift-serverless:GetCredentials`. Por ejemplo:
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>         {
>             "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
>             "Effect": "Allow",
>             "Action": "redshift-serverless:GetCredentials",
>             "Resource": [
>                 "arn:aws:redshift-serverless:*:*:workgroup/*"
>             ]
> ```

```
        }
    ]
}
```

AWS Secrets Manager

Con este método, se proporciona un valor secreto para secret-arn que se almacena en AWS Secrets Manager. Este secreto contiene las credenciales para conectarse a la base de datos. Es posible que haya creado un secreto con las credenciales adecuadas al crear el clúster o el grupo de trabajo. El secreto debe estar etiquetado con la clave `RedshiftDataFullAccess`. Si la clave de etiqueta aún no está presente, utilice la consola de AWS Secrets Manager para agregarla. Para obtener información sobre cómo crear un secreto, consulte Creación de un secreto para las credenciales de conexión a la base de datos.

Para obtener más información acerca de los permisos mínimos, consulte Creación y administración de secretos con AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Credenciales temporales

Con este método, proporcione los valores Nombre de la base de datos y Usuario de la base de datos cuando se conecte a una base de datos de un clúster. Solo necesita proporcionar el Nombre de base de datos cuando se conecte a una base de datos de un grupo de trabajo.

Al conectarse a un clúster, la política `AmazonRedshiftDataFullAccess` permite al usuario de la base de datos denominado `redshift_data_api_user` el permiso para `redshift:GetClusterCredentials`. Si desea utilizar un usuario de base de datos diferente para ejecutar la instrucción SQL, agregue una política al rol de IAM adjunta a su clúster para permitir `redshift:GetClusterCredentials`. La siguiente política de ejemplo permite a los usuarios de la base de datos `awsuser` y `myuser`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UseTemporaryCredentialsForAllDbUsers",
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentials",
            "Resource": [
```

```
                "arn:aws:redshift:*:*:dbuser:*/awsuser",
                "arn:aws:redshift:*:*:dbuser:*/myuser"
            ]
        }
    ]
}
```

Configuración de permisos para el historial de consultas de la programación

Para permitir a los usuarios ver el historial de consultas de la programación, edite el rol de IAM (que se especifica con la programación) Relaciones de confianza para agregar permisos.

El ejemplo siguiente es una política de confianza en un rol de IAM que permite al usuario de IAM *myIAMusername* ver el historial de consultas de la programación. En lugar de permitir a un usuario de IAM el permiso `sts:AssumeRole`, puede elegir permitir a un rol de IAM este permiso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift.amazonaws.com",
                    "redshift-serverless.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "events.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/myIAMusername"
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Monitoreo de la consulta programada

Para el tema de Amazon SNS que especifique para enviar notificaciones por correo electrónico, cree el tema de Amazon SNS mediante el editor de consultas v2; para ello, navegue hasta la sección Notificaciones SNS, active el monitoreo y cree el tema con Crear un tema de SNS. El editor de consultas v2 crea el tema de Amazon SNS y agrega una entidad principal de servicio a la política de acceso para Amazon EventBridge. A continuación, se muestra un ejemplo de Política de acceso que se crea en el tema de Amazon SNS. En el ejemplo, se usan la Región de AWS *us-west-2*, la Cuenta de AWS *123456789012* y el tema de Amazon SNS *select-version-pdx-testunload*.

```
{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "Allow_Publish_Events",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:us-west-2:123456789012:select-version-pdx-testunload"
    }
  ]
}
```

Cuando se ejecuta la consulta programada, Amazon SNS envía correos electrónicos de notificación de AWS. El siguiente ejemplo muestra un correo electrónico enviado a *myemail@example.com* para la consulta programada *QS2-may25a* que se ejecutó en Región de AWS *eu-north-1* en Cuenta de AWS *123456789012* mediante el tema de notificación *may25a-SNS* de Amazon SNS.

```
{"version":"0","id":"8e4323ec-5258-7138-181b-91290e30ff9b","detail-type":"Scheduled
 Event","source":"aws.events","account":"123456789012","time":"2023-05-25T15:22:00Z",
```

```
                    "region":"eu-north-1","resources":["arn:aws:events:eu-
north-1:123456789012:rule/QS2-may25a"],"detail":{}}

--
If you wish to stop receiving notifications from this topic, please click or visit the
 link below to unsubscribe:
https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-
north-1:123456789012:may25a-SNS:0c1a3d05-39c2-4507-
bc3d-47250513d7b0&Endpoint=myemail@example.com

Please do not reply directly to this email. If you have any questions or comments
 regarding this email, please contact us at https://aws.amazon.com/support
```

Solución de problemas de configuración de la programación de una consulta

Tenga en cuenta lo siguiente si tiene problemas para programar una consulta.

Las consultas no se están ejecutando

Compruebe si el rol de IAM utilizado en la programación tiene permiso para obtener las credenciales de clúster temporales. El permiso para los clústeres aprovisionados es `redshift:GetClusterCredentialsWithIAM`. El permiso para los grupos de trabajo de Redshift sin servidor es `redshift-serverless:GetCredentials`.

No se muestra el historial programado

El usuario de IAM o rol de IAM utilizado para iniciar sesión en la consola de AWS no se ha agregado a la política de confianza del rol de IAM utilizado para programar la consulta.

Al utilizar AWS Secrets Manager para la consulta programada para la conexión, confirme que el secreto esté etiquetado con la clave `RedshiftDataFullAccess`.

Si la consulta programada utiliza una conexión de AWS Secrets Manager, el rol de IAM utilizado para programar la consulta debe tener el equivalente a una política administrada `SecretsManagerReadWrite` asociada al rol.

El estado del historial de consultas es **`Failed`**

Consulte la vista del sistema SYS_QUERY_HISTORY para obtener detalles sobre por qué se produjo un error en la consulta. Un problema habitual es que el usuario o el rol de la base de datos que se utilizó para ejecutar la consulta podría no tener los privilegios necesarios para ejecutar el código SQL. Para obtener más información, consulte Autenticación de una consulta programada.

El siguiente código SQL consulta la vista SYS_QUERY_HISTORY para devolver las consultas con errores.

```
SELECT user_id, query_id, transaction_id, session_id, database_name, query_type,
 status, error_message, query_text
FROM sys_query_history
WHERE status = 'failed';
```

Para conocer los detalles de una determinada consulta programada con errorrd , consulte Búsqueda de detalles sobre las consultas programadas con AWS CloudShell.

Búsqueda de detalles sobre las consultas programadas con AWS CloudShell

Puede utilizar AWS CloudShell para conocer los detalles de una consulta programada. Debe tener los permisos adecuados para ejecutar los comandos de la AWS CLI que se muestran en el procedimiento siguiente.

Para ver los resultados de una consulta programada

1. En la consola de AWS, abra el símbolo del sistema de AWS CloudShell. Para obtener más información acerca de AWS CloudShell, consulte ¿Qué es AWS CloudShell? en la Guía del usuario de AWS CloudShell.
2. Asuma el rol de IAM de la consulta programada. Para asumir el rol, busque el rol de IAM asociado a la consulta programada en el editor de consultas v2 y utilícelo en el comando AWS CLI en AWS CloudShell. Por ejemplo, para el rol `scheduler` introduzca un comando AWS STS para asumir el rol que utiliza la consulta programada.

   ```
   aws sts assume-role –role-arn "arn:aws:iam::123456789012:role/scheduler" –role-
   session-name "scheduler-test"
   ```

   Las credenciales devueltas son similares a las siguientes.

   ```
   "Credentials": {
   "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
   "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
   "SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
   "Expiration": "2023-08-18T18:19:44+00:00"
   },
   "AssumedRoleUser": {
   ```

```
"AssumedRoleId": "AROA35B2NH6WBTP7ONL4E:scheduler-test",
"Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
}
}
```

3. Cree variables de entorno en la AWS CLI mediante las credenciales que se muestran al asumir el rol de IAM. Debe utilizar estos tokens antes de que caduquen. Por ejemplo, puede introducir lo siguiente en AWS CloudShell.

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
```

4. Para ver el error de una consulta con errores, ejecute el comando AWS CLI para describir una instrucción. El ID de la instrucción SQL procede del ID que aparece en la sección Historial de programación de una consulta programada en el editor de consultas v2.

```
aws redshift-data describe-statement –id 130d2620-05d2-439c-b7cf-815d9767f513
```

En este ejemplo, la instrucción SQL programada `select * from users limit 100` da como resultado un error de SQL que indica que la tabla `users` no existe.

```
{
"CreatedAt": "2023-08-18T17:39:15.563000+00:00",
"Duration": -1,
"Error": "ERROR: relation \"users\" does not exist",
"HasResultSet": false,
"Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"QueryString": "select * from users limit 100\n–RequestID=a1b2c3d4-5678-90ab-cdef-
EXAMPLE22222; TraceID=1-633c5642-4039308d03f3a0ba53dbdf6f",
"RedshiftPid": 1073766651,
"RedshiftQueryId": 0,
"ResultRows": -1,
"ResultSize": -1,
"Status": "FAILED",
"UpdatedAt": "2023-08-18T17:39:16.116000+00:00",
"WorkgroupName": "default"
}
```

Demostración de la programación de una consulta

Para ver una demostración de cómo programar una consulta, vea el siguiente vídeo. Demostración en vídeo de la programación de una consulta.

Visualización de resultados de las consultas

Después de ejecutar una consulta y mostrar los resultados, puede activar Chart (Gráfico) para mostrar una visualización gráfica de la página actual de resultados. Puede utilizar los siguientes controles para definir el contenido, la estructura y el aspecto del gráfico:

Seguimiento de

Representa un conjunto de marcas gráficas relacionadas en un gráfico. Puede definir varios seguimientos en un gráfico.

Tipo

Puede definir el tipo de seguimiento para representar los datos como uno de los siguientes:

- Gráfico de dispersión para un gráfico de dispersión o gráfico de burbujas.
- Gráfico de barras para representar categorías de datos con barras verticales u horizontales.
- Gráfico de áreas para definir áreas rellenadas.
- Histograma que utiliza barras para representar la distribución de frecuencias.
- Gráfico circular para una representación circular de datos en la que cada sector representa un porcentaje del conjunto.
- Gráfico de embudo o de área de embudo para representar datos a lo largo de varias etapas de un proceso.
- Gráfico OHLC (apertura, máximo, mínimo, cierre), que se utiliza a menudo en datos financieros para representar valores de apertura, máximos, mínimos y de cierre a lo largo del eje x, que suele representar intervalos de tiempo.
- Gráfico de velas para representar un rango de valores de una categoría a lo largo de una línea temporal.
- Gráfico de cascada para representar cómo aumenta o disminuye un valor inicial mediante una serie de valores intermedios. Los valores pueden representar intervalos de tiempo o categorías.
- Gráfico de líneas para representar los cambios en el valor a lo largo del tiempo.

Eje X

Debe especificar una columna de tabla que contenga valores para trazar a lo largo del eje X. Las columnas que contienen valores descriptivos suelen representar datos dimensionales. Las columnas que contienen valores cuantitativos suelen representar datos descriptivos.

Eje Y

Debe especificar una columna de tabla que contiene valores para trazar a lo largo del eje Y. Las columnas que contienen valores descriptivos suelen representar datos dimensionales. Las columnas que contienen valores cuantitativos suelen representar datos descriptivos.

Tramas secundarias

Puede definir presentaciones adicionales de los datos de gráficos.

Transformaciones

Puede definir transformaciones para filtrar los datos de seguimiento. Se utiliza una transformación de división para mostrar varios seguimientos de un único seguimiento de origen. Se utiliza una transformación de agregación para presentar un seguimiento como promedio o valor mínimo. Se usa una transformación de ordenación para ordenar un seguimiento.

Aspecto general

Puede establecer valores predeterminados para el color de fondo, el color de los márgenes, las escalas de color para las paletas de diseño, el estilo y los tamaños del texto, el estilo y el tamaño del título y la barra de modos. Puede definir interacciones para arrastrar, hacer clic y pasar el cursor. Puede definir metatexto. Puede definir aspectos predeterminados para seguimientos, ejes, leyendas y anotaciones.

Elija Traces (Rastros) para mostrar los resultados en forma de gráfico. En Type (Tipo), elija el estilo de gráfico como Bar (Barra), Line (Línea) y así sucesivamente. En Orientation (Orientación), puede elegir Vertical u Horizontal. En X, elija la columna de la tabla que desea utilizar para el eje horizontal. En Y, elija la columna de la tabla que desea utilizar para el eje vertical.

Elija Refresh (Actualizar) para actualizar la visualización del gráfico. Elija Full screen (Pantalla completa) para ampliar la visualización del gráfico.

Para crear una alarma

1. Ejecute una consulta y obtenga resultados.

2. Active Charts (Gráficos).
3. Elija Trace (Rastro) y comience a visualizar sus datos.
4. Elija un estilo de gráfico de los siguientes:

   - Dispersión
   - Barras
   - Área
   - Histograma
   - Circular
   - Embudo
   - Área de embudo
   - OHLC (apertura, máximo, mínimo, cierre)
   - Velas
   - Cascada
   - Línea
5. Elija Style (Estilo) para personalizar el aspecto, incluidos los colores, los ejes, la leyenda y las anotaciones. Puede agregar texto, formas e imágenes.
6. Elija Annotations (Anotaciones) para agregar texto, formas e imágenes.

Para guardar un gráfico

1. Elija Save Chart (Guardar gráfico).
2. Ingrese un nombre para el gráfico.
3. Elija Guardar.

Para exportar un gráfico

1. Seleccione Exportar.
2. Elija PNG o JPEG.
3. Establezca el ancho y la altura del gráfico.
4. Seleccione Exportar.
5. Elija abrir el archivo en su aplicación gráfica predeterminada o guarde el archivo con el nombre predeterminado.

Para buscar y abrir un gráfico guardado

1. Elija la pestaña Charts (Gráficos).
2. Abra el gráfico que desee.

Para organizar los gráficos en carpetas

1. Elija Charts (Gráficos) en el panel de navegación.
2. Elija New folder (Nueva carpeta) y asigne un nombre a la carpeta.
3. Elija Create (Crear) para crear la carpeta en la pestaña Charts (Gráficos).

   Puede mover gráficos dentro y fuera de la carpeta arrastrando y soltando.

Ejemplo: Creación de un gráfico circular para visualizar los resultados de consultas

En el siguiente ejemplo, se utiliza la tabla Sales (Ventas) de la base de datos de muestra. Para obtener más información, consulte Base de datos de muestra en la Guía para desarrolladores de bases de datos de Amazon Redshift.

A continuación, se presenta la consulta que ejecuta para proporcionar los datos del gráfico circular.

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

Para crear un gráfico circular para el evento principal por ventas totales

1. Ejecute la consulta.
2. En el área de resultados de la consulta, active Chart (Gráfico).
3. Elija Trace (Rastro).
4. En Type (Tipo), elija Pie (Circular).
5. En Values (Valores), elija totalsales.
6. En Labels (Etiquetas), elija eventname.
7. Elija Style (Estilo) y luego General.
8. En Colorscales, elija Categorical y luego Pastel2.

Ejemplo: Creación de un gráfico combinado para comparar ingresos y ventas

Siga los pasos de este ejemplo para crear un gráfico que combine un gráfico de barras para los datos de ingresos y uno de líneas para los datos de ventas. En el siguiente ejemplo, se utiliza la tabla Sales (Ventas) de la base de datos de ejemplo TICKIT. Para obtener más información, consulte Base de datos de muestra en la Guía para desarrolladores de bases de datos de Amazon Redshift.

A continuación, se presenta la consulta que ejecuta para proporcionar los datos del gráfico.

```
select eventname, total_price, total_qty_sold
from  (select eventid, total_price, total_qty_sold, ntile(1000) over(order by
 total_price desc) as percentile
       from (select eventid, sum(pricepaid) total_price, sum(qtysold) total_qty_sold
             from   tickit.sales
             group by eventid)) Q, tickit.event E
       where Q.eventid = E.eventid
       and percentile = 1
order by total_price desc;
```

Creación de un gráfico combinado para comparar ingresos y ventas

1. Ejecute la consulta.
2. En el área de resultados de la consulta, active Chart (Gráfico).
3. En trace o, para Type (Tipo), elija Bar (Barras).
4. En X (X), elija eventname.
5. Para Y (Y), elija total_price.

   El gráfico de barras se muestra con nombres de eventos a lo largo del eje X.

6. En Style (Estilo), elija Traces (Seguimientos).
7. En Name (Nombre), ingrese Revenue (Ingresos).
8. En Style (Estilo), elija Axes (Ejes).
9. En Titles (Títulos), elija Y (Y) e ingrese Revenue (Ingresos).

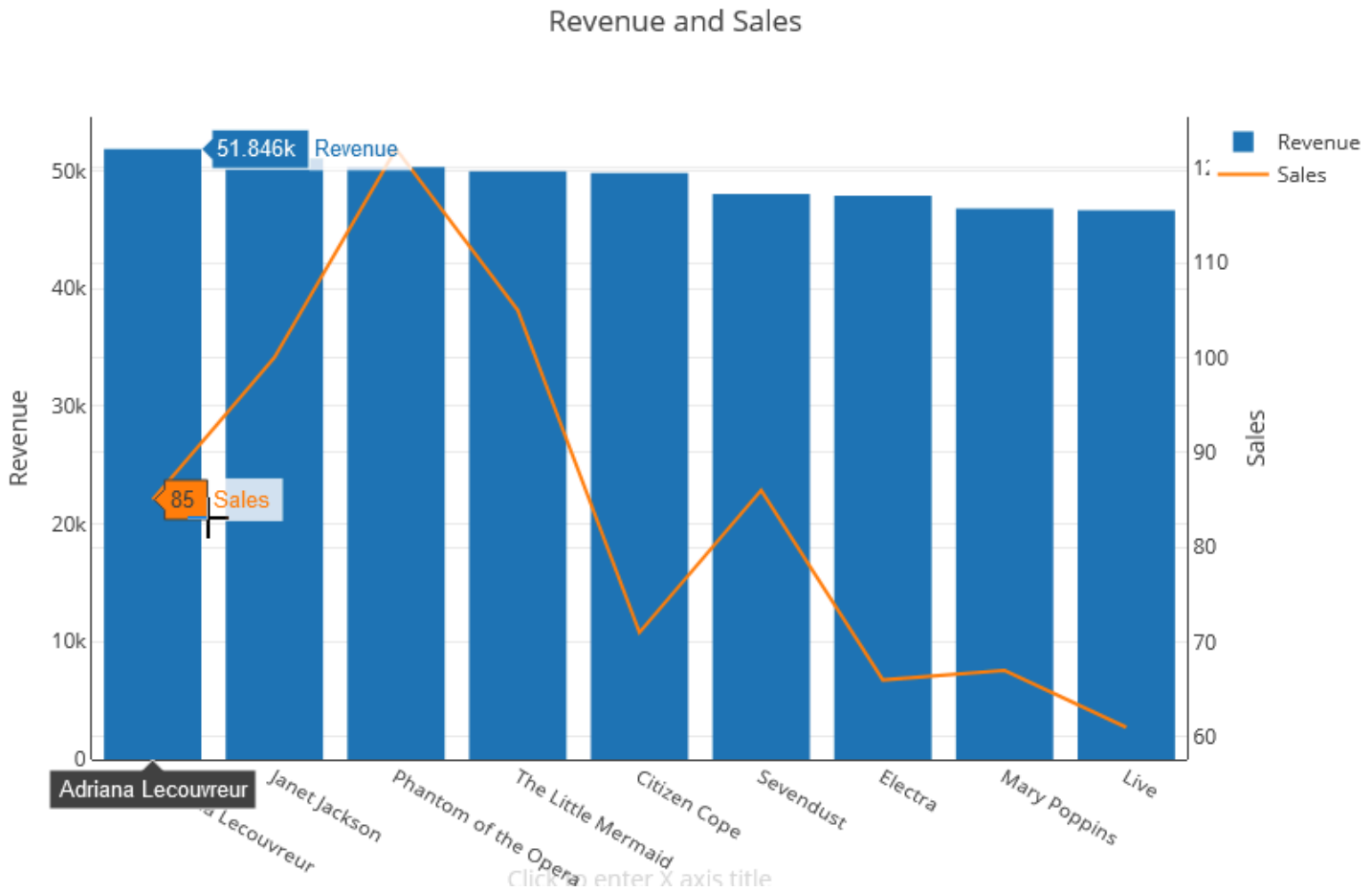
   La etiqueta Revenue (Ingresos) se muestra en el eje Y izquierdo.
10. En Structure (Estructura), elija Traces (Seguimientos).
11. Elija

    Trace (Seguimiento).

    Se muestran las opciones de seguimiento 1.
12. En Type (Tipo), elija Line (De líneas).
13. En X (X), elija eventname.
14. En Y (Y), elija total_qty_sold.
15. En Axes To Use (Ejes que se deben utilizar), para Y Axis (Eje Y) elija

    .

    El Y Axis (Eje Y) muestra Y2.
16. En Style (Estilo), elija Axes (Ejes).
17. En Titles (Títulos), elija Y2 (Y2).
18. En Name (Nombre), ingrese Sales (Ventas).
19. En Lines (Líneas), elija Y:Sales (Y: ventas).
20. En Axis Line (Línea de eje), elija Show (Mostrar) y paraPosition (Posición), elija Right (Derecha).



Demostración: Creación de visualizaciones mediante el editor de consultas de Amazon Redshift V2

Para obtener una demostración de cómo crear visualizaciones, vea el siguiente video. Creación de visualizaciones mediante el editor de consultas de Amazon Redshift V2.

Colaboración y uso compartido en equipo

Puede compartir consultas con su equipo.

Se define un equipo para un conjunto de usuarios que colaboran y comparten recursos del editor de consultas v2. Un administrador puede crear un equipo añadiendo una etiqueta a un rol de IAM. Para obtener más información, consulte Permisos necesarios para usar del editor de consultas v2 .

Guardar, buscar y eliminar consultas

Antes de poder compartir la consulta con su equipo, guarde la consulta. Puede ver y eliminar las consultas guardadas.

Para guardar una consulta

1. Prepare la consulta y elija Save (Guardar).
2. Ingrese un título para la consulta.
3. Elija Guardar.

Para buscar consultas guardadas

1. Elija Queries (Consultas) en el panel de navegación.
2. Puede ver las consultas que son My queries (Mis consultas), Shared by me (Compartidas por mí) o bien Shared to my team (Compartidas con mi equipo). Estas consultas pueden aparecer como consultas individuales o dentro de las carpetas que creó.

Para eliminar una consulta guardada

1. Abra el menú contextual (clic derecho) de una consulta guardada.
2. Elija Delete (Eliminar) y confirme la acción.

Para organizar las consultas guardadas en carpetas

1. Elija Queries (Consultas) en el panel de navegación.
2. Elija New folder (Nueva carpeta) y asigne un nombre a la carpeta.
3. Elija Create (Crear) para crear la carpeta en la pestaña Queries (Consultas).

   Ahora puede mover consultas dentro y fuera de la carpeta arrastrando y soltando.

Compartir una consulta

Puede compartir las consultas con su equipo. También puede ver el historial de consultas guardadas y administrar versiones de consultas.

Para compartir una consulta con su equipo, asegúrese de que tiene la etiqueta principal `sqlworkbench-team` con el mismo valor que el resto de los miembros del equipo de su cuenta. Por ejemplo, un administrador podría establecer el valor en `accounting-team` para todos los miembros del departamento de contabilidad. Para ver un ejemplo, consulte Permisos necesarios para usar del editor de consultas v2 .

Para compartir una consulta con un equipo

1. Elija Queries (Consultas) en el panel de navegación.
2. Abra el menú contextual (clic derecho) de la consulta que desea compartir y elija Share with my team (Compartir con mi equipo).
3. Elija el equipo o los equipos con los que quiere compartir la consulta y, a continuación, elija Save sharing options (Guardar opciones de uso compartido).

Cada vez que guarda una consulta SQL, el editor de consultas v2 la guarda como una nueva versión. Puede explorar versiones de consultas anteriores, guardar una copia de una consulta o restaurar una consulta.

Para administrar versiones de consultas

1. Elija Queries (Consultas) en el panel de navegación.
2. Abra el menú contextual (clic derecho) de la consulta con la que desea trabajar.
3. Elija Version history (Historial de versiones) para abrir una lista de versiones de la consulta.
4. En la página Version history (Historial de versiones), puede hacer lo siguiente:
   - Revert to Selected (Volver a la versión seleccionada): vuelva a la versión seleccionada y continúe trabajando con esta versión.
   - Save selected as (Guardar versión seleccionada como): cree una nueva consulta en el editor.

Consulta de una base de datos mediante el editor de consultas

El uso del editor de consultas es el método más sencillo para ejecutar consultas en las bases de datos alojadas en el clúster de Amazon Redshift. Después de crear el clúster, puede ejecutar consultas de forma inmediata mediante el editor de consultas en la consola de Amazon Redshift.

> **Note**
>
> No puede consultar datos en Amazon Redshift Serverless con este editor de consultas original. Utilice en su lugar el editor de consultas V2 de Amazon Redshift.

En febrero de 2021, se implementó un editor de consultas actualizado y se modificaron los permisos de autorización para utilizar el editor de consultas. El editor de consultas nuevo utiliza la API de

datos de Amazon Redshift para ejecutar consultas. La política `AmazonRedshiftQueryEditor`, que es una política administrada por AWS de AWS Identity and Access Management (IAM), se actualizó para incluir los permisos necesarios. Si tiene una política de IAM personalizada, asegúrese de actualizarla. Utilice `AmazonRedshiftQueryEditor` como una guía. Entre los cambios en `AmazonRedshiftQueryEditor`, se incluyen los siguientes:

- El permiso para administrar los resultados de la instrucción del editor de consultas requiere el usuario propietario de la instrucción.
- Se agregó el permiso para utilizar Secrets Manager para conectarse a una base de datos.

Para obtener más información, consulte Permisos necesarios para usar el editor de consultas de la consola de Amazon Redshift.

Cuando se conecta al clúster desde el editor de consultas nuevo, puede utilizar uno de los dos métodos de autenticación, como se describe en Conexión con el editor de consultas.

Con el editor de consultas, puede realizar lo siguiente:

- Ejecutar consultas con instrucciones SQL.
- Descargar conjuntos de resultados de hasta 100 MB en un archivo de valores separados por comas (CSV).
- Guardar consultas para su reutilización. No se puede guardar consultas en las regiones de Europa (París), Asia-Pacífico (Osaka), Asia-Pacífico (Hong Kong) o Medio Oriente (Baréin).
- Ver los detalles del tiempo de ejecución de consultas para tablas definidas por los usuarios.
- Programar consultas para que se ejecuten en un momento futuro.
- Ver un historial de consultas que creó en el editor de consultas.
- Ejecutar consultas en clústeres mediante el enrutamiento de VPC mejorado.

Consideraciones sobre el editor de consultas

Tenga en cuenta lo siguiente acerca de cómo trabajar con consultas cuando utiliza el editor de consultas:

- La duración máxima de una consulta es de 24 horas.
- El tamaño máximo del resultado de la consulta es de 100 MB. Si una llamada devuelve más de 100 MB de datos de respuesta, la llamada termina.

- El tiempo máximo de retención de los resultados de la consulta es de 24 horas.
- El tamaño máximo de las instrucciones de la consulta es de 100 KB.
- El clúster debe estar en una nube virtual privada (VPC) basada en el servicio Amazon VPC.
- No puede usar transacciones en el editor de consultas. Para obtener más información acerca de las transacciones, consulte BEGIN en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Puede guardar una consulta con un tamaño máximo de 3000 caracteres.

Habilitar el acceso al editor de consultas

Para obtener acceso al editor de consultas, necesita permiso. Para habilitar el acceso, le recomendamos que adjunte las políticas `AmazonRedshiftQueryEditor` y `AmazonRedshiftReadOnlyAccess` administradas por AWS para obtener permisos de IAM para el rol de IAM que utiliza para acceder al clúster. A continuación, puede asignar el rol a un usuario. Puede utilizar la consola de IAM (https://console.aws.amazon.com/iam/) para adjuntar políticas de IAM. Para obtener más información, consulte Uso de políticas basadas en identidad (políticas de IAM) para Amazon Redshift.

Si ya ha creado un usuario para acceder a Amazon Redshift, puede adjuntar las políticas `AmazonRedshiftQueryEditor` y `AmazonRedshiftReadOnlyAccess` administradas por AWS a ese rol asignado. Si aún no ha creado un usuario, cree uno, adjunte la política al rol de IAM y asigne el rol al usuario.

La política administrada por AWS `AmazonRedshiftQueryEditor` permite la acción `redshift:GetClusterCredentials`, que, de forma predeterminada, concede acceso de superusuario a la base de datos. Para restringir el acceso, puede realizar una de las siguientes acciones:

- Crear una política personalizada que permita llamar a `redshift:GetClusterCredentials` y restrinja el recurso a un valor determinado para `DbUser`.
- Agregue una política que deniegue el permiso a `redshift:GetClusterCredentials`. Cualquier usuario al que se le asigne un rol con este permiso adjunto debe iniciar sesión en el editor de consultas con credenciales temporales. Esta política de denegación ilustra el ejemplo.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": {
    "Effect": "Deny",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "*"
  }
}
```

Para obtener más información sobre la creación de un rol y los permisos necesarios, consulte Crear un rol de IAM con permisos para llamar a GetClusterCredentials.

A cualquier usuario al que se le conceda acceso al editor de consultas de Amazon Redshift mediante la política `AmazonRedshiftQueryEditor` administrada por AWS podrá enumerar todos los secretos. Sin embargo, esta política solo permite la creación y la recuperación de secretos etiquetados con la clave `RedshiftQueryOwner` y el valor `${aws:userid}`. Si crea la clave desde el editor de consultas de Amazon Redshift, la clave se etiqueta de forma automática. Para utilizar un secreto que no se creó con el editor de consultas de Amazon Redshift, confirme que el secreto está etiquetado con la clave `RedshiftQueryOwner` y un valor de su identificador de usuario de IAM único; por ejemplo, `AIDACKCEVSQ6C2EXAMPLE`.

Los permisos necesarios para usar el editor de consultas de Amazon Redshift son AmazonRedshiftQueryEditor y AmazonRedshiftReadOnlyAccess.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Conexión con el editor de consultas

Cuando se conecta a un clúster con el editor de consultas, utiliza uno de los siguientes métodos de autenticación. Cada método requiere una combinación diferente de entrada de la consola de Amazon Redshift.

AWS Secrets Manager

Con este método, se proporciona un valor secreto para secret-arn que se almacena en AWS Secrets Manager. Este secreto contiene las credenciales para conectarse a la base de datos.

Credenciales temporales

Con este método, se proporcionan los valores de su base de datos y del db-user (usuario de la base de datos).

Almacenamiento de credenciales de base de datos en AWS Secrets Manager

Cuando llama al editor de consultas, puede pasar las credenciales del clúster mediante un secreto en AWS Secrets Manager. Para pasar credenciales de esta manera, especifique el nombre del secreto o el nombre de recurso de Amazon (ARN) del secreto.

Para obtener más información acerca de los permisos mínimos, consulte Creación y administración de secretos con AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Si desea almacenar las credenciales en un secreto para un clúster de Amazon Redshift

1. Utilice AWS Secrets Manager para crear un secreto que contenga credenciales para el clúster. Cuando elija Store a new secret (Almacenar un secreto nuevo), elija Credentials for Redshift cluster (Credenciales para clúster de Redshift). Almacene un valor para User name (Nombre del usuario) (el usuario de la base de datos), Password (Contraseña) y DB cluster (Clúster de base de datos) (identificador del clúster) en su secreto.

   Para obtener instrucciones, consulte Creación de un secreto básico en la Guía del usuario de AWS Secrets Manager.
2. Utilice la consola de AWS Secrets Manager para ver los detalles del secreto que ha creado, o ejecute el comando de la AWS CLI `aws secretsmanager describe-secret`.

Si opta por utilizar las credenciales de administrador de su clúster con AWS Secrets Manager, puede conectarse a la base de datos con las credenciales de administrador almacenadas en Secrets Manager.

Uso del editor de consultas de

En el siguiente ejemplo, se utiliza el editor de consultas para realizar las siguientes tareas:

- Ejecutar comandos SQL.
- Ver detalles de ejecución de consultas.
- Guardar una consulta.
- Descargar un conjunto de resultados de consultas.

Para completar el siguiente ejemplo, necesita un clúster de Amazon Redshift existente. Si no dispone de un clúster, cree uno mediante el siguiente procedimiento que se describe en Creación de un clúster.

Si desea utilizar el editor de consultas en la consola de Amazon Redshift

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Query editor (Editor de consultas) y conéctese a una base de datos en el clúster.
3. Para Schema (Esquema), elija public (público) para crear una nueva tabla basada en ese esquema.
4. En la ventana del editor de consultas, escriba lo siguiente y elija Run (Ejecutar) para crear una nueva tabla.

```
create table shoes(
                shoetype varchar (10),
                color varchar(10));
```

5. Elija Clear (Borrar).
6. Introduzca el siguiente comando en la ventana del editor de consultas y seleccione Run Query (Ejecutar consulta) para agregar filas a la tabla.

```
insert into shoes values
```

```
('loafers', 'brown'),
('sandals', 'black');
```

7. Elija Clear (Borrar).
8. En la ventana del editor de consultas, escriba el siguiente comando y elija Run (Ejecutar) para realizar una consulta en la nueva tabla.

```
select * from shoes;
```

Query results (Resultados de la consulta) mostrará los resultados.

Tipo de zapato	Color
sandals	black
loafers	brown

9. Seleccione Execution (Ejecución) para ver los detalles de la ejecución.
10. Seleccione Data (Datos) y Export (Exportar) para descargar los resultados de la consulta como un archivo.

Programación de una consulta

> **Important**
>
> El editor de consultas de Amazon Redshift v2 ahora permite programar una consulta. Recomendamos utilizar el editor de consultas v2. Para obtener más información, consulte Programación de consultas con el editor de consultas versión 2.

Para crear una programación que ejecute una instrucción SQL, puede utilizar el editor de consultas en la consola de Amazon Redshift. Puede crear una programación para ejecutar la instrucción SQL en los intervalos de tiempo que concuerden con las necesidades de su empresa. Cuando llega el momento de ejecutar la consulta programada, Amazon EventBridge inicia la consulta.

Para crear una programación que ejecute una instrucción SQL

1. Abra la consola y el editor de consultas como se describe en Uso del editor de consultas de . Solo puede usar este editor de consultas con clústeres aprovisionados.
2. Elija Schedule (Programación) para crear una programación que ejecute una instrucción SQL.

   Cuando se define la programación, se proporciona la siguiente información:

   - Un rol de IAM que se utiliza para asumir los permisos necesarios para ejecutar la consulta. Para obtener más información, consulte Configuración de permisos para programar una consulta.
   - Los valores de autenticación para AWS Secrets Manager o las credenciales temporales para autorizar el acceso al clúster. Para obtener más información, consulte Autenticación de una consulta programada.
   - El nombre de la consulta programada y una instrucción SQL única que se ejecutará.
   - La frecuencia de la programación y las opciones de repetición o un valor con formato cron.
   - Si lo desea, puede habilitar las notificaciones de Amazon SNS para supervisar la consulta programada. Si su consulta se está ejecutando, pero no ve mensajes publicados en su tema de SNS, consulte Mi regla se desencadena, pero no veo ningún mensaje publicado en mi tema de Amazon SNS en la Guía del usuario de Amazon EventBridge.

También puede administrar y actualizar las consultas programadas mediante la consola de Amazon Redshift. Según la versión de la consola, es posible que las consultas programadas se muestren en los siguientes lugares:

- En la pestaña Schedules (Programaciones) de la página de detalles del clúster.
- En la pestaña Scheduled queries (Consultas programadas) del editor de consultas.

Si elige Schedule name (Nombre de la programación) en una de estas ubicaciones, podrá ver y editar la definición de la consulta programada.

Configuración de permisos para programar una consulta en la consola de Amazon Redshift

Para programar consultas, el usuario de AWS Identity and Access Management (IAM) que define la programación y el rol de IAM asociado a la programación se deben configurar de la siguiente manera.

Para el usuario de IAM que ha iniciado sesión en la consola de Amazon Redshift, haga lo siguiente:

- Adjunte la política `AmazonEventBridgeFullAccess` administrada por AWS a un rol de IAM.
- Adjunte una política con el permiso `sts:AssumeRole` del rol de IAM que especificará cuando defina la instrucción SQL programada.

  En el siguiente ejemplo, se muestra una política que asume un rol de IAM específico.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "AssumeIAMRole",
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::account-id:role/sql-statement-iam-role"
        }
    ]
}
```

Para el rol de IAM que especifique para permitir que el programador ejecute una consulta, haga lo siguiente:

- Asegúrese de que el rol de IAM especifique la entidad principal del servicio EventBridge (`events.amazonaws.com`). A continuación, se muestra un ejemplo de relación de confianza.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Para obtener más información acerca de cómo crear un rol de IAM para eventos de EventBridge, consulte Permisos necesarios para usar el programador de Amazon EventBridge.

- Adjunte la política `AmazonRedshiftDataFullAccess` administrada por AWS al rol de IAM.
- Para permitir a los usuarios ver el historial de programación, edite el rol de IAM para agregar el permiso `sts:AssumeRole`.

El ejemplo siguiente es una política de confianza en un rol de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Autenticación de una consulta programada

Cuando programa una consulta, utiliza uno de los siguientes métodos de autenticación cuando se ejecuta la consulta SQL. Cada método requiere una combinación diferente de entrada de la consola de Amazon Redshift.

AWS Secrets Manager

Con este método, se proporciona un valor secreto para secret-arn que se almacena en AWS Secrets Manager. Este secreto contiene las credenciales para conectarse a la base de datos. El secreto debe estar etiquetado con la clave `RedshiftDataFullAccess`.

Para obtener más información acerca de los permisos mínimos, consulte Creación y administración de secretos con AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Credenciales temporales

Con este método, se proporcionan los valores de su base de datos y del db-user (usuario de la base de datos).

La política `AmazonRedshiftDataFullAccess` otorga al usuario de la base de datos llamado `redshift_data_api_user` el permiso para `redshift:GetClusterCredentials`. Si desea utilizar un usuario de base de datos diferente para ejecutar la instrucción SQL, agregue una política al rol de IAM para permitir `redshift:GetClusterCredentials`. La siguiente política de ejemplo permite a los usuarios de la base de datos `awsuser` y `myuser`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UseTemporaryCredentialsForAllDbUsers",
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentials",
            "Resource": [
                "arn:aws:redshift:*:*:dbuser:*/awsuser",
                "arn:aws:redshift:*:*:dbuser:*/myuser"
            ]
        }
    ]
}
```

Creación de una regla de Amazon EventBridge que se ejecuta cuando finaliza una consulta

Puede crear una regla de evento para enviar una notificación cuando finaliza una consulta. Para obtener información sobre el procedimiento mediante la consola de Amazon EventBridge, consulte Creación de reglas de Amazon EventBridge que reaccionan a los eventos en la Guía del usuario de Amazon EventBridge. Para obtener más información sobre patrones de eventos, consulte Patrones de eventos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Por ejemplo, el siguiente evento de ejemplo se envía cuando una consulta es `FINISHED`.

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
```

```
    "detail-type": "Redshift Data Statement Status Change",
    "source": "aws.redshift-data",
    "account": "123456789012",
    "time": "2020-12-22T17:00:00Z",
    "region": "us-west-1",
    "resources": [
        "arn:aws:redshift:us-east-2:123456789:cluster:t1"
    ],
    "detail": {
        "statementId": "01bdaca2-8967-4e34-ae3f-41d9728d5644",
        "clusterId": "test-dataapi",
        "statementName": "awesome query",
        "state": "FINISHED",
        "pages": 5,
        "expireAt": "2020-12-22T18:43:48Z",
        "principal": "arn:aws:sts::123456789012:assumed-role/any",
        "queryId": 123456
    }
}
```

Puede crear una regla de patrón de eventos para filtrar el evento.

```
{
    "source": [
        "aws.redshift-data"
    ],
    "detail-type": [
        "Redshift Data Statement Status Change"
    ],
    "detail": {
        "state": [
            "FINISHED"
        ]
    }
}
```

Conexión a un almacenamiento de datos de Amazon Redshift mediante herramientas de cliente SQL

Puede conectarse a almacenamientos de datos de Amazon Redshift desde herramientas de cliente SQL mediante conexiones Java Database Connectivity (JDBC), Python y Open Database

Connectivity (ODBC). Amazon Redshift no proporciona ni instala ninguna biblioteca o herramienta de cliente SQL. Para utilizar estas herramientas o bibliotecas para trabajar con datos de los almacenamientos de datos, instálelas en el equipo cliente o la instancia de Amazon EC2. Puede utilizar la mayoría de las herramientas de cliente SQL que admiten los controladores JDBC, Python u ODBC.

Utilice la lista de secciones al final de este tema para ayudarle a seguir el proceso de configuración del equipo cliente o la instancia de Amazon EC2 para utilizar una conexión JDBC, Python u ODBC. En estos temas, también se tratan las opciones de seguridad relacionadas para la conexión del cliente al servidor. Además, busque información sobre la configuración y la conexión desde herramientas del cliente de SQL, como SQL Workbench/J, una herramienta de terceros y Amazon Redshift RSQL. Puede probar estas herramientas si aún no tiene una herramienta de inteligencia empresarial que usar. También puede utilizar esta sección para aprender sobre cómo conectarse a su almacenamiento de datos mediante programación. Por último, si surge algún problema cuando pruebe conectarse a su almacenamiento de datos, puede revisar la información de solución de problemas para identificar soluciones.

Recomendaciones para conectarse con las herramientas cliente

Si se conecta a su clúster de Redshift mediante una dirección IP, puede provocar un tiempo de inactividad adicional si se produce una interrupción o una pérdida de conexión y el clúster se pone en línea en una nueva zona de disponibilidad (AZ). Sin embargo, si aún desea que su aplicación se conecte a Redshift mediante una dirección IP, use la dirección IP privada asociada al punto de conexión de nube privada virtual (VPC) del clúster. Puede encontrarla en los detalles del clúster en Red y seguridad, en la pestaña Propiedades.

> **Note**
>
> Si su aplicación utiliza la dirección IP del nodo principal para acceder al clúster de Redshift, la práctica recomendada es cambiarla para que utilice la URL del punto de conexión del clúster. Para obtener más información, consulte Configuración de conexiones en Amazon Redshift.

Temas

- Configuración de conexiones en Amazon Redshift
- Configuración de las opciones de seguridad para las conexiones
- Conexión desde herramientas y código cliente

- Conexión con SQL Workbench/J
- Conexión a un almacenamiento de datos mediante programación
- Puede conectarse a Amazon Redshift con un perfil de autenticación.
- Solución de problemas de conexión en Amazon Redshift

Configuración de conexiones en Amazon Redshift

En la siguiente sección, obtenga información sobre cómo configurar conexiones JDBC, Python y ODBC para conectarse al clúster desde las herramientas de cliente SQL. En esta sección se describe cómo configurar conexiones JDBC, Python y ODBC. También describe cómo utilizar la Capa de conexión segura (SSL) y certificados de servidor para cifrar la comunicación entre el cliente y el servidor.

Controladores JDBC, Python y ODBC para Amazon Redshift

Para trabajar con datos en el clúster, debe tener controladores JDBC, Python u ODBC con objeto de establecer una conectividad desde el equipo cliente o instancia. Cifre sus aplicaciones para utilizar operaciones de API de acceso a datos JDBC, Python u ODBC y utilice las herramientas de cliente SQL que admitan JDBC, Python o bien con ODBC.

Amazon Redshift permite descargar los controladores JDBC, Python y ODBC. Estos controladores admiten AWS Support. El equipo de Amazon Redshift no prueba los controladores de PostgreSQL ni ofrece asistencia para los mismos. Utilice los controladores específicos de Amazon Redshift cuando se conecte a un clúster de Amazon Redshift. Los controladores de Amazon Redshift tienen las siguientes ventajas:

- compatibilidad con IAM, SSO y autenticación federada
- compatibilidad con los nuevos tipos de datos de Amazon Redshift
- compatibilidad con perfiles de autenticación
- rendimiento mejorado junto con las mejoras de Amazon Redshift

Para obtener más información acerca de cómo descargar los controladores JDBC y ODBC y cómo configurar las conexiones a su clúster, consulte Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift, Configuración del conector Python de Amazon Redshift y Configuración de una conexión ODBC.

Para obtener más información sobre cómo administrar las identidades de IAM, incluidas las prácticas recomendadas para los roles de IAM, consulte Administración de identidades y accesos en Amazon Redshift.

Obtención de la cadena de conexión a su clúster

Para conectarse al clúster con la herramienta de cliente SQL, debe tener la cadena de conexión de clúster. Puede encontrar la cadena de conexión al clúster en la consola de Amazon Redshift en la página de detalles del clúster.

Para encontrar la cadena de conexión de un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles.
3. Las cadenas de conexión de la URL de JDBC y la URL de ODBC están disponibles, junto con detalles adicionales, en la sección Información general. Cada cadena se basa en la región de AWS en la que se ejecuta el clúster. Haga clic en el icono situado junto a la cadena de conexión adecuada para copiarlo.

Para conectarse a un punto de conexión de clúster, puede utilizar la URL del punto de conexión de clúster de una solicitud de la API DescribeClusters. A continuación se muestra un ejemplo de URL de un punto de conexión de clúster.

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

Si ha configurado un nombre de dominio personalizado para el clúster, también puede utilizarlo para conectarse a él. Para obtener más información sobre la creación de un nombre de dominio personalizado, consulte Configuración de un nombre de dominio personalizado.

> **Note**
>
> Cuando se conecte, no utilice la dirección IP de un nodo del clúster ni la dirección IP del punto de conexión de VPC. Utilice siempre el punto de conexión de Redshift para evitar una interrupción innecesaria. La única excepción a utilizar la URL del punto de conexión

es cuando se utiliza un nombre de dominio personalizado. Para obtener más información, consulte Uso de un nombre de dominio personalizado para las conexiones de cliente.

Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift

Puede utilizar una conexión del controlador JDBC versión 2.1 para conectarse a su clúster de Amazon Redshift desde distintas herramientas de cliente SQL de terceros. El conector JDBC de Amazon Redshift proporciona una solución de código abierto. Puede examinar el código fuente, solicitar mejoras, informar problemas y realizar aportaciones.

Para utilizar una conexión JDBC, consulte las siguientes secciones.

Temas

- Descargar el controlador JDBC versión 2.1 de Amazon Redshift
- Instalación del controlador JDBC versión 2.1 de Amazon Redshift
- Obtención de la URL de JDBC
- Creación de la URL de conexión
- Configuración de keepalives de TCP para su conexión JDBC
- Configuración de la conexión JDBC con Apache Maven
- Configuración de la autenticación y SSL
- Configuración del registro
- Conversión de tipos de datos
- Uso de la compatibilidad con instrucciones preparadas
- Diferencias entre las versiones 2.1 y 1.x del controlador JDBC
- Creación de archivos de inicialización (.ini) para el controlador JDBC versión 2.1
- Opciones de configuración del controlador JDBC versión 2.1
- Versiones anteriores del controlador JDBC versión 2.1

Descargar el controlador JDBC versión 2.1 de Amazon Redshift

Amazon Redshift ofrece controladores para herramientas compatibles con la API JDBC 4.2. El nombre de clase para este controlador es `com.amazon.redshift.Driver`.

Para obtener información detallada acerca de cómo instalar el controlador JDBC, referenciar las bibliotecas del controlador JDBC y registrar la clase de controlador, consulte los siguientes temas.

En cada computadora en la que utilice el controlador JDBC versión 2.1 de Amazon Redshift, asegúrese de que está instalado Java Runtime Environment (JRE) 8.0.

Si utiliza el controlador JDBC de Amazon Redshift para la autenticación de bases de datos, debe asegurarse de tener la versión 1.11.118 o posterior de AWS SDK for Java en la ruta de clases de Java. Si no tiene AWS SDK for Java instalado, descargue el archivo ZIP con el controlador compatible con JDBC 4.2 y las bibliotecas dependientes del controlador para AWS SDK:

- Versión 2.1 del controlador compatible con JDBC 4.2 y bibliotecas dependientes del controlador con AWS SDK

  Este archivo ZIP contiene la versión 2.1 del controlador que admite JDBC 4.2 y los archivos de biblioteca dependientes del controlador de AWS SDK para Java 1.x. Descomprima los archivos jar dependientes en la misma ubicación que el controlador JDBC. Solo el controlador JDBC debe estar en CLASSPATH.

  Este archivo ZIP no incluye el AWS SDK para Java 1.x completo. No obstante, incluye las bibliotecas dependientes del controlador de AWS SDK para Java 1.x que son necesarias para la autenticación de la base de datos de AWS Identity and Access Management (IAM).

  Utilice el controlador JDBC de Amazon Redshift con el AWS SDK necesario para la autenticación de la base de datos de IAM.

  Para instalar el AWS SDK para Java 1.x completo, consulte AWS SDK para Java 1.x en la Guía para desarrolladores de AWS SDK for Java.
- Versión 2.1 del controlador compatible con JDBC 4.2 (sin AWS SDK)

Revise la licencia de software y el archivo de registro de cambios del controlador JDBC versión 2.1:

- Licencia del controlador JDBC versión 2.1
- Registro de cambios del controlador JDBC versión 2.1

Los controladores JDBC versión 1.2.27.1051 y posterior admiten los procedimientos almacenados de Amazon Redshift. Para obtener más información, consulte Creación de procedimientos almacenados en Amazon Redshift en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Instalación del controlador JDBC versión 2.1 de Amazon Redshift

Para instalar la versión 2.1 del controlador que admite JDBC 4.2 de Amazon Redshift y las bibliotecas dependientes del controlador para AWS SDK, extraiga los archivos del archivo ZIP al directorio de su elección.

Para instalar la versión 2.1 del controlador que admite JDBC 4.2 de Amazon Redshift (sin el AWS SDK), copie el archivo JAR al directorio de su elección.

Para acceder a un almacén de datos de Amazon Redshift mediante el controlador JDBC de Amazon Redshift, debe realizar la configuración tal como se describe a continuación.

Temas

- Referencia a las bibliotecas de controladores JDBC
- Registro de la clase de controlador

Referencia a las bibliotecas de controladores JDBC

La aplicación JDBC o el código Java que utiliza para conectarse a los datos debe obtener acceso a los archivos JAR del controlador. En la aplicación o el código, especifique todos los archivos JAR que haya extraído del archivo ZIP.

Uso del controlador en una aplicación JDBC

Por lo general, las aplicaciones de JDBC proporcionan un conjunto de opciones de configuración que permiten agregar una lista de archivos de bibliotecas de controladores. Utilice las opciones proporcionadas para incluir todos los archivos JAR del archivo ZIP como parte de la configuración del controlador en la aplicación. Para obtener más información, consulte la documentación de su aplicación de JDBC.

Uso del controlador en código Java

Debe incluir todos los archivos de la biblioteca de controladores en la ruta de clase. Esta es la ruta en la que Java Runtime Environment busca las clases y otros archivos de recursos. Para obtener más información, consulte la documentación de Java SE correspondiente con el fin de establecer la ruta de clase para su sistema operativo.

- Windows: https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html
- Linux y Solaris: https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html

- MacOS: la ruta de clases predeterminada de MacOS es el directorio en el que está instalado el controlador JDBC.

Registro de la clase de controlador

Asegúrese de registrar la clase adecuada para su aplicación. Utilice las siguientes clases para conectar el controlador JDBC de Amazon Redshift a los almacenes de datos de Amazon Redshift:

- Las clases `Driver` amplían `java.sql.Driver`.
- Las clases `DataSource` amplían `javax.sql.DataSource` y `javax.sql.ConnectionPoolDataSource`.

El controlador admite los siguientes nombres de clase completamente calificados que son independientes a la versión de JDBC:

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

En el siguiente ejemplo, se muestra cómo utilizar la clase DriverManager para establecer una conexión para JDBC 4.2.

```
            private static Connection connectViaDM() throws Exception
{
Connection connection = null;
connection = DriverManager.getConnection(CONNECTION_URL);
return connection;
}
```

En el siguiente ejemplo, se muestra cómo utilizar la clase `DataSource` para establecer una conexión.

```
 private static Connection connectViaDS() throws Exception
{
Connection connection = null;
11
```

```
Amazon Redshift JDBC Driver Installation and Configuration Guide
DataSource ds = new com.amazon.redshift.jdbc.DataSource
();
ds.setURL(CONNECTION_URL);
connection = ds.getConnection();
return connection;
}
```

Obtención de la URL de JDBC

Para poder conectarse a su clúster de Amazon Redshift desde una herramienta de cliente SQL, necesita saber la URL de JDBC de su clúster. La URL de JDBC tiene el siguiente formato: `jdbc:redshift://`*`endpoint`*`:`*`port`*`/`*`database`*.

Los campos del formato anterior presentan los siguientes valores.

Campo	Valor
`jdbc`	Protocolo para la conexión.
`redshift`	El subprotocolo que especifica el uso de un controlador de Amazon Redshift para conectarse a la base de datos.
`endpoint`	El punto de conexión del clúster de Amazon Redshift.
`port`	Número de puerto que especificó cuando lanzó el clúster. Si tiene un firewall, asegúrese de que este puerto esté abierto para poder usarlo.
`database`	Base de datos que creó para su clúster.

A continuación, se muestra un ejemplo de la URL de un JDBC: `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Asegúrese de ingresar los valores de URL; por ejemplo, los valores de SessionToken, en un formato codificado como URL.

Para obtener información acerca de cómo crear su propia conexión JDBC, consulte Obtención de la cadena de conexión a su clúster.

Si el equipo cliente no puede conectarse a la base de datos, puede solucionar los posibles problemas. Para obtener más información, consulte Solución de problemas de conexión en Amazon Redshift.

Creación de la URL de conexión

Utilice la URL de conexión para proporcionar información de conexión al almacén de datos al que se accede. A continuación, se muestra el formato de la URL de conexión del controlador JDBC versión 2.1 de Amazon Redshift. A continuación, [Host] es el punto de conexión del servidor de Amazon Redshift y [Port] es el número del puerto del protocolo de control de transmisión (TCP) que utiliza el servidor para atender las solicitudes de los clientes.

```
jdbc:redshift://[Host]:[Port]
```

A continuación, se muestra el formato de una URL de conexión que especifica algunos parámetros de configuración opcionales.

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];
[Property2]=[Value];
```

Por ejemplo, imagine que desea conectarse al puerto 9000 en un clúster de Amazon Redshift en la región EE. UU. Oeste (Norte de California) en AWS. Además, desea acceder a la base de datos denominada `dev` y autenticar la conexión mediante un nombre de usuario de base de datos y una contraseña. En este caso, se utiliza la siguiente URL de conexión.

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/
dev;UID=amazon;PWD=amazon
```

Puede utilizar los siguientes caracteres para separar las opciones de configuración del resto de la cadena de URL:

- ;
- ?

Por ejemplo, las siguientes cadenas de URL son equivalentes:

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev?ssl=false;defaultRowFetchSize=100
```

Puede utilizar los siguientes caracteres para separar las opciones de configuración unas de otras en la cadena de URL:

- ;
- &

Por ejemplo, las siguientes cadenas de URL son equivalentes:

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev;ssl=false&defaultRowFetchSize=100
```

En el siguiente ejemplo de URL, se especifica un nivel de registro igual a 6 y la ruta a los registros.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

No duplique las propiedades en la URL de conexión.

Para obtener una lista completa de las opciones de configuración que se pueden especificar, consulte Opciones de configuración del controlador JDBC versión 2.1.

> **Note**
>
> Cuando se conecte, no utilice la dirección IP de un nodo del clúster ni la dirección IP del punto de conexión de VPC. Utilice siempre el punto de conexión de Redshift para evitar una interrupción innecesaria. La única excepción a utilizar la URL del punto de conexión es cuando se utiliza un nombre de dominio personalizado. Para obtener más información, consulte Uso de un nombre de dominio personalizado para las conexiones de cliente.

Configuración de keepalives de TCP para su conexión JDBC

De forma predeterminada, el controlador JDBC de Amazon Redshift está configurado para usar keepalives de TCP y, de este modo, evitar que se agote el tiempo de espera en las conexiones. Puede especificar cuándo comienza el controlador a enviar paquetes keepalive o desactivar la

característica mediante la configuración de las propiedades correspondientes en la URL de conexión. Para obtener más información acerca de la sintaxis de la URL de conexión, consulte Creación de la URL de conexión.

Propiedad	Descripción
`TCPKeepAlive`	Para desactivar keepalives de TCP, establezca esta propiedad en `FALSE`.

Configuración de la conexión JDBC con Apache Maven

Apache Maven es una herramienta de software para la comprensión y administración de proyectos. AWS SDK for Java es compatible con los proyectos de Apache Maven. Para obtener más información, consulte Uso del SDK con Apache Maven en la Guía para desarrolladores de AWS SDK for Java.

Si usa Apache Maven, puede configurar y crear sus proyectos de forma que utilicen un controlador JDBC de Amazon Redshift para conectarse al clúster de Amazon Redshift. Para hacerlo, agregue el controlador JDBC como dependencia en el archivo `pom.xml` de su proyecto. Si usa Maven para configurar su proyecto y desea usar una conexión JDBC, siga los pasos que se indican en la siguiente sección.

Configuración del controlador JDBC como una dependencia de Maven

Pasos para configurar el controlador JDBC como una dependencia de Maven

1. Agregue el repositorio de Amazon o el de Maven Central a la sección de repositorios de su archivo `pom.xml`.

   > **Note**
   >
   > La URL del siguiente código devuelve un error si se utiliza en un navegador. Utilice esta URL solo en el contexto de un proyecto Maven.

   En el caso de un repositorio de Amazon Maven, utilice lo siguiente.

   ```
   <repositories>
   ```

```
    <repository>
      <id>redshift</id>
      <url>http://redshift-maven-repository.s3-website-us-east-1.amazonaws.com/
release</url>
    </repository>
</repositories>
```

Para conectarse mediante la capa de conexión segura (SSL), agregue el siguiente repositorio al archivo `pom.xml`.

```
<repositories>
    <repository>
      <id>redshift</id>
      <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
    </repository>
</repositories>
```

En el caso de un repositorio de Maven Central, agregue lo siguiente al archivo `pom.xml`.

```
<repositories>
    <repository>
      <id>redshift</id>
      <url>https://repo1.maven.org/maven2</url>
    </repository>
</repositories>
```

2. Declare la versión del controlador que desea usar en la sección de dependencias de su archivo `pom.xml`.

   Amazon Redshift ofrece controladores para herramientas compatibles con la API JDBC 4.2. Para obtener información acerca de la funcionalidad admitida por estos controladores, consulte Descargar el controlador JDBC versión 2.1 de Amazon Redshift.

   Agregue una dependencia para el controlador tal como se muestra a continuación.

   En el siguiente ejemplo, reemplace *`driver-version`* por la versión de su controlador; por ejemplo, `2.1.0.1`.

   En el caso de un controlador compatible con JDBC 4.2, utilice lo siguiente.

```
<dependency>
```

```
    <groupId>com.amazon.redshift</groupId>
    <artifactId>redshift-jdbc42</artifactId>
    <version>driver-version</version>
</dependency>
```

El nombre de clase para este controlador es `com.amazon.redshift.Driver`.

Los controladores Maven de Amazon Redshift necesitan contar con las siguientes dependencias opcionales cuando se utiliza la autenticación de base de datos de IAM.

```
<dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-core</artifactId>
      <version>1.12.23</version>
      <scope>runtime</scope>
      <optional>true</optional>
</dependency>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-redshift</artifactId>
      <version>1.12.23</version>
      <scope>runtime</scope>
      <optional>true</optional>
</dependency>
<dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-sts</artifactId>
      <version>1.12.23</version>
      <scope>runtime</scope>
      <optional>true</optional>
</dependency>
```

Actualización a la versión más reciente del controlador

Para actualizar o cambiar el controlador JDBC de Amazon Redshift a la última versión, modifique primero la sección de versión de la dependencia a la última versión del controlador. Luego limpie su proyecto con el Maven Clean Plugin, como se indica a continuación.

```
mvn clean
```

Configuración de la autenticación y SSL

Con el fin de proteger los datos contra accesos no autorizados, los almacenes de datos de Amazon Redshift requieren la autenticación de todas las conexiones mediante credenciales de usuario. Algunos almacenes de datos también requieren que las conexiones se realicen a través del protocolo de capa de conexión segura (SSL), ya sea con autenticación unidireccional o sin ella.

El controlador JDBC Versión 2.1 de Amazon Redshift proporciona compatibilidad total con estos protocolos de autenticación.

La versión de SSL que admite el controlador depende de la versión de JVM que se utilice. Para obtener información acerca de las versiones de SSL compatibles con cada versión de Java, consulte Diagnóstico de TLS, SSL y HTTPS en el Blog de Administración de productos de Java Platform Group.

La versión de SSL utilizada para la conexión es la versión más alta que admiten tanto el controlador como el servidor, la cual se determina en el momento de la conexión.

Configure el controlador JDBC de Amazon Redshift versión 2.1 para autenticar la conexión de acuerdo con los requisitos de seguridad del servidor de Redshift al que se está conectando.

Para autenticar la conexión, proporcione siempre su nombre de usuario y contraseña de Redshift. En función de si SSL está habilitado y requerido en el servidor, es posible que también necesite configurar el controlador para que se conecte a través de SSL. También podría utilizar la autenticación SSL unidireccional para que el cliente (el propio controlador) verifique la identidad del servidor.

Debe proporcionar la información de configuración al controlador en la URL de conexión. Para obtener más información acerca de la sintaxis de la URL de conexión, consulte Creación de la URL de conexión.

SSL referencia TLS o SSL, es decir, Transport Layer Security y capa de conexión segura, respectivamente. El controlador es compatible con las versiones estándar del sector de TLS o SSL.

Uso del nombre de usuario y la contraseña únicamente

Si el servidor al que se conecta no utiliza SSL, solo tendrá que proporcionar su nombre de usuario de Redshift y contraseña para autenticar la conexión.

Para configurar la autenticación mediante su nombre de usuario de Redshift y contraseña únicamente

1. Establezca la propiedad `UID` a su nombre de usuario de Redshift para obtener acceso al servidor de Amazon Redshift.
2. Establezca la propiedad PWD a la contraseña correspondiente a su nombre de usuario de Redshift.

Uso de SSL sin verificación de identidad

Si el servidor al que se conecta utiliza SSL pero no requiere verificación de identidad, entonces se puede configurar el controlador para que use una fábrica de SSL sin validación.

Para configurar una conexión SSL sin verificación de identidad

1. Establezca la propiedad `UID` a su nombre de usuario de Redshift para obtener acceso al servidor de Amazon Redshift.
2. Establezca la propiedad `PWD` a la contraseña correspondiente a su nombre de usuario de Redshift.
3. Establezca la propiedad `SSLFactory` en `com.amazon.redshift.ssl.NonValidatingFactory`.

Uso de la autenticación SSL unidireccional

Si el servidor al que se conecta utiliza SSL y dispone de un certificado, entonces se puede configurar el controlador de modo que verifique la identidad del servidor mediante una autenticación unidireccional.

La autenticación unidireccional requiere un certificado SSL firmado y de confianza que permita verificar la identidad del servidor. Se puede configurar el controlador para que utilice un certificado específico u obtenga acceso a un TrustStore que contenga el certificado pertinente. Si no se especifica un certificado o TrustStore, el controlador utiliza el TrustStore de Java predeterminado (por lo general, `jssecacerts` o `cacerts`).

Para configurar la autenticación SSL unidireccional

1. Establezca la propiedad UID a su nombre de usuario de Redshift para obtener acceso al servidor de Amazon Redshift.

2. Establezca la propiedad PWD a la contraseña correspondiente a su nombre de usuario de Redshift.
3. Establezca la propiedad SSL en “true” (verdadera).
4. Establezca la propiedad SSLRootCert en la ubicación del certificado de entidad de certificación raíz.
5. Si no utiliza uno de los TrustStores de Java predeterminados, realice una de las siguientes acciones:
   - Si desea especificar un certificado de servidor, establezca la propiedad SSLRootCert en la ruta completa del certificado.
   - Para especificar un TrustStore, realice lo siguiente:
     a. Utilice el programa keytool para agregar el certificado del servidor al TrustStore que desea usar.
     b. Especifique el TrustStore y la contraseña que se utilizará cuando se inicie la aplicación Java con el controlador. Por ejemplo:

```
-Djavax.net.ssl.trustStore=[TrustStoreName]
-Djavax.net.ssl.trustStorePassword=[TrustStorePassword]
-Djavax.net.ssl.trustStoreType=[TrustStoreType]
```

6. Elija una:
   - Para validar el certificado, establezca la propiedad SSLMode en verify-ca.
   - Para validar el certificado y verificar el nombre de alojamiento que aparece en él, establezca la propiedad SSLMode en verify-full.

Configuración de la autenticación de IAM

Si se conecta a un servidor de Amazon Redshift mediante la autenticación de IAM, establezca las siguientes propiedades como parte de la cadena de conexión del origen de datos.

Para obtener más información acerca de la autenticación de IAM, consulte Administración de identidades y accesos en Amazon Redshift.

Para usar la autenticación de IAM, utilice uno de los siguientes formatos de cadena de conexión:

Cadena de conexión	Descripción
`jdbc:redshift:iam:// [host]:[port]/[db]`	Una cadena de conexión normal. El controlador infiere el ClusterID y la región del alojamiento.
`jdbc:redshift:iam:// [cluster-id]: [region]/[db]`	A partir del ClusterID y de la región, el controlador recupera la información del alojamiento.
`jdbc:redshift:iam:// [host]/[db]`	El controlador utiliza el puerto 5439 de forma predeterminada e infiere el ClusterID y la región del alojamiento. Según el puerto que haya seleccionado al crear, modificar o migrar el clúster, se permitirá el acceso al puerto seleccionado.

Especificación de perfiles

Si utiliza la autenticación de IAM, puede especificar cualquier otra propiedad de conexión necesaria u opcional en un nombre de perfil. De este modo, puede evitar incluir determinada información directamente en la cadena de conexión. El nombre del perfil se especifica en la cadena de conexión mediante la propiedad Profile (Perfil).

Se pueden agregar perfiles al archivo de credenciales de AWS. La ubicación predeterminada de este archivo es `~/.aws/credentials`

Puede cambiar el valor predeterminado si configura la ruta en la siguiente variable de entorno: `AWS_CREDENTIAL_PROFILES_FILE`

Para obtener más información acerca de los perfiles, consulte Uso de las credenciales de AWS en la AWS SDK for Java.

Uso de credenciales del perfil de instancias

Si ejecuta una aplicación en una instancia de Amazon EC2 que está asociada a un rol de IAM, puede conectarse mediante las credenciales del perfil de instancias.

Para ello, utilice uno de los formatos de cadena de conexión de IAM que figuran en la tabla precedente y establezca la propiedad de conexión dbuser en el nombre de usuario de Amazon Redshift al que se conectará.

Para obtener más información acerca de los perfiles de instancias, consulte Administración de accesos en la Guía del usuario de IAM.

Uso de proveedores de credenciales

Además, el controlador es compatible con los complementos de proveedores de credenciales correspondientes a los siguientes servicios:

- Active Directory Federation Service (ADFS)
- Servicio de JSON Web Tokens (JWT)
- Servicio de Microsoft Azure Active Directory (AD) y navegador del servicio de Microsoft Azure Active Directory (AD)
- Servicio de Okta
- Servicio de PingFederate
- Navegador de SAML para servicios de SAML, tales como Okta, Ping o ADFS

Si utiliza uno de estos servicios, la URL de conexión debe especificar las siguientes propiedades:

- Plugin_Name: la ruta de clase completa para la clase de complemento del proveedor de credenciales.
- IdP_Host: el alojamiento del servicio que se utiliza para la autenticación en Amazon Redshift.
- IdP_Port: el puerto en el que se atiende el alojamiento para el servicio de autenticación. No es necesario para el caso de Okta.
- Usuario: el nombre de usuario para el servidor idp_host.
- Contraseña: la contraseña asociada al nombre de usuario idp_host.
- DbUser: el nombre de usuario de Amazon Redshift con el cual se conecta.
- SSL_insecure: indica si se debe verificar el certificado del servidor IDP.
- client_id: el ID de cliente asociado al nombre de usuario en el portal de Azure AD. Se usa únicamente para Azure AD.
- Client_Secret: el secreto del cliente asociado al ID del cliente en el portal de Azure AD. Se usa únicamente para Azure AD.

- IdP_Tenant: el ID de inquilino de Azure AD para su aplicación de Amazon Redshift. Se usa únicamente para Azure AD.
- App_ID: el ID de la aplicación Okta para su aplicación de Amazon Redshift. Se usa únicamente para Okta.
- App_Name: el nombre de la aplicación Okta opcional para su aplicación de Amazon Redshift. Se usa únicamente para Okta.
- Partner_SPID: el valor opcional del SPID (ID del proveedor de servicios) del socio. Se usa únicamente para PingFederate.

Si utiliza un complemento del navegador para uno de estos servicios, la URL de conexión también puede incluir lo siguiente:

- Login_URL: la dirección URL del recurso en el sitio web del proveedor de identidad cuando se utiliza el lenguaje de marcado para confirmaciones de seguridad (SAML) o los servicios Azure AD a través de un complemento del navegador. Este parámetro es obligatorio si utiliza un complemento del navegador.

- Listen_Port: el puerto que utiliza el controlador para obtener la respuesta SAML del proveedor de identidad cuando se usan los servicios SAML o Azure AD a través de un complemento del navegador.

- IdP_Response_Timeout: la cantidad de tiempo, en segundos, que espera el controlador para obtener la respuesta SAML del proveedor de identidad cuando se usan los servicios SAML o Azure AD a través de un complemento del navegador.

Para obtener más información acerca de las propiedades adicionales de la cadena de conexión, consulte Opciones de configuración del controlador JDBC versión 2.1.

Configuración del registro

Puede activar el registro en el controlador para que sea de ayuda en el diagnóstico de problemas.

Puede registrar la información del controlador mediante los siguientes métodos:

- Para guardar la información registrada en archivos .log, consulte Uso de archivos de registros.

- Para enviar la información registrada a LogStream o LogWriter que se especifica en DriverManager, consulte Uso de LogStream o LogWriter.

Debe proporcionar la información de configuración al controlador en la URL de conexión. Para obtener más información acerca de la sintaxis de la URL de conexión, consulte Creación de la URL de conexión.

Uso de archivos de registros

Solo active el registro durante tiempo suficiente para capturar un problema. El registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Establezca la clave LogLevel en su URL de conexión para activar el registro y especificar la cantidad de detalles incluidos en los archivos de registros. En la siguiente tabla, se enumeran los niveles de registro proporcionados por el controlador JDBC versión 2.1 de Amazon Redshift, ordenados desde el menos detallado hasta el más detallado.

Valor de LogLevel	Descripción
1	Se registran eventos de errores graves que harán que el controlador se anule.
2	Se registran eventos de errores que podrían hacer que el controlador siga ejecutándose.
3	Se registran eventos que podrían dar lugar a un error si no se toman medidas al respecto. Este nivel de registro y los niveles superiores también registran las consultas del usuario.
4	Se registra información general que describe el progreso del controlador.
5	Se registra información detallada útil para depurar el controlador.
6	Se registra toda la actividad del controlador.

Para configurar el registro que utiliza los archivos de registros

1. Establezca la propiedad LogLevel en el nivel de información que desee incluir en los archivos de registros.
2. Establezca la propiedad LogPath en la ruta completa de la carpeta en la que desea guardar los archivos de registros.

   Por ejemplo, la siguiente URL de conexión habilita el nivel de registro 3 y guarda los archivos de registro en la carpeta C:\temp: `jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp`
3. Para asegurarse de que la nueva configuración surta efecto, reinicie su aplicación JDBC y vuelva a conectarse al servidor.

   El controlador JDBC de Amazon Redshift produce los siguientes archivos de registros en la ubicación que se especifica en la propiedad LogPath:

   - El archivo redshift_jdbc.log que registra la actividad del controlador y no es específica de una conexión.
   - El archivo redshift_jdbc_connection_[Number].log correspondiente a cada conexión realizada a la base de datos, en el que [Number] es un número que identifica a cada archivo de registro. Este archivo registra la actividad del controlador específica de la conexión.

Si el valor de LogPath no es válido, el controlador envía la información registrada a la secuencia de salida estándar (`System.out`)

Uso de LogStream o LogWriter

Solo active el registro durante tiempo suficiente para capturar un problema. El registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Establezca la clave LogLevel en su URL de conexión para activar el registro y especificar la cantidad de detalles enviados a LogStream o LogWriter que se indican en DriverManager.

Para activar el registro que utiliza el LogStream o LogWriter:

1. Para configurar el controlador de modo que registre información general que describa el progreso del controlador, establezca la propiedad LogLevel en 1 o INFO.
2. Para asegurarse de que la nueva configuración surta efecto, reinicie su aplicación JDBC y vuelva a conectarse al servidor.

Para desactivar el registro que utiliza LogStream o LogWriter:

1. Elimine la propiedad LogLevel de la URL de conexión.
2. Para asegurarse de que la nueva configuración surta efecto, reinicie su aplicación JDBC y vuelva a conectarse al servidor.

Conversión de tipos de datos

El controlador JDBC versión 2.1 de Amazon Redshift admite varios formatos de datos frecuentes, por lo que permite la conversión entre los tipos de datos de Amazon Redshift, SQL y Java.

En la siguiente tabla, se enumeran los mapeos de tipos de datos admitidos.

Tipo de Amazon Redshift	Tipo de SQL	Tipo de Java
BIGINT	SQL_BIGINT	Largo
BOOLEAN	SQL_BIT	Booleano
CHAR	SQL_CHAR	Cadena
FECHA	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMERIC	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Doble
GEOMETRY	SQL_ LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	Entero
OID	SQL_BIGINT	Largo
SUPER	SQL_LONGVARCHAR	Cadena
REAL	SQL_REAL	Flotante
SMALLINT	SQL_SMALLINT	Short
TEXT	SQL_VARCHAR	Cadena

Tipo de Amazon Redshift	Tipo de SQL	Tipo de Java
TIME	SQL_TYPE_TIME	java.sql.time
TIMETZ	SQL_TYPE_TIME	java.sql.time
TIMESTAMP	SQL_TYPE_ TIMESTAMP	java.sql.Timestamp
TIMESTAMPTZ	SQL_TYPE_ TIMESTAMP	java.sql.Timestamp
VARCHAR	SQL_VARCHAR	Cadena

Uso de la compatibilidad con instrucciones preparadas

El controlador JDBC de Amazon Redshift admite instrucciones preparadas. Puede utilizar instrucciones preparadas para mejorar el rendimiento de las consultas basadas en parámetros que deban ejecutarse varias veces durante la misma conexión.

Una instrucción preparada es una instrucción SQL que se compila en el lado del servidor pero que no se ejecuta de inmediato. La instrucción compilada se almacena en el servidor como un objeto PreparedStatement hasta que se cierra dicho objeto o la conexión. Mientras exista ese objeto, se puede ejecutar la instrucción preparada tantas veces como sea necesario con distintos valores de parámetros, sin necesidad de volver a compilar la instrucción. Gracias a esta reducción de la sobrecarga, el conjunto de consultas se ejecuta con mayor rapidez.

Para obtener más información acerca de las instrucciones preparadas, consulte “Uso de instrucciones preparadas” en el Tutorial sobre conocimientos básicos de JDBC de Oracle.

Puede preparar una instrucción que contenga varias consultas. Por ejemplo, la siguiente instrucción preparada contiene dos consultas INSERT:

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

Asegúrese de que estas consultas no dependan de los resultados de otras consultas que se hayan especificado dentro de la misma instrucción preparada. Como las consultas no se ejecutan durante el paso de preparación, los resultados aún no se han devuelto y no se encuentran disponibles para las demás consultas en la misma instrucción preparada.

Por ejemplo, no se permite la siguiente instrucción preparada, en la que se crea una tabla y, a continuación, se insertan valores en esa tabla recién creada:

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

Si se intenta preparar esta instrucción, el servidor devuelve un error en el que se indica que la tabla de destino (myTable) aún no existe. La consulta CREATE se debe ejecutar antes de que se pueda preparar la consulta INSERT.

Diferencias entre las versiones 2.1 y 1.x del controlador JDBC

En esta sección, se describen las diferencias que presenta la información devuelta por las versiones 2.1 y 1.x del controlador JDBC. El controlador JDBC versión 1.x se suspende.

En la siguiente tabla, se muestra la información de DatabaseMetadata que devuelven las funciones getDatabaseProductName() y getDatabaseProductVersion() para cada versión del controlador JDBC. El controlador JDBC versión 2.1 obtiene los valores mientras se establece la conexión. El controlador JDBC versión 1.x obtiene los valores a partir de una consulta.

Versión del controlador JDBC	Resultado de getDatabaseProductName()	Resultado de getDatabaseProductVersion()
2.1	Redshift	8.0.2
1.x	PostgreSQL	08.00.0002

En la siguiente tabla, se muestra la información de DatabaseMetadata que devuelve la función getTypeInfo para cada versión del controlador JDBC.

Versión del controlador JDBC	Resultado de getTypeInfo
2.1	Consistente con los tipos de datos de Redshift
1.x	Consistente con los tipos de datos de PostgreSQL

Creación de archivos de inicialización (.ini) para el controlador JDBC versión 2.1

Mediante el uso de archivos de inicialización (.ini) para el controlador JDBC versión 2.1 de Amazon Redshift, es posible especificar los parámetros de configuración en el nivel del sistema. Por ejemplo, los parámetros de autenticación del IdP federado pueden variar para cada aplicación. El archivo .ini proporciona una ubicación común para que los clientes SQL obtengan los parámetros de configuración necesarios.

Se puede crear un archivo de inicialización (.ini) del controlador JDBC versión 2.1 que contenga opciones de configuración para clientes SQL. El nombre del archivo predeterminado es `rsjdbc.ini`. El controlador JDBC versión 2.1 busca el archivo .ini en las siguientes ubicaciones, enumeradas según el orden de prioridad:

- El parámetro `IniFile` en la URL de conexión o en el cuadro de diálogo de propiedades de conexión del cliente SQL. Asegúrese de que el parámetro `IniFile` contenga la ruta completa al archivo .ini, incluido el nombre de este. Para obtener información acerca del parámetro `IniFile`, consulte IniFile. Si el parámetro `IniFile` no especifica de manera correcta la ubicación del archivo .ini, se mostrará un error.
- Variables de entorno como AMAZON_REDSHIFT_JDBC_INI_FILE con la ruta completa, incluido el nombre del archivo. Puede utilizar `rsjdbc.ini` o especificar un nombre de archivo. Si la variable de entorno AMAZON_REDSHIFT_JDBC_INI_FILE no especifica de manera correcta la ubicación del archivo .ini, se mostrará un error.
- Directorio donde se encuentra el archivo JAR del controlador.
- Directorio de inicio del usuario.
- Directorio temporal del sistema.

Puede organizar el archivo .ini en secciones; por ejemplo, [DRIVER]. Cada una de las secciones contiene pares de valor de clave que especifican varios parámetros de conexión. Puede utilizar el parámetro `IniSection` para especificar una sección en el archivo .ini. Para obtener información acerca del parámetro `IniSection`, consulte IniSection.

A continuación, se muestra un ejemplo del formato del archivo .ini, con secciones para [DRIVER], [DEV], [QA] y [PROD]. La sección [DRIVER] puede aplicarse a cualquier conexión.

```
[DRIVER]
key1=val1
key2=val2
```

```
[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
key1=val1
key2=val2
```

El controlador JDBC versión 2.1 carga los parámetros de configuración desde las siguientes ubicaciones, enumeradas según el orden de prioridad:

- parámetros de configuración predeterminados en el código de la aplicación
- propiedades de la sección [DRIVER] del archivo .ini, en caso de estar incluidas
- parámetros de configuración de la sección personalizada, siempre que la opción `IniSection` se proporcione en la URL de conexión o en el cuadro de diálogo de propiedades de la conexión del cliente SQL
- propiedades del objeto de propiedad de conexión especificado en la llamada a `getConnection`
- parámetros de configuración especificados en la URL de conexión

Opciones de configuración del controlador JDBC versión 2.1

A continuación, puede encontrar descripciones relativas a las opciones que puede especificar para la versión 2.1 del controlador JDBC de Amazon Redshift. Las opciones de configuración no distinguen entre mayúsculas y minúsculas.

Puede establecer las propiedades de configuración mediante la URL de conexión. Para obtener más información, consulte Creación de la URL de conexión.

Temas

- AccessKeyID
- AllowDBUserOverride
- App_ID
- App_Name

- ApplicationName
- AuthProfile
- AutoCreate
- Client_ID
- Client_Secret
- ID del clúster
- Compresión
- connectTimeout
- connectionTimezone
- databaseMetadataCurrentDbOnly
- DbUser
- DbGroups
- DBNAME
- defaultRowFetchSize
- DisableIsValidQuery
- enableFetchRingBuffer
- enableMultiSqlSupport
- fetchRingBufferSize
- ForceLowercase
- groupFederation
- HOST
- IAMDisableCache
- IAMDuration
- Identity_Namespace
- IdP_Host
- IdP_Port
- IdP_Tenant
- IdP_Response_Timeout
- IniFile

- IniSection
- isServerless
- Login_URL
- loginTimeout
- loginToRp
- LogLevel
- LogPath
- OverrideSchemaPatternType
- Partner_SPID
- Password
- Plugin_Name
- PORT
- Preferred_Role
- Perfil
- PWD
- queryGroup
- readOnly
- Región
- reWriteBatchedInserts
- reWriteBatchedInsertsSize
- roleArn
- roleSessionName
- scope
- SecretAccessKey
- SessionToken
- serverlessAcctId
- serverlessWorkGroup
- socketFactory
- socketTimeout
- SSL

- SSL_Insecure
- SSLCert
- SSLFactory
- SSLKey
- SSLMode
- SSLPassword
- SSLRootCert
- StsEndpointUrl
- tcpKeepAlive
- UID
- Usuario
- webIdentityToken

AccessKeyID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Puede especificar este parámetro para ingresar la clave de acceso de IAM correspondiente al usuario o rol. Por lo general, puede localizar la clave si busca en una cadena o en un perfil de usuario existente. Si especifica este parámetro, también debe especificar el parámetro `SecretAccessKey`. Si se pasa en la URL de JDBC, AccessKeyID debe estar codificado en URL.

Este parámetro es opcional.

AllowDBUserOverride

- Valor predeterminado: 0
- Tipo de datos: cadena

Esta opción especifica si el controlador utiliza el valor `DbUser` de la aserción SAML o el valor que se especifica en la propiedad de conexión `DbUser` en la URL de conexión.

Este parámetro es opcional.

1

El controlador utiliza el valor `DbUser` de la aserción SAML.

Si la aserción SAML no especifica un valor para `DBUser`, el controlador utiliza el valor especificado en la propiedad de conexión `DBUser`. Si la propiedad de conexión no especifica un valor, el controlador utiliza el valor especificado en el perfil de conexión.

0

El controlador utiliza el valor `DBUser` especificado en la propiedad de conexión `DBUser`.

Si la propiedad de conexión `DBUser` no especifica un valor, el controlador utiliza el valor especificado en el perfil de conexión. Además, si el perfil de conexión no especifica un valor, el controlador utiliza el valor de la aserción SAML.

App_ID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID único proporcionado por Okta que se asocia a su aplicación de Amazon Redshift.

Este parámetro es necesario si la autenticación se realiza a través del servicio de Okta.

App_Name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de la aplicación Okta que utiliza en la autenticación de la conexión con Amazon Redshift.

Este parámetro es opcional.

ApplicationName

- Valor predeterminado: nulo
- Tipo de datos: cadena

Nombre de la aplicación que se va a pasar a Amazon Redshift con fines de auditoría.

Este parámetro es opcional.

AuthProfile

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del perfil de autenticación que se utilizará para conectarse a Amazon Redshift.

Este parámetro es opcional.

AutoCreate

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si el controlador logra que se cree un nuevo usuario cuando el usuario especificado no existe.

Este parámetro es opcional.

true

Si el usuario especificado por `DBUser` o ID único (UID) no existe, se crea un nuevo usuario con ese nombre.

false

El controlador no logra que se creen nuevos usuarios. Si el usuario especificado no existe, se produce un error en la autenticación.

Client_ID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de cliente que se utilizará al autenticar la conexión mediante el servicio Azure AD.

Este parámetro es necesario si la autenticación se realiza a través del servicio Azure AD.

Client_Secret

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El secreto del cliente que se utilizará al autenticar la conexión mediante el servicio Azure AD.

Este parámetro es necesario si la autenticación se realiza a través del servicio Azure AD.

ID del clúster

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del clúster de Amazon Redshift al que desea conectarse. El controlador intenta detectar este parámetro desde el host dado. Si utiliza un equilibrador de carga de red (NLB) y se conecta a través de IAM, el controlador no lo detectará, por lo que puede configurarlo con esta opción de conexión.

Este parámetro es opcional.

Compresión

- Valor predeterminado: desconectado
- Tipo de datos: cadena

Método de compresión utilizado para la comunicación mediante protocolo de conexión entre el servidor de Amazon Redshift y el cliente o el controlador.

Este parámetro es opcional.

Puede especificar los valores siguientes:

- lz4

  Establece el método de compresión utilizado para la comunicación mediante protocolo de conexión con Amazon Redshift a lz4.
- off

No utiliza la compresión para la comunicación mediante protocolo de conexión con Amazon Redshift.

connectTimeout

- Valor predeterminado: 10
- Tipo de datos: entero

Valor de tiempo de espera que se utilizará para las operaciones de conexión de socket. Si el tiempo necesario para establecer una conexión de Amazon Redshift supera este valor, se considera que la conexión no está disponible. El tiempo de espera se especifica en segundos. Un valor de 0 indica que no se especifica ningún tiempo de espera.

Este parámetro es opcional.

connectionTimezone

- Valor predeterminado: LOCAL
- Tipo de datos: cadena

Zona horaria en el nivel de sesión.

Este parámetro es opcional.

Puede especificar los valores siguientes:

LOCAL

Configura la zona horaria en el nivel de sesión en la zona horaria de la JVM LOCAL.

SERVER

Configura la zona horaria en el nivel de sesión en la zona horaria establecida para el usuario en el servidor de Amazon Redshift. Puede configurar las zonas horarias en el nivel de sesión para los usuarios con el siguiente comando:

```
ALTER USER
[...]
SET TIMEZONE TO [...];
```

databaseMetadataCurrentDbOnly

- Valor predeterminado: true
- Tipos de datos: booleano

Esta opción especifica si la API de metadatos recupera datos de todas las bases de datos accesibles o únicamente de la base de datos que está conectada.

Este parámetro es opcional.

Puede especificar los valores siguientes:

true

La aplicación recupera los metadatos de una base de datos única.

false

La aplicación recupera los metadatos de todas las bases de datos a las que se puede acceder.

DbUser

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de usuario que se utilizará con su cuenta de Amazon Redshift. Puede utilizar un ID que no exista actualmente si ha habilitado la propiedad AutoCreate.

Este parámetro es opcional.

DbGroups

- Valor predeterminado: PUBLIC
- Tipo de datos: cadena

Una lista separada por comas de los nombres de grupos de bases de datos existentes que `DBUser` une para la sesión actual.

Este parámetro es opcional.

DBNAME

- Valor predeterminado: nulo
- Tipo de datos: cadena

Nombre de la base de datos a la que se va a conectar. Puede utilizar esta opción para especificar el nombre de la base de datos en la URL de conexión de JDBC.

Este parámetro es obligatorio. Debe especificar el nombre de la base de datos, ya sea en la URL de conexión o en las propiedades de conexión de la aplicación cliente.

defaultRowFetchSize

- Valor predeterminado: 0
- Tipo de datos: entero

Esta opción especifica un valor predeterminado para getFetchSize.

Este parámetro es opcional.

Puede especificar los valores siguientes:

0

Recupere todas las filas en una sola operación.

Entero positivo

Número de filas que se recuperan de la base de datos en cada una de las iteraciones de recuperación de ResultSet.

DisableIsValidQuery

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si el controlador envía una nueva consulta a la base de datos cuando se utiliza el método Connection.isValid() para determinar si la conexión a la base de datos se encuentra activa.

Este parámetro es opcional.

true

El controlador no envía una consulta cuando se utiliza el método Connection.isValid() para determinar si la conexión a la base de datos se encuentra activa. Con ello, es posible que el controlador identifique de manera incorrecta la conexión a la base de datos como activa en caso de que el servidor de la base de datos se haya apagado inesperadamente.

false

El controlador envía una consulta cuando se utiliza el método Connection.isValid() para determinar si la conexión a la base de datos se encuentra activa.

enableFetchRingBuffer

- Valor predeterminado: true
- Tipos de datos: booleano

Esta opción especifica que el controlador recupera las filas mediante un búfer de anillo en un subproceso separado. El parámetro fetchRingBufferSize determina el tamaño del búfer de anillo.

Si una transacción detecta una instrucción que contiene varios comandos SQL separados por punto y coma, el búfer del anillo de recuperación de esa transacción se establece en falso. El valor de enableFetchRingBuffer no cambia.

Este parámetro es opcional.

enableMultiSqlSupport

- Valor predeterminado: true
- Tipos de datos: booleano

Esta opción especifica si se deben procesar varios comandos SQL separados por punto y coma en una instrucción.

Este parámetro es opcional.

Puede especificar los valores siguientes:

true

El controlador procesa varios comandos SQL, separados por punto y coma, en un objeto Statement.

false

El controlador devuelve un error en caso de varios comandos SQL en un mismo Statement.

fetchRingBufferSize

- Valor predeterminado: 1G
- Tipo de datos: cadena

Esta opción especifica el tamaño del búfer de anillo utilizado mientras se recupera el conjunto de resultados. Puede especificar un tamaño expresado en bytes; por ejemplo, 1K para 1 KB, 5000 para 5000 bytes, 1M para 1 MB, 1G para 1 GB, etc. También puede especificar un porcentaje de memoria heap. El controlador deja de recuperar filas una vez que alcanza el límite establecido. La recuperación se reanuda en el momento en que la aplicación hace una lectura de las filas y libera espacio en el búfer de anillo.

Este parámetro es opcional.

ForceLowercase

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si el controlador escribe en minúsculas todos los grupos de bases de datos (DbGroups) que se envían desde el proveedor de identidad a Amazon Redshift cuando se utiliza la autenticación de inicio de sesión único.

Este parámetro es opcional.

true

El controlador escribe en minúsculas todos los grupos de bases de datos que se envían desde el proveedor de identidad.

false

El controlador no modifica los grupos de la base de datos.

groupFederation

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si se utilizarán grupos de IDP de Amazon Redshift. Esto es compatible con la API GetClusterCredentialSV2.

Este parámetro es opcional.

true

Utilice grupos de proveedores de identidad (IDP) de Amazon Redshift.

false

Utilice la API STS y GetClusterCredentials para la federación de usuarios y especifique explícitamente DbGroups para la conexión.

HOST

- Valor predeterminado: nulo
- Tipo de datos: cadena

El nombre del host del servidor de Amazon Redshift al que va a conectarse. Puede utilizar esta opción para especificar el nombre de host en la URL de conexión de JDBC.

Este parámetro es obligatorio. Debe especificar el nombre de host, ya sea en la URL de conexión o en las propiedades de conexión de la aplicación cliente.

IAMDisableCache

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si las credenciales de IAM se almacenan en caché.

Este parámetro es opcional.

true

Las credenciales de IAM no se almacenan en caché.

false

Las credenciales de IAM se almacenan en caché. De este modo, se mejora el rendimiento en los casos en que, por ejemplo, las solicitudes a API Gateway tienen limitación controlada.

IAMDuration

- Valor predeterminado: 900
- Tipo de datos: entero

El tiempo, en segundos, hasta que se vencen las credenciales temporales de IAM.

- Valor mínimo: 900
- Valor máximo: 3600

Este parámetro es opcional.

Identity_Namespace

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Espacio de nombres de identidades que se utiliza al autenticarse con IdpTokenAuthPlugin. Ayuda a Redshift a determinar qué instancia de IAM Identity Center utilizar.

Si solo hay una instancia del IAM Identity Center o si se ha establecido el espacio de nombres de identidad predeterminado, este parámetro es opcional; de lo contrario, es obligatorio.

IdP_Host

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El alojamiento del IdP (proveedor de identidad) que utiliza para la autenticación en Amazon Redshift. Esto puede especificarse tanto en la cadena de conexión como en un perfil.

Este parámetro es opcional.

IdP_Port

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El puerto usado por un IdP (proveedor de identidad). Se puede especificar el puerto en la cadena de conexión o en un perfil. El puerto predeterminado es 5439. Según el puerto que haya seleccionado al crear, modificar o migrar el clúster, se permitirá el acceso al puerto seleccionado.

Este parámetro es opcional.

IdP_Tenant

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de inquilino de Azure AD para su aplicación de Amazon Redshift.

Este parámetro es necesario si la autenticación se realiza a través del servicio Azure AD.

IdP_Response_Timeout

- Valor predeterminado: 120
- Tipo de datos: entero

La cantidad de tiempo, en segundos, que espera el controlador en obtener la respuesta SAML del proveedor de identidad cuando se utilizan los servicios Azure AD o SAML a través de un complemento del navegador.

Este parámetro es opcional.

IniFile

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La ruta completa del archivo .ini, incluido el nombre del archivo. Por ejemplo:

```
IniFile="C:\tools\rsjdbc.ini"
```

Para obtener más información acerca del archivo .ini, consulte Creación de archivos de inicialización (.ini) para el controlador JDBC versión 2.1.

Este parámetro es opcional.

IniSection

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de una sección del archivo .ini que contiene las opciones de configuración. Para obtener más información acerca del archivo .ini, consulte Creación de archivos de inicialización (.ini) para el controlador JDBC versión 2.1.

En el siguiente ejemplo, se especifica la sección [Prod] del archivo .ini:

```
IniSection="Prod"
```

Este parámetro es opcional.

isServerless

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si el host de punto de conexión de Amazon Redshift es una instancia sin servidor. El controlador intenta detectar este parámetro desde el host dado. Si utiliza un equilibrador de carga de red (NLB), el controlador no lo detectará, por lo que puede configurarlo aquí.

Este parámetro es opcional.

true

El host de punto de conexión de Amazon Redshift es una instancia sin servidor.

false

El host de punto de conexión de Amazon Redshift es un clúster aprovisionado.

Login_URL

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La dirección URL del recurso en el sitio web del proveedor de identidad en caso de que se utilicen los servicios Azure AD o SAML a través de un complemento del navegador.

Este parámetro es necesario si la autenticación se realiza con el servicio Azure AD o SAML a través de un complemento del navegador.

loginTimeout

- Valor predeterminado: 0
- Tipo de datos: entero

La cantidad de segundos que se debe esperar antes de que se agote el tiempo de espera cuando se conecta y se realiza la autenticación correspondiente al servidor. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión.

Cuando esta propiedad se establece en 0, las conexiones no agotan el tiempo de espera.

Este parámetro es opcional.

loginToRp

- Valor predeterminado: `urn:amazon:webservices`
- Tipo de datos: cadena

La relación de confianza para usuario autenticado que desea utilizar para el tipo de autenticación de AD FS.

Este parámetro es opcional.

LogLevel

- Valor predeterminado: 0
- Tipo de datos: entero

Utilice esta propiedad para activar o desactivar el registro en el controlador y especificar la cantidad de detalles incluidos en los archivos de registros.

Habilite el registro solo durante el tiempo suficiente para detectar un problema. El registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Este parámetro es opcional.

Establezca el parámetro en uno de los siguientes valores:

0

Desactive todos los registros.

1

Habilite el registro en el nivel FATAL, en el que se registran eventos de errores muy graves que harán que el controlador se anule.

2

Habilite el registro en el nivel ERROR, en el que se registran eventos de errores que aún podrían permitir que el controlador siga ejecutándose.

3

Habilite el registro en el nivel WARNING, en el que se registran los eventos que podrían dar lugar a un error si no se toman medidas al respecto.

4

Habilite el registro en el nivel INFO, en el que se registra la información general que describe el progreso del controlador.

5

Habilite el registro en el nivel DEBUG, en el que se registra información detallada que resulta de gran utilidad para la depuración del controlador.

6

Habilite el registro en el nivel TRACE, en el que se registra toda la actividad del controlador.

Cuando se habilita el registro, el controlador crea los siguientes archivos de registro en la ubicación que se especifica en la propiedad `LogPath`:

- **`redshift_jdbc.log`**: archivo que registra la actividad del controlador que no es específica de una conexión.
- **`redshift_jdbc_connection_[Number].log`**: archivo para cada conexión que se realiza a la base de datos, en el que `[Number]` es un número que permite la distinción de cada archivo de registro respecto a los demás. Este archivo registra la actividad del controlador específica de la conexión.

Si el valor de LogPath no es válido, el controlador envía la información registrada a la secuencia de salida estándar, `System.out`.

LogPath

- Valor predeterminado: el directorio de trabajo actual.
- Tipo de datos: cadena

La ruta completa a la carpeta en la que el controlador guarda los archivos de registros cuando la propiedad DSILogLevel está habilitada.

Para asegurarse de que la URL de conexión es compatible con todas las aplicaciones JDBC, se recomienda que evite las barras diagonales invertidas (\) en la ruta del archivo y escriba una nueva.

Este parámetro es opcional.

OverrideSchemaPatternType

- Valor predeterminado: nulo
- Tipo de datos: entero

Esta opción especifica si invalidar el tipo de consulta usada en las llamadas a getTables.

0

Consulta universal sin esquema

1

Consulta de esquema local

2

Consulta de esquema externo

Este parámetro es opcional.

Partner_SPID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El valor del SPID (ID del proveedor de servicios) del socio que se utilizará cuando se autentique la conexión mediante el servicio PingFederate.

Este parámetro es opcional.

Password

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Cuando se conecta con la autenticación de IAM a través de un IDP, esta es la contraseña para el servidor IDP_Host. Cuando se utiliza la autenticación estándar, se puede utilizar esta opción como contraseña de la base de datos de Amazon Redshift en lugar de PWD.

Este parámetro es opcional.

Plugin_Name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de la clase completamente calificado que implementa un complemento de proveedor de credenciales específico.

Este parámetro es opcional.

Se admiten las siguientes opciones de proveedores:

- **`AdfsCredentialsProvider`**: Active Directory Federation Service
- **`AzureCredentialsProvider`**: servicio de Microsoft Azure Active Directory (AD)
- **`BasicJwtCredentialsProvider`**: servicio de JSON Web Tokens (JWT)
- **`BasicSamlCredentialsProvider`**: credenciales de lenguaje de marcado de aserción de seguridad (SAML) que puede utilizar con muchos proveedores de servicios de SAML.
- **`BrowserAzureCredentialsProvider`**: servicio del navegador de Microsoft Azure Active Directory (AD)
- **`BrowserAzureOAuth2CredentialsProvider`**: servicio del navegador de Microsoft Azure Active Directory (AD) para la autenticación nativa
- **`BrowserSamlCredentialsProvider`**: navegador SAML para servicios de SAML, tales como Okta, Ping o ADFS
- **`IdpTokenAuthPlugin`**: complemento de autorización que acepta un token de Identity Center (IdC) o token de identidad basados en JSON (JWT) de OpenID Connect (OIDC) de cualquier proveedor de identidad web vinculado al IdC.
- **`OktaCredentialsProvider`**: servicio de Okta
- **`PingCredentialsProvider`**: servicio de PingFederate

PORT

- Valor predeterminado: nulo
- Tipo de datos: entero

El puerto del servidor de Amazon Redshift al que va a conectarse. Puede utilizar esta opción para especificar el puerto en la URL de conexión de JDBC.

Este parámetro es opcional.

Preferred_Role

- Valor predeterminado: ninguno

- Tipo de datos: cadena

El rol de IAM que desea asumir durante la conexión a Amazon Redshift.

Este parámetro es opcional.

Perfil

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del perfil que utilizará para la autenticación de IAM. Este perfil contiene cualquier propiedad de conexión adicional que no se haya especificado en la cadena de conexión.

Este parámetro es opcional.

PWD

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La contraseña correspondiente al nombre de usuario de Amazon Redshift que proporcionó mediante la propiedad UID.

Este parámetro es opcional.

queryGroup

- Valor predeterminado: nulo
- Tipo de datos: cadena

Esta opción permite asignar una consulta a una cola en tiempo de ejecución al asignar la consulta al grupo de consultas adecuado. El grupo de consultas se establece para la sesión. Todas las consultas que se ejecutan en la conexión corresponden a este grupo de consultas.

Este parámetro es opcional.

readOnly

- Valor predeterminado: false

- Tipos de datos: booleano

Esta propiedad determina si el controlador se encuentra en modo de solo lectura.

Este parámetro es opcional.

true

La conexión se encuentra en modo de solo lectura y no se puede escribir en el almacén de datos.

false

La conexión se encuentra en modo de solo lectura y se puede escribir en el almacén de datos.

Región

- Valor predeterminado: nulo
- Tipo de datos: cadena

Esta opción especifica la región de AWS en la que está ubicado el clúster. Si especifica la opción StsEndPoint, se omitirá la opción Region. La operación de la API `GetClusterCredentials` de Redshift también utiliza la opción Region.

Este parámetro es opcional.

reWriteBatchedInserts

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción permite optimizar la reescritura y la combinación de instrucciones INSERT compatibles en lotes.

Este parámetro es opcional.

reWriteBatchedInsertsSize

- Valor predeterminado: 128
- Tipo de datos: entero

Esta opción permite optimizar la reescritura y la combinación de instrucciones INSERT compatibles en lotes. Este valor debe aumentar a nivel exponencial por la potencia de 2.

Este parámetro es opcional.

roleArn

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de recurso de Amazon (ARN) del rol. Asegúrese de indicar este parámetro cada vez que especifique BasicJwtCredentialsProvider para la opción Plugin_Name. Especifique el ARN en el siguiente formato:

`arn:partition:service:region:account-id:resource-id`

Este parámetro es necesario siempre que se especifique BasicJwtCredentialsProvider para la opción Plugin_Name.

roleSessionName

- Valor predeterminado: jwt_redshift_session
- Tipo de datos: cadena

Un identificador para la sesión del rol asumido. Por lo general, se pasa el nombre o el identificador que se asocia con el usuario de su aplicación. Las credenciales de seguridad temporales que utiliza su aplicación se asocian a ese usuario. Puede indicar este parámetro cada vez que especifique BasicJwtCredentialsProvider para la opción Plugin_Name.

Este parámetro es opcional.

scope

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Una lista separada por espacios de los ámbitos a los que el usuario puede dar su consentimiento. Especifique este parámetro para que su aplicación de Microsoft Azure pueda obtener el

consentimiento para las API a las que desee llamar. Puede especificar este parámetro cuando indique BrowserAzureOAuth2CredentialsProvider para la opción Plugin_Name.

Este parámetro es necesario para el complemento BrowserAzureOAuth2CredentialsProvider.

SecretAccessKey

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave de acceso de IAM para el usuario o el rol. Si esto se especifica, entonces también se debe especificar AccessKeyID. Si se pasa en la URL de JDBC, SecretAccessKey debe estar codificado en URL.

Este parámetro es opcional.

SessionToken

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El token de sesión temporal de IAM asociado con el rol de IAM que se está utilizando para la autenticación. Si se pasa en la URL de JDBC, el token de sesión de IAM temporal debe estar codificado en URL.

Este parámetro es opcional.

serverlessAcctId

- Valor predeterminado: nulo
- Tipo de datos: cadena

El ID de la cuenta de Amazon Redshift sin servidor. El controlador intenta detectar este parámetro desde el host dado. Si utiliza un equilibrador de carga de red (NLB), el controlador no lo detectará, por lo que puede configurarlo aquí.

Este parámetro es opcional.

serverlessWorkGroup

- Valor predeterminado: nulo
- Tipo de datos: cadena

El nombre del grupo de trabajo de Amazon Redshift sin servidor. El controlador intenta detectar este parámetro desde el host dado. Si utiliza un equilibrador de carga de red (NLB), el controlador no lo detectará, por lo que puede configurarlo aquí.

Este parámetro es opcional.

socketFactory

- Valor predeterminado: nulo
- Tipo de datos: cadena

Esta opción especifica una fábrica de sockets para la creación de sockets.

Este parámetro es opcional.

socketTimeout

- Valor predeterminado: 0
- Tipo de datos: entero

La cantidad de segundos que se debe esperar durante las operaciones de lectura del conector antes de que se agote el tiempo de espera. Si una operación dura más tiempo que este límite, se cierra la conexión. Cuando esta propiedad se establece en 0, la conexión no agota el tiempo de espera.

Este parámetro es opcional.

SSL

- Valor predeterminado: TRUE
- Tipo de datos: cadena

Utilice esta propiedad para activar o desactivar SSL para la conexión.

Este parámetro es opcional.

Puede especificar los valores siguientes:

TRUE

El controlador se conecta al servidor a través de SSL.

FALSE

El controlador se conecta al servidor sin utilizar SSL. Esta opción no es compatible con la autenticación de IAM.

Como alternativa, puede configurar la propiedad AuthMech.

SSL_Insecure

- Valor predeterminado: true
- Tipo de datos: cadena

Esta propiedad indica si se debe verificar el certificado de servidor de alojamientos de IDP.

Este parámetro es opcional.

Puede especificar los valores siguientes:

true

El controlador no verifica la autenticidad del certificado del servidor IDP.

false

El controlador verifica la autenticidad del certificado del servidor IDP.

SSLCert

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La ruta completa de un archivo .pem o .crt que contiene certificados de entidad de certificación de confianza adicionales destinados a verificar la instancia de servidor de Amazon Redshift cuando se utiliza SSL.

Este parámetro es obligatorio si se especifica SSLKey.

SSLFactory

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La fábrica SSL que se utilizará cuando se conecte al servidor a través de TLS o SSL sin emplear un certificado de servidor.

SSLKey

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La ruta completa del archivo .der que contiene el archivo de claves PKCS8 destinado a verificar los certificados especificados en SSLCert.

Este parámetro no es obligatorio si se especifica SSLCert.

SSLMode

- Valor predeterminado: verify-ca
- Tipo de datos: cadena

Utilice esta propiedad para especificar la forma en que el controlador valida los certificados cuando TLS o SSL está habilitado.

Este parámetro es opcional.

Puede especificar los valores siguientes:

verify-ca

El controlador verifica que el certificado proviene de una entidad de certificación (CA) de confianza.

verify-full

El controlador verifica que el certificado proviene de una entidad de certificación de confianza y que el nombre de alojamiento del certificado concuerda con el nombre de alojamiento especificado en la URL de conexión.

SSLPassword

- Valor predeterminado: 0
- Tipo de datos: cadena

La contraseña para el archivo de clave cifrado que se especifica en SSLKey.

Se requiere este parámetro si se especifica SSLKey y si se cifra el archivo clave.

SSLRootCert

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La ruta completa de un archivo .pem o .crt que contiene el certificado de entidad de certificación raíz que permite verificar la instancia de servidor de Amazon Redshift cuando se utiliza SSL.

StsEndpointUrl

- Valor predeterminado: nulo
- Tipo de datos: cadena

Puede especificar un punto de conexión AWS Security Token Service (AWS STS). Si especifica la opción, se omitirá la opción Region. Solo puede especificar un protocolo seguro (HTTPS) para este punto de conexión.

tcpKeepAlive

- Valor predeterminado: TRUE
- Tipo de datos: cadena

Utilice esta propiedad para activar o desactivar keepalives de TCP.

Este parámetro es opcional.

Puede especificar los valores siguientes:

TRUE

El controlador utiliza keepalives de TCP para evitar que se agote el tiempo de espera en las conexiones.

FALSE

El controlador no utiliza keepalives de TCP.

UID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de usuario de base de datos que utiliza para obtener acceso a la base de datos.

Este parámetro es obligatorio.

Usuario

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Cuando se conecta mediante la autenticación de IAM a través de un IDP, este es el nombre de usuario que corresponde al servidor idp_host. Si se utiliza la autenticación estándar, se puede utilizar esta opción como nombre de usuario de la base de datos de Amazon Redshift.

Este parámetro es opcional.

webIdentityToken

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El token de acceso de OAuth 2.1 o el token del ID de OpenID Connect proporcionado por el proveedor de identidad. Su aplicación debe obtener este token mediante la autenticación del usuario

de su aplicación con un proveedor de identidad web. Asegúrese de indicar este parámetro cada vez que especifique BasicJwtCredentialsProvider para la opción Plugin_Name.

Este parámetro es necesario siempre que se especifique BasicJwtCredentialsProvider para la opción Plugin_Name.

Versiones anteriores del controlador JDBC versión 2.1

Descargue una versión anterior del controlador JDBC versión 2.1 de Amazon Redshift solo si su herramienta requiere una versión específica del controlador.

Estos son los controladores JDBC versión 2.1 que admiten los anteriores JDBC 4.2:

- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.25/redshift-jdbc42-2.1.0.25.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.24/redshift-jdbc42-2.1.0.24.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.23/redshift-jdbc42-2.1.0.23.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.22/redshift-jdbc42-2.1.0.22.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.21/redshift-jdbc42-2.1.0.21.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.20/redshift-jdbc42-2.1.0.20.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.19/redshift-jdbc42-2.1.0.19.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.18/redshift-jdbc42-2.1.0.18.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.17/redshift-jdbc42-2.1.0.17.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.16/redshift-jdbc42-2.1.0.16.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.15/redshift-jdbc42-2.1.0.15.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.14/redshift-jdbc42-2.1.0.14.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.13/redshift-jdbc42-2.1.0.13.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.12/redshift-jdbc42-2.1.0.12.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.11/redshift-jdbc42-2.1.0.11.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.10/redshift-jdbc42-2.1.0.10.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.9/redshift-jdbc42-2.1.0.9.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.8/redshift-jdbc42-2.1.0.8.zip
- https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.7/redshift-jdbc42-2.1.0.7.zip

Configuración del conector Python de Amazon Redshift

Mediante el conector de Amazon Redshift para Python, puede integrar el trabajo al AWS SDK para Python (Boto3), y también pandas y Python numérico (NumPy). Para obtener más información sobre pandas, consulte el repositorio de GitHub de pandas. Para obtener más información sobre NumPy, consulte el repositorio de GitHub de NumPy.

El conector Python de Amazon Redshift proporciona una solución de código abierto. Puede examinar el código fuente, solicitar mejoras, informar problemas y realizar aportaciones.

Para utilizar el conector Python de Amazon Redshift, asegúrese de tener Python versión 3.6 o posterior. Para obtener más información, consulte el acuerdo de licencia del controlador Python de Amazon Redshift.

El conector Python de Amazon Redshift proporciona lo siguiente:

- Authentication de AWS Identity and Access Management (IAM). Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.
- Autenticación de proveedores de identidad mediante acceso a API federado. El acceso a la API federado admite proveedores de identidad corporativa, como los siguientes:
  - Azure AD. Para obtener más información, consulte la entrada del blog de Big Data de AWS Federate Amazon Redshift access with Microsoft Azure AD single sign-on.
  - Active Directory Federation Services. Para obtener más información, consulte la entrada del blog de Big Data de AWS Federate access to your Amazon Redshift cluster with Active Directory Federation Services (AD FS): Part 1.
  - Okta. Para obtener más información, consulte la entrada del blog de Big Data de AWS Federate Amazon Redshift access with Okta as an identity provider.
  - PingFederate. Para obtener más información, consulte el sitio de PingFederate.
  - JumpCloud. Para obtener más información, cpnsulte el sitio de JumpCloud.
- Tipos de datos de Amazon Redshift

El conector Python de Amazon Redshift implementa la especificación 2.0 de la API de base de datos de Python. Para obtener más información, consulte PEP 249—Python Database API Specification v2.0 en el sitio web de Python.

Temas

- Instalación del conector Python de Amazon Redshift

- Opciones de configuración para el conector Python de Amazon Redshift
- Importación del conector Python
- Integración del conector Python a NumPy
- Integración del conector Python a pandas
- Uso de complementos de proveedores de identidades
- Ejemplos de uso del conector Python de Amazon Redshift
- Referencia de la API para el conector Python de Amazon Redshift

Instalación del conector Python de Amazon Redshift

Puede utilizar cualquiera de los siguientes métodos para instalar el conector Python de Amazon Redshift:

- Índice de paquetes de Python (PyPI)
- Conda
- Clonación del repositorio de GitHub

Instalación del conector Python desde PyPI

Para instalar el conector Python desde el Índice de paquetes de Python (PyPI), puede utilizar pip. Para ello, ejecute el siguiente comando.

```
>>> pip install redshift_connector
```

Puede instalar el conector en un entorno virtual. Para ello, ejecute el siguiente comando.

```
>>> pip install redshift_connector
```

Opcionalmente, puede instalar pandas y NumPy con el conector.

```
>>> pip install "redshift_connector[full]"
```

Para obtener más información sobre pip, consulte el sitio de pip.

Instalación del conector Python desde Conda

Puede instalar el conector Python desde Anaconda.org.

```
>>>conda install -c conda-forge redshift_connector
```

Instalación del conector Python mediante la clonación del repositorio de GitHub desde AWS

Para instalar el conector Python desde el origen, clone el repositorio GitHub desde AWS. Después de instalar Python y virtualenv, configure su entorno e instale las dependencias necesarias mediante la ejecución de los siguientes comandos.

```
$ git clone https://github.com/aws/amazon-redshift-python-driver.git
$ cd RedshiftPythonDriver
$ virtualenv venv
$ . venv/bin/activate
$ python -m pip install -r requirements.txt
$ python -m pip install -e .
$ python -m pip install redshift_connector
```

Opciones de configuración para el conector Python de Amazon Redshift

A continuación, puede encontrar descripciones relativas a las opciones que puede especificar para el conector Python de Amazon Redshift.

access_key_id

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave de acceso del rol o usuario de IAM configurado para la autenticación de la base de datos de IAM.

Este parámetro es opcional.

allow_db_user_override

- Valor predeterminado: false
- Tipos de datos: booleano

True

Especifica que el conector utiliza el valor `DbUser` de la aserción del lenguaje de marcado de aserción de seguridad (SAML).

False

Especifica que se utiliza el valor del parámetro de conexión `DbUser`.

Este parámetro es opcional.

app_name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de la aplicación de proveedor de identidades (IdP) utilizado para la autenticación.

Este parámetro es opcional.

auth_profile

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de un perfil de autenticación de Amazon Redshift que tiene propiedades de conexión como JSON. Para obtener más información sobre cómo asignar nombres a los parámetros de conexión, consulte la clase `RedshiftProperty`. La clase `RedshiftProperty` almacena los parámetros de conexión proporcionados por el usuario final y, si procede, generados durante el proceso de autenticación de IAM (por ejemplo, credenciales de IAM temporales). Para obtener más información, consulte la clase RedshiftProperty.

Este parámetro es opcional.

auto_create

- Valor predeterminado: false
- Tipos de datos: booleano

Un valor que indica si se va a crear el usuario si el usuario no existe.

Este parámetro es opcional.

client_id

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de cliente del IdP de Azure.

Este parámetro es opcional.

client_secret

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El secreto del cliente del IdP de Azure.

Este parámetro es opcional.

cluster_identifier

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El identificador de clúster del clúster de Amazon Redshift.

Este parámetro es opcional.

credentials_provider

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El IdP que se utiliza para la autenticación en Amazon Redshift. Los siguientes valores son válidos:

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`
- `BrowserSamlCredentialsProvider`

- `IdpTokenAuthPlugin`: complemento de autorización que acepta un token de Identity Center (IdC) o token de identidad basados en JSON (JWT) de OpenID Connect (OIDC) de cualquier proveedor de identidad web vinculado al IdC.
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

Este parámetro es opcional.

base de datos

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de la base de datos a la que desea conectarse.

Este parámetro es opcional.

database_metadata_current_db_only

- Valor predeterminado: true
- Tipos de datos: booleano

Un valor que indica si una aplicación admite catálogos de recursos compartidos de datos de varias bases de datos. El valor predeterminado de True indica que la aplicación no admite catálogos de recursos compartidos de datos de varias bases de datos para compatibilidad con versiones anteriores.

Este parámetro es opcional.

db_groups

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Una lista separada por comas de los nombres de grupos de bases de datos existentes que el usuario indicó al unir el DbUser para la sesión actual.

Este parámetro es opcional.

db_user

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de usuario que se utilizará con Amazon Redshift.

Este parámetro es opcional.

endpoint_url

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La URL del punto de conexión de Amazon Redshift. Esta opción es solo para uso interno de AWS.

Este parámetro es obligatorio.

group_federation

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si se utilizarán grupos de IDP de Amazon Redshift.

Este parámetro es opcional.

true

Utilice grupos de proveedores de identidad (IDP) de Amazon Redshift.

false

Utilice la API STS y GetClusterCredentials para la federación de usuarios y especifique db_groups para la conexión.

host

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del host del clúster de Amazon Redshift.

Este parámetro es opcional.

iam

- Valor predeterminado: false
- Tipos de datos: booleano

La autenticación de IAM está habilitada.

Este parámetro es obligatorio.

iam_disable_cache

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si las credenciales de IAM se almacenan en caché. De manera predeterminada, las credenciales de IAM se almacenan en caché. De este modo, se mejora el rendimiento en los casos en que las solicitudes a la API Gateway tienen limitación controlada.

Este parámetro es opcional.

identity_namespace

- Valor predeterminado: null
- Tipo de datos: cadena

Espacio de nombres de identidad que se utiliza al autenticarse con IdpTokenAuthPlugin. Ayuda a Redshift a decidir qué instancia de Identity Center utilizar.

Si solo existe una instancia de Identity Center o si se ha establecido un espacio de nombres de identidad predeterminado, este parámetro es opcional. De lo contrario, es obligatorio.

idpPort

- Valor predeterminado: 7890
- Tipo de datos: entero

El puerto de escucha al que el IdP envía la aserción SAML.

Este parámetro es obligatorio.

Idp_response_timeout

- Valor predeterminado: 120
- Tipo de datos: entero

Tiempo de espera para recuperar la aserción SAML del IdP.

Este parámetro es obligatorio.

idp_tenant

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El inquilino del IdP.

Este parámetro es opcional.

listen_port

- Valor predeterminado: 7890
- Tipo de datos: entero

El puerto de escucha al que el IdP envía la aserción SAML.

Este parámetro es opcional.

login_url

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La URL de inicio de sesión único para el IdP.

Este parámetro es opcional.

max_prepared_statements

- Valor predeterminado: 1000
- Tipo de datos: entero

El número máximo de instrucciones preparadas que se pueden abrir simultáneamente.

Este parámetro es obligatorio.

numeric_to_float

- Valor predeterminado: false
- Tipos de datos: booleano

Esta opción especifica si el conector convierte valores de tipo de datos numéricos de decimal.Decimal a float. De forma predeterminada, el conector recibe valores de tipo de datos numéricos como decimal.Decimal y no los convierte.

No recomendamos habilitar numeric_to_float para casos de uso que requieren precisión, ya que los resultados se pueden redondear.

Para obtener más información sobre decimal.Decimal y las compensaciones entre él y float, consulte decimal — Aritmética decimal de coma fija y coma flotante en el sitio web de Python.

Este parámetro es opcional.

partner_sp_id

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de SP de socio utilizado para la autenticación en Ping.

Este parámetro es opcional.

password

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La contraseña que se utilizará para la autenticación.

Este parámetro es opcional.

port

- Valor predeterminado: 5439
- Tipo de datos: entero

El número de puerto del clúster de Amazon Redshift.

Este parámetro es obligatorio.

preferred_role

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El rol de IAM preferido para la conexión actual.

Este parámetro es opcional.

principal_arn

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de recurso de Amazon (ARN) del usuario o rol de IAM para el que está generando una política. Se recomienda asociar una política a un rol y luego asignar el rol a su usuario, para el acceso.

Este parámetro es opcional.

profile

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de un perfil de en un archivo de credenciales de AWS que contiene credenciales de AWS.

Este parámetro es opcional.

provider_name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del proveedor de autenticación nativo de Redshift.

Este parámetro es opcional.

región

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La Región de AWS donde se encuentra el clúster.

Este parámetro es opcional.

role_arn

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de recurso de Amazon (ARN) del rol que la persona que llama va a tomar. Este parámetro lo utiliza el proveedor indicado por `JwtCredentialsProvider`.

Para el proveedor de `JwtCredentialsProvider`, este parámetro es obligatorio. De lo contrario, este parámetro es opcional.

role_session_name

- Valor predeterminado: jwt_redshift_session
- Tipo de datos: cadena

Un identificador para la sesión del rol asumido. Por lo general, se pasa el nombre o el identificador que se asocia con el usuario que está usando su aplicación. Las credenciales de seguridad

temporales que utiliza su aplicación se asocian a ese usuario. Este parámetro lo utiliza el proveedor indicado por `JwtCredentialsProvider`.

Este parámetro es opcional.

scope

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Una lista separada por espacios de los ámbitos a los que el usuario puede dar su consentimiento. Especifique este parámetro para que su aplicación pueda obtener el consentimiento para las API a las que desee llamar. Puede especificar este parámetro cuando indique BrowserAzureOAuth2CredentialsProvider para la opción Plugin_Name.

Este parámetro es necesario para el complemento BrowserAzureOAuth2CredentialsProvider.

secret_access_key_id

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave de acceso secreta del rol o usuario de IAM configurado para la autenticación de la base de datos de IAM.

Este parámetro es opcional.

session_token

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave de acceso del rol o usuario de IAM configurado para la autenticación de la base de datos de IAM. Este parámetro es obligatorio si se están utilizando credenciales de AWS temporales.

Este parámetro es opcional.

serverless_acct_id

- Valor predeterminado: ninguno

- Tipo de datos: cadena

El ID de la cuenta de Amazon Redshift Serverless.

Este parámetro es opcional.

serverless_work_group

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del grupo de trabajo de Amazon Redshift Serverless.

Este parámetro es opcional.

ssl

- Valor predeterminado: true
- Tipos de datos: booleano

La capa de sockets seguros (SSL) está habilitada.

Este parámetro es obligatorio.

ssl_insecure

- Valor predeterminado: true
- Tipos de datos: booleano

Un valor que especifica si el certificado de servidor de hosts de IdP se debe verificar.

Este parámetro es opcional.

sslmode

- Valor predeterminado: verify-ca
- Tipo de datos: cadena

La seguridad de la conexión a Amazon Redshift. Puede especificar cualquiera de los siguientes:

- verify-ca
- verify-full

Este parámetro es obligatorio.

timeout

- Valor predeterminado: ninguno
- Tipo de datos: entero

La cantidad de segundos antes de que la conexión al servidor se agote.

Este parámetro es opcional.

token

- Valor predeterminado: null
- Tipo de datos: cadena

El token de acceso proporcionado por Identity Center (IdC) o un token de identidad basado en JSON (JWT) de OpenID Connect (OIDC) proporcionado por un proveedor de identidades web que esté vinculado con el IdC. Su aplicación debe generar este token autenticando al usuario de su aplicación con el IdC o un proveedor de identidad web vinculado con el IdC.

Este parámetro solo es obligatorio cuando se autentica con IdpTokenAuthPlugin.

token_type

- Valor predeterminado: null
- Tipo de datos: cadena

Tipo de token que se utiliza en IdpTokenAuthPlugin.

Este parámetro solo es obligatorio cuando se autentica con IdpTokenAuthPlugin.

Puede especificar los valores siguientes:

- `ACCESS_TOKEN`: especifique este valor si utiliza un token de acceso proporcionado por Identity Center (IdC).

- `EXT_JWT`: especifique este valor si utiliza un token de identidad (JWT) basado en JSON (JWT) de OpenID Connect (OIDC) proporcionado por un proveedor de identidad web externo vinculado al IdC.

usuario

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de usuario que se va a utilizar para la autorización.

Este parámetro es opcional.

web_identity_token

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El token de acceso de OAuth 2.0 o el token del ID de OpenID Connect proporcionado por el proveedor de identidad. Asegúrese de que su aplicación obtenga este token mediante la autenticación del usuario que usa la aplicación con un proveedor de identidad web. El proveedor indicado por `JwtCredentialsProvider` utiliza este parámetro.

Para el proveedor de `JwtCredentialsProvider`, este parámetro es obligatorio. De lo contrario, este parámetro es opcional.

Importación del conector Python

Para importar el conector Python, ejecute en siguiente comando.

```
>>> import redshift_connector
```

Importación de NumPy y conexión a Amazon Redshift

Para importar el conector Python de Amazon Redshift y Numerical Python (NumPy), ejecute los siguientes comandos.

```
import redshift_connector
```

```
import numpy
```

Para conectarse a un clúster de Amazon Redshift mediante credenciales de AWS, ejecute el siguiente comando.

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
 )
```

Integración del conector Python a NumPy

A continuación se muestra un ejemplo de integración del conector Python a NumPy.

```
>>>  import numpy
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     port=5439,
     database='dev',
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")

result: numpy.ndarray = cursor.fetch_numpy_array()
print(result)
```

A continuación, se muestra el resultado.

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
['A Brief History of Time' 'Stephen Hawking']]
```

Integración del conector Python a pandas

A continuación se muestra un ejemplo de integración del conector Python a pandas.

```
>>> import pandas

#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     port=5439,
     database='dev',
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")
result: pandas.DataFrame = cursor.fetch_dataframe()
print(result)
```

Uso de complementos de proveedores de identidades

Para obtener información general sobre cómo utilizar los complementos de proveedores de identidades, consulte Opciones para proporcionar credenciales de IAM. Para obtener más información sobre cómo administrar las identidades de IAM, incluidas las prácticas recomendadas para los roles de IAM, consulte Administración de identidades y accesos en Amazon Redshift.

Autenticación mediante el complemento de proveedores de identidades de AD FS

A continuación se muestra un ejemplo del uso del complemento de proveedores de identidades de Servicios de federación de Active Directory (AD FS) para autenticar a un usuario que se conecta a una base de datos de Amazon Redshift.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
```

```
    credentials_provider='AdfsCredentialsProvider',
    user='brooke@myadfshostname.com',
    password='Hunter2',
    idp_host='myadfshostname.com'
)
```

Autenticación mediante el complemento de proveedores de identidades Azure

A continuación se muestra un ejemplo de autenticación mediante el complemento de proveedores de identidades Azure. Puede crear valores para `client_id` y `client_secret` para una aplicación para empresas Azure tal y como se muestra a continuación.

```
>>>  con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AzureCredentialsProvider',
    user='brooke@myazure.org',
    password='Hunter2',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
    client_secret='my_client_secret',
    preferred_role='arn:aws:iam:123:role/DataScientist'
)
```

Autenticación mediante el complemento de proveedores de identidades Azure Browser

A continuación se muestra un ejemplo del uso del complemento de proveedores de identidades Azure Browser para autenticar a un usuario que se conecta a una base de datos de Amazon Redshift.

La autenticación multifactor se produce en el navegador, donde las credenciales de inicio de sesión las proporciona el usuario.

```
>>>con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserAzureCredentialsProvider',
```

```
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
)
```

Autenticación mediante el complemento de proveedores de identidades Okta

A continuación se muestra un ejemplo de autenticación mediante el complemento de proveedores de identidades Okta. Puede obtener los valores de `idp_host`, `app_id` y `app_name` a través de la aplicación Okta.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='OktaCredentialsProvider',
    user='brooke@myazure.org',
    password='hunter2',
    idp_host='my_idp_host',
    app_id='my_first_appetizer',
    app_name='dinner_party'
)
```

Autenticación mediante JumpCloud con un complemento de proveedores de identidades de navegador SAML genérico

A continuación se muestra un ejemplo de autenticación mediante JumpCloud con un complemento de proveedores de identidades de navegador SAML genérico.

La contraseña del parámetro es obligatoria. No obstante, no tiene que ingresar este parámetro porque la autenticación multifactor se produce en el navegador.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserSamlCredentialsProvider',
    user='brooke@myjumpcloud.org',
    password='',
    login_url='https://sso.jumpcloud.com/saml2/plustwo_melody'
```

```
)
```

Ejemplos de uso del conector Python de Amazon Redshift

A continuación se muestran ejemplos de cómo utilizar el conector Python de Amazon Redshift. Para ejecutarlos, primero debe instalar el conector Python. Para obtener más información sobre la instalación del conector Python de Amazon Redshift, consulte Instalación del conector Python de Amazon Redshift. Para obtener más información sobre las opciones de configuración que puede utilizar con el conector Python, consulte Opciones de configuración para el conector Python de Amazon Redshift.

Temas

- Conexión y consulta a un clúster de Amazon Redshift mediante credenciales de AWS
- Habilitación de la confirmación automática
- Configuración del estilo de parámetro del cursor
- Uso de COPY para copiar datos de un bucket de Amazon S3 y UNLOAD para escribirlos en este

Conexión y consulta a un clúster de Amazon Redshift mediante credenciales de AWS

El siguiente ejemplo le guía a través del proceso de conexión a un clúster de Amazon Redshift con sus credenciales de AWS y, a continuación, de consulta de una tabla y de recuperación de los resultados de la consulta.

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
     host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
     database='dev',
     port=5439,
     user='awsuser',
     password='my_password'
  )

# Create a Cursor object
>>> cursor = conn.cursor()

# Query a table using the Cursor
>>> cursor.execute("select * from book")
```

```
#Retrieve the query result set
>>> result: tuple = cursor.fetchall()
>>> print(result)
 >> (['One Hundred Years of Solitude', 'Gabriel García Márquez'], ['A Brief History of
 Time', 'Stephen Hawking'])
```

Habilitación de la confirmación automática

La propiedad de confirmación automática se desactiva de manera predeterminada, de acuerdo con la especificación de la API de base de datos de Python. Puede utilizar los siguientes comandos para activar la propiedad de confirmación automática de la conexión después de ejecutar un comando de reversión para asegurarse de que no haya una transacción en curso.

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(...)

# Run a rollback command
>>>  conn.rollback()

# Turn on autocommit
>>>  conn.autocommit = True
>>>  conn.run("VACUUM")

# Turn off autocommit
>>>  conn.autocommit = False
```

Configuración del estilo de parámetro del cursor

El estilo de parámetro de un cursor se puede modificar mediante cursor.paramstyle. El estilo de parámetro predeterminado que se utiliza es `format`. Los valores válidos del estilo de parámetro son `qmark`, `numeric`, `named`, `format` y `pyformat`.

A continuación, se muestran ejemplos del uso de varios estilos de parámetro para pasar parámetros a una instrucción SQL de ejemplo.

```
# qmark
redshift_connector.paramstyle = 'qmark'
sql = 'insert into foo(bar, jar) VALUES(?, ?)'
cursor.execute(sql, (1, "hello world"))
```

```
# numeric
redshift_connector.paramstyle = 'numeric'
sql = 'insert into foo(bar, jar) VALUES(:1, :2)'
cursor.execute(sql, (1, "hello world"))

# named
redshift_connector.paramstyle = 'named'
sql = 'insert into foo(bar, jar) VALUES(:p1, :p2)'
cursor.execute(sql, {"p1":1, "p2":"hello world"})

# format
redshift_connector.paramstyle = 'format'
sql = 'insert into foo(bar, jar) VALUES(%s, %s)'
cursor.execute(sql, (1, "hello world"))

# pyformat
redshift_connector.paramstyle = 'pyformat'
sql = 'insert into foo(bar, jar) VALUES(%(bar)s, %(jar)s)'
cursor.execute(sql, {"bar": 1, "jar": "hello world"})
```

Uso de COPY para copiar datos de un bucket de Amazon S3 y UNLOAD para escribirlos en este

En el siguiente ejemplo, se muestra cómo copiar datos de un bucket de Amazon S3 en una tabla y luego descargarlos de esa tabla en el bucket.

Un archivo de texto denominado `category_csv.txt` que contiene los siguientes datos se carga en un bucket de Amazon S3.

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

A continuación se muestra un ejemplo del código de Python, que se conecta primero a la base de datos de Amazon Redshift. A continuación crea una tabla llamada `category` y copia los datos CSV del bucket de S3 en la tabla.

```
#Connect to the cluster and create a Cursor
>>> import redshift_connector
>>> with redshift_connector.connect(...) as conn:
>>> with conn.cursor() as cursor:
```

```
#Create an empty table
>>>     cursor.execute("create table category (catid int, cargroup varchar, catname
 varchar, catdesc varchar)")

#Use COPY to copy the contents of the S3 bucket into the empty table
>>>     cursor.execute("copy category from 's3://testing/category_csv.txt' iam_role
 'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the table
>>>     cursor.execute("select * from category")
>>>     print(cursor.fetchall())

#Use UNLOAD to copy the contents of the table into the S3 bucket
>>>     cursor.execute("unload ('select * from category') to 's3://testing/
unloaded_category_csv.txt'  iam_role 'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the bucket
>>>     print(cursor.fetchall())
 >> ([12, 'Shows', 'Musicals', 'Musical theatre'], [13, 'Shows', 'Plays', 'All "non-
musical" theatre'], [14, 'Shows', 'Opera', 'All opera, light, and "rock" opera'], [15,
 'Concerts', 'Classical', 'All symphony, concerto, and choir concerts'])
```

Si no lo ha establecido `autocommit` a true, confirme con `conn.commit()` después de ejecutar las instrucciones `execute()`.

Los datos se descargan en el archivo `unloaded_category_csv.text0000_part00` del bucket de S3 con el siguiente contenido:

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

Referencia de la API para el conector Python de Amazon Redshift

A continuación encontrará una descripción de las operaciones de la API del conector Python de Amazon Redshift.

redshift_connector

A continuación encontrará una descripción de la operación de la API `redshift_connector`.

`connect(user, database, password[, port, …])`

Establece una conexión a un clúster de Amazon Redshift. Esta función valida la entrada del usuario, se autentica opcionalmente mediante un complemento de proveedores de identidades y, a continuación, crea un objeto de conexión.

`apilevel`

El nivel DBAPI admite, actualmente “2.0”.

`paramstyle`, `str(object='') -> str str(bytes_or_buffer[, encoding[, errors]]) -> str`

El estilo de parámetro de la API de base de datos que se va a utilizar globalmente.

Connection

A continuación encontrará una descripción de las operaciones de la API de conexión para el conector Python de Amazon Redshift.

`__init__(user, password, database[, host, …])`

Inicializa un objeto de conexión sin procesar.

`cursor`

Crea un objeto cursor vinculado a esta conexión.

`commit`

Confirma la transacción de la base de datos actual.

`rollback`

Retrocede la transacción de la base de datos actual.

`close`

Cierra la conexión a la base de datos.

`execute(cursor, operation, vals)`

Ejecuta los comandos SQL especificados. Puede proporcionar los parámetros en forma de secuencia o como una asignación, según el valor de `redshift_connector.paramstyle`.

`run(sql[, stream])`

Ejecuta los comandos SQL especificados. De forma opcional, puede proporcionar una secuencia para utilizarla con el comando COPY.

`xid(format_id, global_transaction_id, …)`

Cree un ID de transacción. Solo utiliza el parámetro `global_transaction_id` en postgres. format_id y branch_qualifier no se utilizan en postgres. El `global_transaction_id` puede ser cualquier identificador de cadena que admite postgres que devuelva una tupla (`format_id`, `global_transaction_id`, `branch_qualifier`).

`tpc_begin(xid)`

Inicia una transacción de TPC con un ID de transacción `xid` que consiste en un ID de formato, un ID de transacción global y un calificador de ramificación.

`tpc_prepare`

Realiza la primera fase de una transacción iniciada con .tpc_begin.

`tpc_commit([xid])`

Cuando se llama sin argumentos, .tpc_commit confirma una transacción de TPC preparada previamente con .tpc_prepare().

`tpc_rollback([xid])`

Cuando se llama sin argumentos, .tpc_rollback revierte una transacción de TPC.

`tpc_recover`

Devuelve una lista de los ID de transacción pendientes adecuados para su uso con .tpc_commit(xid) o .tpc_rollback(xid).

Cursor

A continuación encontrará una descripción de la operación de la API de cursor.

`__init__(connection[, paramstyle])`

Inicializa un objeto cursor sin procesar.

`insert_data_bulk(filename, table_name, parameter_indices, column_names, delimiter, batch_size)`

Ejecuta una instrucción INSERT masiva.

`execute(operation[, args, stream, …])`

Ejecuta una operación de base de datos.

`executemany(operation, param_sets)`

Prepara una operación de base de datos y, a continuación, la ejecuta para todas las secuencias de parámetros o asignaciones proporcionadas.

`fetchone`

Recupera la siguiente fila de un conjunto de resultados de consultas.

`fetchmany([num])`

Recupera el siguiente conjunto de filas de un resultado de consultas.

`fetchall`

Recupera todas las filas restantes de un resultado de consultas.

`close`

Cierre el cursor ahora.

`__iter__`

Se puede iterar un objeto cursor para recuperar las filas de una consulta.

`fetch_dataframe([num])`

Devuelve un marco de datos de los resultados de la última consulta.

`write_dataframe(df, table)`

Escribe el mismo marco de datos de estructura en una base de datos de Amazon Redshift.

`fetch_numpy_array([num])`

Devuelve una matriz NumPy de los resultados de la última consulta.

`get_catalogs`

Amazon Redshift no admite varios catálogos desde una única conexión. Amazon Redshift solo devuelve el catálogo actual.

`get_tables([catalog, schema_pattern, …])`

Devuelve las tablas públicas únicas que están definidas por el usuario dentro del sistema.

`get_columns([catalog, schema_pattern, …])`

Devuelve una lista de todas las columnas de una tabla específica de una base de datos de Amazon Redshift.

Complemento AdfScredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento AdfsCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

Complemento AzureCredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento AzureCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.AzureCredentialsProvider()
```

Complemento BrowserAzureCredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento BrowserAzureCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

Complemento BrowserSamlCredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento BrowserSamlCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

Complemento OktaCredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento OktaCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.OktaCredentialsProvider()
```

Complemento PingCredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento PingCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.PingCredentialsProvider()
```

Complemento SamlCredentialsProvider

A continuación se muestra la sintaxis de la operación de la API del complemento SamlCredentialsProvider para el conector Python de Amazon Redshift.

```
redshift_connector.plugin.SamlCredentialsProvider()
```

Integración de Amazon Redshift para Apache Spark

Apache Spark es un modelo de marco de procesamiento distribuido y de programación que le ayuda a aplicar machine learning, procesamiento de flujos o análisis de gráficos. Del mismo modo que Apache Hadoop, Spark es un sistema de procesamiento distribuido de código abierto utilizado frecuentemente para cargas de trabajo de big data. Spark cuenta con un motor de ejecución optimizado de grafos acíclicos dirigidos (DAG) y almacena activamente los datos en caché en la memoria. Esto puede aumentar el rendimiento, sobre todo en el caso de determinados algoritmos y consultas interactivas.

Esta integración le proporciona un conector Spark que puede utilizar para crear aplicaciones Apache Spark que lean y escriban en datos en Amazon Redshift y Amazon Redshift sin servidor. Estas aplicaciones no comprometen el rendimiento de la aplicación ni la coherencia transaccional de los datos. Esta integración se incluye automáticamente en Amazon EMR y AWS Glue, por lo que puede ejecutar inmediatamente trabajos de Apache Spark que accedan a los datos y los carguen en Amazon Redshift como parte de sus canalizaciones de ingesta y transformación de datos.

Actualmente, puede utilizar las versiones 3.3.0, 3.3.1, 3.3.2 y 3.4.0 de Spark con esta integración.

Esta integración proporciona lo siguiente:

- Authentication de AWS Identity and Access Management (IAM). Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.
- Inserción de predicados y consultas para mejorar el rendimiento.
- Tipos de datos de Amazon Redshift
- Conectividad con Amazon Redshift y Amazon Redshift sin servidor.

Consideraciones y limitaciones al utilizar el conector de Spark

- El URI de directorio temporal apunta a una ubicación de Amazon S3. Este directorio temporal no se limpia automáticamente y podría agregar costos adicionales. Recomendamos utilizar las políticas de ciclo de vida de Amazon S3 de la Guía del usuario de Amazon Simple Storage Service para definir las reglas de retención del bucket de Amazon S3.
- De forma predeterminada, las copias entre Amazon S3 y Redshift no funcionan si el bucket de S3 y el clúster de Redshift se encuentran en regiones de AWS diferentes. Para usar regiones de AWS independientes, establezca el parámetro `tempdir_region` a la región del bucket de S3 utilizada para `tempdir`.
- Escrituras entre regiones entre S3 y Redshift si se escriben datos de Parquet con el parámetro `tempformat`.
- Recomendamos utilizar el cifrado del servidor de Amazon S3 para cifrar los buckets de Amazon S3 utilizados.
- Recomendamos bloquear el acceso público a los buckets de Amazon S3.
- Recomendamos que el clúster de Amazon Redshift no sea de acceso público.
- Recomendamos activar el registro de auditoría de Amazon Redshift.
- Recomendamos activar el cifrado en reposo de Amazon Redshift.
- Recomendamos activar SSL para la conexión JDBC desde Spark en Amazon EMR a Amazon Redshift.
- Recomendamos pasar un rol de IAM mediante el parámetro `aws_iam_role` para el parámetro de autenticación de Amazon Redshift.

Autenticación con el conector de Spark

En el siguiente diagrama se describe la autenticación entre Amazon S3, Amazon Redshift, el controlador de Spark y los ejecutores de Spark.

Autenticación entre Redshift y Spark

Puede utilizar el controlador JDBC versión 2 proporcionado por Amazon Redshift para conectarse a Amazon Redshift con el conector de Spark mediante la especificación de credenciales de inicio de sesión. Para utilizar IAM, configure su URL de JDBC para que utilice la autenticación de IAM. Para conectarse a un clúster de Redshift desde Amazon EMR o AWS Glue, asegúrese de que su rol de IAM tiene los permisos necesarios para recuperar credenciales de IAM temporales. En la siguiente lista se describen todos los permisos que su rol de IAM necesita para recuperar credenciales y ejecutar operaciones de Amazon S3.

- Redshift:GetClusterCredentials (para clústeres de Redshift aprovisionados)
- Redshift:DescribeClusters (para clústeres de Redshift aprovisionados)
- Redshift:GetWorkgroup (para grupos de trabajo de Amazon Redshift sin servidor)
- Redshift:GetCredentials (para grupos de trabajo de Amazon Redshift sin servidor)
- s3:ListBucket
- s3:GetBucket
- s3:GetObject
- s3:PutObject
- s3:GetBucketLifecycleConfiguration

Para obtener más información sobre GetClusterCredentials, consulte Políticas de recursos para GetClusterCredentials.

También debe asegurarse de que Amazon Redshift puede asumir el rol de IAM durante las operaciones `COPY` y `UNLOAD`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        }
    ]
}
```

Si utiliza el controlador JDBC más reciente, este administrará automáticamente la transición de un certificado autofirmado de Amazon Redshift a un certificado de ACM. No obstante, deberá especificar las opciones de SSL para la URL de JDBC.

A continuación, se muestra un ejemplo de cómo especificar la URL del controlador JDBC y `aws_iam_role` para conectarse a Amazon Redshift.

```
df.write \
  .format("io.github.spark_redshift_community.spark.redshift ") \
  .option("url", "jdbc:redshift:iam://<the-rest-of-the-connection-string>") \
  .option("dbtable", "<your-table-name>") \
  .option("tempdir", "s3a://<your-bucket>/<your-directory-path>") \
  .option("aws_iam_role", "<your-aws-role-arn>") \
  .mode("error") \
  .save()
```

Autenticación entre Amazon S3 y Spark

Si utiliza un rol de IAM para la autenticación entre Spark y Amazon S3, utilice uno de los siguientes métodos:

- El SDK de AWS para Java intentará encontrar automáticamente las credenciales de AWS mediante la cadena de proveedores de credenciales predeterminada implementada por la clase DefaultAWSCredentialsProviderChain. Para obtener más información, consulte Using the Default Credential Provider Chain (Uso de la cadena de proveedores de credenciales predeterminada).
- Puede especificar claves de AWS a través de las propiedades de configuración de Hadoop. Por ejemplo, si su configuración de `tempdir` apunta a un sistema de archivos `s3n://`, establezca las propiedades `fs.s3n.awsAccessKeyId` y `fs.s3n.awsSecretAccessKey` en un archivo de configuración XML de Hadoop o llame a `sc.hadoopConfiguration.set()` para cambiar la configuración de Hadoop global de Spark.

Por ejemplo, si utiliza el sistema de archivos s3n, agregue:

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

Para el sistema de archivos s3a, agregue:

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

Si utiliza Python, utilice las siguientes operaciones:

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",
 "YOUR_SECRET_ACCESS_KEY")
```

- Codifique las claves de autenticación en la URL `tempdir`. Por ejemplo, el URI `s3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dir` codifica el par de claves (`ACCESSKEY`, `SECRETKEY`).

Autenticación entre Redshift y Amazon S3

Si utiliza los comandos COPY y UNLOAD en la consulta, también deberá conceder acceso a Amazon S3 a Amazon Redshift para que ejecute las consultas en su nombre. Para ello, autorice primero a Amazon Redshift a acceder a otros servicios de AWS y, a continuación, autorice las operaciones COPY y UNLOAD mediante roles de IAM.

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Integración con AWS Secrets Manager

Puede recuperar las credenciales de nombre de usuario y contraseña de Redshift de un secreto almacenado en AWS Secrets Manager. Para proporcionar automáticamente las credenciales de Redshift, utilice el parámetro `secret.id`. Para obtener más información sobre cómo crear un secreto de credenciales de Redshift, consulte Crear un secreto de base de datos de AWS Secrets Manager.

GroupID	ArtifactID	Revisiones compatibles	Descripción
com.amazonaws.secretsmanager	aws-secretsmanager-jdbc	1.0.12	La biblioteca de conexiones SQL

GroupID	ArtifactID	Revisiones compatibles	Descripción
			de AWS Secrets Manager para Java permite a los desarrolladores de Java conectarse fácilmente a las bases de datos SQL con los secretos almacenados en AWS Secrets Manager.

> **Note**
>
> Reconocimiento: esta documentación contiene código y lenguaje de muestra desarrollados por la Apache Software Foundation con licencia Apache 2.0.

Mejoras de rendimiento con la inserción

El conector de Spark aplica automáticamente la inserción de predicados y consultas para optimizar el rendimiento. Esta asistencia implica que, si utiliza una función compatible en su consulta, el conector de Spark convertirá la función en una consulta SQL y ejecutará la consulta en Amazon Redshift. Con esta optimización se recuperan menos datos, por lo que Apache Spark puede procesar menos datos y tener un mejor rendimiento. De forma predeterminada, la inserción está activada automáticamente. Para desactivarla, establezca `autopushdown` a false.

```
import sqlContext.implicits._val
 sample= sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url",jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "event")
    .option("autopushdown", "false")
    .load()
```

Las siguientes funciones son compatibles con la inserción. Si utiliza una función que no está en esta lista, el conector de Spark realizará la función en Spark en lugar de hacerlo en Amazon Redshift, lo que provocará un rendimiento no optimizado. Para obtener una lista completa de las funciones de Spark, consulte Built-in Functions (Funciones incorporadas).

- Funciones de agregación
  - avg
  - count
  - máx.
  - min
  - sum
  - stddev_samp
  - stddev_pop
  - var_samp
  - var_pop
- Operadores booleanos
  - in
  - isnull
  - isnotnull
  - contiene
  - endswith
  - startswith
- Logical operators (Operadores lógicos)
  - Protección de los datos
  - o bien
  - not (o !)
- Funciones matemáticas
  - +
  - -
  - *
  - /
  - - (unitario)

- abs
- acos
- asin
- atan
- ceil
- cos
- exp
- floor
- greatest
- least
- log10
- pi
- pow
- round
- sin
- sqrt
- tan

- Funciones varias
  - cast
  - coalesce
  - decimal
  - if
  - in
- Operadores relacionales
  - **!=**
  - **=**
  - **>**
  - **>=**
  - **<**
  - **<=**

- Funciones de cadena
  - ascii
  - lpad
  - rpad
  - translate
  - upper
  - lower
  - longitud
  - trim
  - ltrim
  - rtrim
  - like
  - subcadena
  - concat
- Funciones de fecha y hora
  - add_months
  - date
  - date_add
  - date_sub
  - date_trunc
  - timestamp
  - trunc
- Operadores matemáticos
  - CheckOverflow
  - PromotePrecision
- Operaciones relacionales
  - Aliases (por ejemplo, AS)
  - CaseWhen
  - Distinct
  - InSet

- Uniones y uniones cruzadas
- Límites
- Unions, union all
- ScalarSubquery
- Sorts (ascendente y descendente)
- UnscaledValue

Otras opciones de configuración

Cambio del tamaño máximo de las columnas de cadenas

Redshift crea columnas de cadena como columnas de texto al crear tablas, que se almacenan como VARCHAR(256). Si desea columnas que admitan tamaños mayores, puede utilizar maxlength para especificar la longitud máxima de las columnas de cadenas. A continuación se muestra un ejemplo de cómo especificar `maxlength`.

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Configuración de un tipo de columna

Para establecer un tipo de columna, utilice el campo `redshift_type`.

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

Establecimiento de una codificación de compresión en una columna

Para utilizar una codificación de compresión específica en una columna, use el campo de codificación. Para obtener una lista completa de las codificaciones de compresión admitidas, consulte Codificaciones de compresión.

Establecimiento de una descripción para una columna

Para establecer una descripción, utilice el campo `description`.

Autenticación entre Redshift y Amazon S3

De forma predeterminada, el resultado se descarga en Amazon S3 en formato parquet. Para descargar el resultado como archivo de texto delimitado por barras verticales, especifique la siguiente opción.

```
.option("unload_s3_format", "TEXT")
```

Ejecutar perezosamente instrucciones de empuje

Parámetro	Obligatorio	Valor predeterminado	Descripción
spark.datasource.redshift.community.autopushdown.lazyMode	No	True	Especifica si el conector debe ejecutar perezosamente las instrucciones de empuje de Redshift. Si es verdadero, el conector de Spark recupera todos los modelos y la información relacionados antes de ejecutar la consulta, lo que generalmente produce un mejor rendimiento. Si es falso, el conector de Spark ejecuta las instrucciones de empuje inmediatamente en el hilo principal del controlador de Spark y se serializa en

Parámetro	Obligatorio	Valor predeterminado	Descripción
			todas las expresion es.

Parámetros de conector

La asignación de parámetros u `OPTIONS` en Spark SQL admite las siguientes configuraciones.

Parámetro	Obligatorio	Valor predeterminado	Descripción
dbtable	Sí, a menos que se especifique la consulta	N/A	La tabla que se creará o de la que se leerá en Redshift. Este parámetro es necesario cuando se vuelven a guardar los datos en Redshift.
query	Sí, a menos que se especifique dbtable	N/A	La consulta desde la que se leerá en Redshift.
user	No	N/A	El nombre de usuario de Redshift. Debe utilizarse con el parámetro password. Válido solo si el usuario y la contraseña no son parámetros en la URL. El uso de ambos provocará un error.
password	No	N/A	La contraseña de Redshift. Debe utilizarse con el

Parámetro	Obligatorio	Valor predeterminado	Descripción
			parámetro user. Válido solo si el usuario y la contraseña no son parámetros en la URL. El uso de ambos provocará un error.

Parámetro	Obligatorio	Valor predeterminado	Descripción
url	No	N/A	Una URL de JDBC. El formato es jdbc:subprotocolo://host:port/base_de_datos?user=nombre_de_usuario&password=contraseña. El subprotocolo puede ser postgresql o Redshift, según el controlador JDBC que haya cargado. Tenga en cuenta que en classpath debe haber un controlador compatible con Redshift y coincidir con esta URL. El host y el puerto deben apuntar al nodo maestro de Redshift, por lo que debe configurar grupos de seguridad o VPC para permitir el acceso desde su aplicación de controlador. La base de datos es el nombre de la base de datos de Redshift.

Parámetro	Obligatorio	Valor predeterminado	Descripción
			El usuario y la contraseña son las credenciales para acceder a la base de datos, que deben estar insertadas en esta URL para JDBC, y su cuenta de usuario de base de datos debe tener los permisos necesario s para acceder a la tabla.
aws_iam_role	Solo si se utilizan roles de IAM para autorizar las operaciones COPY/ UNLOAD de Redshift	N/A	ARN completamente especificado del rol de IAM adjunto al clúster de Redshift.

Parámetro	Obligatorio	Valor predeterminado	Descripción
forward_spark_s3_credentials	No	False	Indica si esta biblioteca debe descubrir automáticamente las credenciales que utiliza Spark para conectarse a Amazon S3, y si debe reenviarlas a Redshift a través del controlador JDBC. Estas credenciales se envían como parte de la consulta JDBC. Por lo tanto, le recomendamos que active el cifrado SSL con la conexión de JDBC cuando utilice esta opción.
temporary_aws_access_key_id	No	N/A	Clave de acceso de AWS. Debe tener permisos de escritura en ese bucket de S3.
temporary_aws_secret_access_key	No	N/A	Clave de acceso secreta de AWS que corresponde a la clave de acceso.
temporary_aws_session_token	No	N/A	Token de sesión de AWS correspondiente a la clave de acceso proporcionada.

Parámetro	Obligatorio	Valor predeterminado	Descripción
tempdir	No	N/A	Una ubicación en la que se puede escribir en Amazon S3. Se utiliza para descargar datos al leer y datos de Avro que se deben cargar en Redshift al escribir. Si utiliza un origen de datos de Redshift para Spark como parte de una canalización ETL normal, puede ser útil establecer una política de ciclo de vida a un bucket y utilizarlo como ubicación temporal de estos datos.

Parámetro	Obligatorio	Valor predeterminado	Descripción
jdbcdriver	No	Determinado por el subprotocolo de la URL de JDBC	El nombre de la clase del controlador JDBC que se usará. Esta clase debe estar en classpath. En la mayoría de los casos, no debe ser necesario especific ar esta opción, ya que el nombre de clase del controlad or apropiado se determinará automáticamente por el subprotocolo de la URL de JDBC.
diststyle	No	Even	El estilo de distribuc ión de Redshift que se utilizará al crear una tabla. Las opciones válidas son EVEN, KEY o ALL. Cuando utilice KEY, también debe establecer una clave de distribución con la opción distkey.
distkey	No, a menos que se utilice DISTSTYLE _KEY	N/A	El nombre de una columna de la tabla que se utilizará como la clave de distribuc ión al crear una tabla.

Parámetro	Obligatorio	Valor predeterminado	Descripción
sortkeyspec	No	N/A	Una definición completa de la clave de clasificación de Redshift.
include_column_list	No	False	Indica si esta biblioteca debe extraer automáticamente las columnas del esquema y agregarlas al comando COPY según las opciones de mapeo de columnas.
description	No	N/A	Una descripción de la tabla. La descripción se establece con el comando COMMENT de SQL y aparece en la mayoría de las herramientas de consulta. Consulte los metadatos de `description` para establecer descripciones en columnas individuales.

Parámetro	Obligatorio	Valor predeterminado	Descripción
preactions	No	N/A	A una lista delimitada por punto y coma de comandos SQL que deben ejecutarse antes de cargar el comando COPY. Podría ser útil ejecutar comandos DELETE o similares antes de cargar nuevos datos. Si el comando contiene %s, se formateará el nombre de la tabla antes de la ejecución (en caso de que utilice una tabla provisional). Si se produce un error en este comando, se tratará como una excepción. Si utiliza una tabla provisional, los cambios se revertirán y se restaurará la tabla de copia de seguridad si se produce un error en las acciones previas.

Parámetro	Obligatorio	Valor predeterminado	Descripción
extracopyoptions	No	N/A	Una lista de opciones adicionales para agregarlas al comando COPY de Redshift al cargar datos (como `TRUNCATECOLUMNS` o `MAXERROR n`). Consulte Optional parameter (Parámetro opcional) para ver una lista completa de los parámetros disponibles. Tenga en cuenta que como estas opciones se adjuntan al final del comando `COPY`, solo puede utilizar opciones que tengan sentido al final de él. Eso debería abarcar la mayoría de los casos de uso posibles.

Parámetro	Obligatorio	Valor predeterminado	Descripción
sse_kms_key	No	N/A	El ID de la clave de AWS KMS que se utilizará para el cifrado en el servidor en S3 durante la operación UNLOAD de Redshift en lugar del cifrado predeterminado de AWS. El rol de IAM de Redshift debe tener acceso a la clave de KMS para escribir con ella y el rol de IAM de Spark debe tener acceso a la clave para las operaciones de lectura. La lectura de los datos cifrados no requiere cambios (AWS se encarga de ello) siempre y cuando el rol de IAM de Spark tenga el acceso adecuado.

Parámetro	Obligatorio	Valor predeterminado	Descripción
tempformat	No	AVRO	El formato en el que se guardan los archivos temporales en Amazon S3 al escribir en Redshift. Los valores válidos son AVRO, CSV y CSV GZIP (CSV comprimido).
csvnullstring (experimental)	No	Null	El valor de cadena que se escribirá para los valores nulos cuando se utilice el formato temporal CSV. Debe ser un valor que no aparezca en sus datos reales.
autopushdown	No	True	Indica si se aplica la inserción de predicados y consultas mediante la captura y el análisis de los planes lógicos de Spark para las operaciones SQL. Las operaciones se traducen en una consulta SQL y, a continuación, se ejecutan en Redshift para mejorar el rendimiento.

Parámetro	Obligatorio	Valor predeterminado	Descripción
autopushdown.s3_result_cache	No	False	Almacene en caché la consulta SQL para descargar datos de la asignación de rutas de Amazon S3 en la memoria, de modo que no sea necesario volver a ejecutar la misma consulta en la misma sesión de Spark. Solo se admite cuando la autoinserción está activada. No recomendamos utilizar este parámetro cuando se mezclen operaciones de lectura y escritura porque los resultados almacenados en caché podrían contener información obsoleta.

Parámetro	Obligatorio	Valor predeterminado	Descripción
unload_s3_format	No	Parquet	El formato con el que se descargan los resultados de consulta. Las opciones válidas son Parquet y Text, que especifica que se descarguen los resultados de la consulta en formato de texto delimitado por barra vertical.
extraunloadoptions	No	N/A	Opciones adicionales que se anexarán al comando UNLOAD de Redshift. No se garantiza que funcionen todas las opciones, ya que algunas pueden entrar en conflicto con otras establecidas en el conector.
copydelay	No	30000	Retraso (en ms) entre los reintentos de las operaciones COPY de Redshift.
copyretrycount	No	2	Número de veces que se vuelven a intentar las operaciones COPY de Redshift.

Parámetro	Obligatorio	Valor predeterminado	Descripción
tempdir_region	No	N/A	Región de AWS donde se encuentra `tempdir`. Al configurar esta opción, se mejora el rendimiento del conector para las interacciones con `tempdir` además de proporcionar automáticamente este valor como parte de las operaciones COPY y UNLOAD durante las operaciones de lectura y escritura del conector. Esta configuración se recomienda en las siguientes situaciones: 1) Cuando el conector se ejecuta fuera de AWS, ya que se producirá un error en la detección automática de regiones y el rendimiento del conector se verá afectado negativamente.

Parámetro	Obligatorio	Valor predeterminado	Descripción
			2) Cuando `tempdir` se encuentra en una región diferente a la del clúster de Redshift, ya que con esta configuración se elimina la necesidad de suministrar la región manualmente mediante los parámetros `extracopyoptions` y `extraunloadoptions`. `tempdir` no se puede encontrar en una región diferente a la del clúster de Redshift cuando se utiliza `PARQUET` como `tempformat` incluso si se utiliza este parámetro. 3) Cuando el conector se ejecuta en una región diferente a `tempdir`, ya que mejora el rendimiento de acceso del conector de `tempdir`.

Parámetro	Obligatorio	Valor predeterminado	Descripción
secret.id	No	N/A	El nombre o el ARN del secreto almacenado en AWS Secrets Manager. Puede usar este parámetro para proporcionar automáticamente las credenciales de Redshift, pero solo si el usuario, la contraseña y las credenciales de `DbUser` no se pasan a la URL de JDBC ni a través de otras opciones.

Parámetro	Obligatorio	Valor predeterminado	Descripción
secret.region	No	N/A	La región principal de AWS, como por ejemplo Este de EE. UU. (Norte de Virginia), para buscar el valor `secret.id` . Si no se especific a esta región, el conector intentará utilizar la Cadena de proveedores de credenciales predeterminada para resolver la región del `secret.id` . En algunos casos, por ejemplo, si utiliza el conector fuera de una, el conector no podrá encontrar la región. Recomenda mos usar esta configuración en las siguientes situacion es: 1) Cuando el conector funciona fuera de AWS, ya que la detección automática de regiones producirá un error e impedirá

Parámetro	Obligatorio	Valor predeterminado	Descripción
			la autenticación con Redshift Cuando el conector se ejecuta en una región diferente `secret.id` , ya que mejora el rendimien to de acceso del conector del secreto.
secret.vpcEndpointUrl	No	N/A	La URL del punto de conexión DNS de PrivateLink para AWS Secrets Manager al invalidar la Cadena de proveedores de credenciales predeterminada.
secret.vpcEndpoint Region	No	N/A	La región del punto de conexión DNS de PrivateLi nk para AWS Secrets Manager al invalidar la Cadena de proveedores de credenciales predeterminada.

Parámetro	Obligatorio	Valor predeterminado	Descripción
jdbc.*	No	N/A	Parámetros adicionales para pasarlos al controlador JDBC subyacente, donde el comodín es el nombre del parámetro JDBC, como jdbc.ssl. Tenga en cuenta que el prefijo `jdbc` se eliminará antes de pasarlo al controlador JDBC. Para ver todas las opciones posibles del controlador JDBC de Redshift, consulte Opciones de configuración del controlador JDBC versión 2.1.

Parámetro	Obligatorio	Valor predeterminado	Descripción
label	No	" "	Un identificador para incluir en el conjunto de grupos de consultas al ejecutar consultas con el conector. Debe tener 100 caracteres o menos y todos los caracteres deben ser válidos `unicodeIdentifierParts` . Si el identificador tiene más de 100 caracteres, se eliminará el exceso. Al ejecutar una consulta con el conector, el grupo de consultas se establecerá como una cadena en formato JSON, como `{"spark-redshift-connector":{"svc":"","ver":"5.1.0-amzn-1-spark_3.3","op":"Read","lbl":""}}`) . Esta opción sustituye el valor de la clave `lbl`.

> **Note**
>
> Reconocimiento: esta documentación contiene código y lenguaje de muestra desarrollados por la Apache Software Foundation con licencia Apache 2.0.

Tipos de datos admitidos

Los siguientes tipos de datos de Amazon Redshift son compatibles con el conector de Spark. Para obtener una lista completa de los tipos de datos compatibles con Amazon Redshift, consulte Data types (Tipos de datos). Si un tipo de datos no se encuentra en la tabla siguiente, no está admitido en el conector de Spark.

Tipo de datos	Alias
SMALLINT	INT2
INTEGER	INT, INT4
BIGINT	INT8
DECIMAL	NUMERIC
REAL	FLOAT4
DOUBLE PRECISION	FLOAT8, FLOAT
BOOLEANO	BOOL
CHAR	CHARACTER, NCHAR, BPCHAR
VARCHAR	CHARACTER VARYING, NVARCHAR, TEXT
DATE	
TIMESTAMP	TIMESTAMP sin zona horaria
TIMESTAMPTZ	Timestamp with time zone
SUPER	

Tipo de datos	Alias
TIME	Hora sin zona horaria
TIMETZ	Time with time zone
VARBYTE	VARBINARY, BINARY VARYING

Tipos de datos complejos

Puede usar el conector Spark para leer y escribir tipos de datos complejos de Spark, como `ArrayType`, `MapType` y `StructType` hacia y desde las columnas de tipos de datos SUPER de Redshift. Si proporciona un esquema durante una operación de lectura, los datos de la columna se convertirán en los tipos complejos correspondientes en Spark, incluidos los tipos anidados. Además, si `autopushdown` está habilitado, la proyección de los atributos anidados, los valores del mapa y los índices de matriz se reducen a Redshift, de modo que ya no es necesario descargar toda la estructura de datos anidada al acceder solo a una parte de los datos.

Cuando escribe DataFrames desde el conector, cualquier columna de tipo `MapType` (con `StringType`), `StructType` o `ArrayType` se escribe en una columna de tipos de datos SUPER de Redshift. Al escribir estas estructuras de datos anidadas, el parámetro `tempformat` debe ser del tipo `CSV`, `CSV GZIP` o `PARQUET`. Con `AVRO` provocará una excepción. La escritura de una estructura de datos `MapType` que tiene un tipo de clave distinto de `StringType` también provocará una excepción.

StructType

En el siguiente ejemplo se muestra cómo crear una tabla con un tipo de datos SUPER que contiene una estructura

```
create table contains_super (a super);
```

A continuación, puede utilizar el conector para consultar un campo `StringType` `hello` de la columna SUPER a en la tabla utilizando un esquema como el del siguiente ejemplo.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)
```

```
val schema = StructType(StructField("a", StructType(StructField("hello",
 StringType) ::Nil)) :: Nil)

val helloDF = sqlContext.read
.format("io.github.spark_redshift_community.spark.redshift")
.option("url", jdbcURL )
.option("tempdir", tempS3Dir)
.option("dbtable", "contains_super")
.schema(schema)
.load().selectExpr("a.hello")
```

En el siguiente ejemplo se muestra cómo se escribe una estructura en la columna `a`.

```
import org.apache.spark.sql.types._
import org.apache.spark.sql._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
 StringType) ::Nil)) :: Nil)
val data = sc.parallelize(Seq(Row(Row("world"))))
val mydf = sqlContext.createDataFrame(data, schema)

mydf.write.format("io.github.spark_redshift_community.spark.redshift").
option("url", jdbcUrl).
option("dbtable", tableName).
option("tempdir", tempS3Dir).
option("tempformat", "CSV").
mode(SaveMode.Append).save
```

MapType

Si prefiere usar `MapType` para representar los datos, puede usar una estructura de datos `MapType` en el esquema y recupera el valor correspondiente a una clave en el mapa. Tenga en cuenta que todas las claves de la estructura de datos `MapType` debe ser de tipo String y todos los valores deben ser del mismo tipo, como int.

En el siguiente ejemplo se muestra cómo obtener el valor de la clave `hello` en la columna `a`.

```
import org.apache.spark.sql.types._
```

```
val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", MapType(StringType, IntegerType))::Nil)

val helloDF = sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url", jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "contains_super")
    .schema(schema)
    .load().selectExpr("a['hello']")
```

ArrayType

Si la columna contiene una matriz en lugar de una estructura, puede usar el conector para consultar el primer elemento de la matriz.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", ArrayType(IntegerType)):: Nil)

val helloDF = sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url", jdbcURL )
    .option("tempdir", tempS3Dir)
    .option("dbtable", "contains_super")
    .schema(schema)
    .load().selectExpr("a[0]")
```

Limitaciones

Con los tipos de datos complejos con el conector de Spark se presentan las siguientes limitaciones:

- Todos los nombres de los campos de estructura anidados y las claves de mapa deben estar en minúsculas. Si busca nombres de campos complejos con letras mayúsculas, puede intentar omitir el esquema y usar la función de Spark `from_json` para convertir la cadena devuelta localmente como una solución alternativa.

- Todos los campos del mapa utilizados en las operaciones de lectura o escritura deben tener solo claves `StringType`.
- Solo `CSV`, `CSV GZIP` y `PARQUET` son valores de formato temporal compatibles para escribir tipos complejos en Redshift. Al intentar usar `AVRO` se generará una excepción.

Configuración de una conexión del controlador ODBC versión 2.x para Amazon Redshift

Puede utilizar una conexión ODBC para conectarse a su clúster de Amazon Redshift desde distintas aplicaciones y herramientas de cliente SQL de terceros. Si la herramienta de cliente es compatible con JDBC, puede elegir utilizar ese tipo de conexión en lugar de una conexión ODBC, ya que JDBC es más fácil de configurar. Sin embargo, si la herramienta de cliente no es compatible con JDBC, puede seguir los pasos de esta sección para configurar una conexión ODBC en el equipo cliente o en la instancia de Amazon EC2.

Amazon Redshift proporciona controladores ODBC de 64 bits para los sistemas operativos Linux y Windows; los controladores ODBC de 32 bits ya no se fabrican. Actualmente, no se admite macOS X. No se publicarán más actualizaciones de los controladores ODBC de 32 bits, excepto las revisiones de seguridad urgentes. Para descargar e instalar controladores ODBC para macOS X y sistemas operativos de 32 bits, consulte Configuración de una conexión ODBC.

Para obtener la información más reciente acerca de los cambios del controlador ODBC, consulte Registro de cambios.

Temas

- Obtención de la URL de ODBC
- Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows
- Instalación y configuración del controlador ODBC de Amazon Redshift en Linux
- Configuración de la autenticación
- Conversión de tipos de datos
- Configuración de las opciones del controlador ODBC
- Versiones anteriores del controlador ODBC

Obtención de la URL de ODBC

Amazon Redshift muestra la URL de ODBC de su clúster en la consola de Amazon Redshift. Esta dirección URL contiene la información necesaria para configurar la conexión entre el equipo cliente y la base de datos.

Un URL de ODBC tiene el siguiente formato:

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;
 PWD=password; Port=port_number
```

Los campos del formato anterior tienen los siguientes valores:

Valores de campo de la URL de ODBC

Campo	Valor
Driver	Nombre del controlador ODBC de 64 bits que se va a utilizar: Amazon Redshift ODBC Driver (x64) (Controlador ODBC de Amazon Redshift [x64])
Server	El host de punto de conexión del clúster de Amazon Redshift.
Database	Base de datos que creó para su clúster.
UID	Nombre de usuario de base de datos de una cuenta de usuario que tiene permiso para conectarse a la base de datos. Si bien este valor es un permiso de la base de datos, no un permiso de clúster, puede utilizar la cuenta de usuario administrador de Redshift que configuró cuando lanzó el clúster.
PWD	Contraseña de la cuenta de usuario de base de datos para conectarse a la base de datos.
Port	Número de puerto que especificó cuando lanzó el clúster. Si tiene un firewall, asegúrese de que este puerto esté abierto para poder usarlo.

A continuación, se muestra un ejemplo de la URL de ODBC:

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com; Database=dev; UID=adminuser;
 PWD=insert_your_admin_user_password_here; Port=5439
```

Para obtener información sobre dónde encontrar la URL de ODBC, consulte Obtención de la cadena de conexión a su clúster.

Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows

Requisitos del sistema

Debe instalar el controlador ODBC de Amazon Redshift en los equipos cliente que tienen acceso a un almacenamiento de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir con los siguientes requisitos mínimos:

- Derechos de administrador en la máquina.
- La máquina cumple con los siguientes requisitos del sistema:
  - Uno de los sistemas operativos siguientes:
    - Windows 10 u 8.1.
    - Windows Server 2019, 2016 o 2012.
  - 100 MB de espacio disponible en el disco.
  - Visual C++ Redistributable for Visual Studio 2015 para Windows de 64 bits instalado. Puede descargar el paquete de instalación en Descargar Visual C++ Redistributable for Visual Studio 2022 en el sitio web de Microsoft.

Instalación del controlador ODBC de Amazon Redshift

Utilice el procedimiento a continuación para descargar e instalar el controlador ODBC de Amazon Redshift para los sistemas operativos Windows. Utilice un controlador diferente solo si está ejecutando una aplicación de terceros certificada para su uso con Amazon Redshift que requiere un controlador específico.

Para descargar e instalar el controlador ODBC:

1. Descargue el siguiente controlador: controlador ODBC de 64 bits versión 2.1.0.0

   El nombre de este controlador es Amazon Redshift ODBC Driver (x64) (Controlador ODBC de Amazon Redshift [x64]).

> **Note**
>
> Los controladores ODBC de 32 bits se suspenden. No se publicarán más actualizaciones, excepto las revisiones de seguridad urgentes. Para descargar e instalar controladores ODBC para sistemas operativos de 32 bits, consulte Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.

2. Consulte Licencia del controlador ODBC versión 2.x de Amazon Redshift.
3. Haga doble clic en el archivo .msi y, a continuación, siga los pasos en el asistente para instalar el controlador.

Creación de una entrada de sistema DSN para una conexión ODBC

Después de descargar e instalar el controlador ODBC, agregue una entrada de nombre de origen de datos (DSN) al equipo cliente o a la instancia de Amazon EC2. Las herramientas de cliente SQL pueden utilizar este origen de datos para conectarse a la base de datos de Amazon Redshift.

Se recomienda crear un DSN del sistema en lugar de un DSN de usuario. Algunas aplicaciones cargan los datos mediante una cuenta de usuario de base de datos diferente y es posible que no puedan detectar los DSN de usuario que se crean en otra cuenta de usuario de base de datos.

> **Note**
>
> Para la autenticación con credenciales de AWS Identity and Access Management (IAM) o credenciales de proveedor de identidad (IdP), se requieren pasos adicionales. Para obtener más información, consulte Configurar una conexión JDBC u ODBC para usar credenciales de IAM.

Para crear una entrada DSN del sistema para una conexión ODBC:

1. En el menú Start (Inicio), escriba “ODBC Data Sources” (Orígenes de datos ODBC). Elija ODBC Data Sources (Orígenes de datos ODBC).

   Asegúrese de elegir el Administrador de orígenes de datos ODBC que tenga el mismo valor de bits que la aplicación cliente que está utilizando para conectarse a Amazon Redshift.

2. En ODBC Data Source Administrator (Administrador de orígenes de datos ODBC), elija la pestaña Driver (Controlador) y busque la siguiente carpeta del controlador: Amazon Redshift ODBC Driver (x64) (Controlador ODBC de Amazon Redshift [x64]).
3. Elija la pestaña DSN de sistema para configurar el controlador para todos los usuarios del equipo o la pestaña DSN de usuario para configurar solamente el controlador para la cuenta de usuario.
4. Elija Añadir. Se abrirá la ventana Create New Data Source (Crear nuevo origen de datos).
5. Elija Amazon Redshift ODBC Driver (x64) (Controlador ODBC de Amazon Redshift [x64]) y, a continuación, elija Finish (Finalizar). Se abrirá la ventana Amazon Redshift ODBC Driver DSN Setup (Configuración de DSN del controlador ODBC de Amazon Redshift).
6. En la sección Connection Settings (Configuración de conexión), escriba la siguiente información:

   Nombre de origen de datos

   Escriba un nombre para el origen de datos. Por ejemplo, si siguió la Guía de introducción a Amazon Redshift, podría escribir `exampleclusterdsn` para que le sea más fácil recordar el clúster que asocia a este DSN.

   Server

   Especifique el host de punto de conexión del clúster de Amazon Redshift. Puede encontrar esta información en la consola de Amazon Redshift en la página de detalles del clúster. Para obtener más información, consulte Configuración de conexiones en Amazon Redshift.

   Puerto

   Escriba el número de puerto que usa la base de datos. Según el puerto que haya seleccionado al crear, modificar o migrar el clúster, se permitirá el acceso al puerto seleccionado.

   Base de datos

   Introduzca el nombre de la base de datos de Amazon Redshift. Si ha lanzado el clúster sin especificar un nombre de base de datos, escriba `dev`. De lo contrario, utilice el nombre que eligió durante el proceso de inicio. Si siguió la Guía de introducción a Amazon Redshift, ingrese `dev`.
7. En la sección Authentication (Autenticación), especifique las opciones de configuración para configurar la autenticación de IAM o estándar.
8. Elija SSL Options (Opciones de SSL) y especifique un valor para el siguiente campo:

   Modo de autenticación

Elija un modo para controlar la Capa de conexión segura (SSL). En un entorno de prueba, podría usar `prefer`. No obstante, para entornos de producción y cuando se requiera un intercambio seguro de datos, use `verify-ca` o `verify-full`.

9. En la pestaña Proxy, especifique cualquier configuración de conexión proxy.
10. En la pestaña Additional Options (Opciones adicionales), especifique las opciones sobre cómo devolver los resultados de la consulta a la herramienta o aplicación de cliente SQL.
11. En Opciones avanzadas, especifique valores para `logLevel`, `logPath`, `compression` y otras opciones.
12. Seleccione Probar. Si el equipo cliente puede conectarse a la base de datos de Amazon Redshift, aparecerá el siguiente mensaje: Connection successful (Conexión realizada correctamente).
    Si el equipo cliente no puede conectarse a la base de datos, genere un archivo de registro y póngase en contacto con soporte de AWS para solucionar los posibles problemas. Para obtener información sobre la generación de registros, consulte (LINK).
13. Seleccione Aceptar.

Instalación y configuración del controlador ODBC de Amazon Redshift en Linux

Requisitos del sistema

Debe instalar el controlador ODBC de Amazon Redshift en los equipos cliente que tienen acceso a un almacenamiento de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir con los siguientes requisitos mínimos:

- Acceso raíz en la máquina.
- Una de las siguientes distribuciones:
  - Red Hat® Enterprise Linux® (RHEL) 8 o versiones posteriores
  - CentOS 8 o versiones posteriores.
- 150 MB de espacio disponible en el disco.
- unixODBC 2.2.14 o posterior.
- glibc 2.26 o posterior.

Instalación del controlador ODBC de Amazon Redshift

Para descargar e instalar el controlador ODBC versión 2.x de Amazon Redshift para Linux:

1. Descargue el siguiente controlador: controlador RPM de 64 bits versión 2.1.0.0

   > **Note**
   >
   > Los controladores ODBC de 32 bits se suspenden. No se publicarán más actualizaciones, excepto las revisiones de seguridad urgentes.

2. Vaya a la ubicación en la que descargó el paquete y, a continuación, ejecute alguno de los siguientes comandos. Utilice el comando que corresponda a su distribución Linux.

   En los sistemas operativos RHEL y CentOS, ejecute el siguiente comando:

   ```
   yum --nogpgcheck localinstall RPMFileName
   ```

   Reemplace `RPMFileName` por el nombre de archivo del paquete RPM. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 64 bits:

   ```
   yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
   ```

Uso de un administrador de controladores ODBC para configurar el controlador ODBC en Linux

En Linux, debe utilizar un administrador de controlador ODBC para configurar la conexión ODBC. Los administradores del controlador ODBC usan archivos de configuración para definir y configurar los controladores y el origen de datos de ODBC. El administrador del controlador ODBC que utiliza depende del sistema operativo que utiliza.

Configuración del controlador ODBC mediante el administrador de controladores UnixODBC

Para configurar el controlador ODBC de Amazon Redshift, se requieren los siguientes archivos:

- `amazon.redshiftodbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Si instaló el controlador en la ubicación predeterminada, el archivo de configuración `amazon.redshiftodbc.ini` se encuentra en `/opt/amazon/redshiftodbcx64`.

Además, en /opt/amazon/redshiftodbcx64, puede encontrar archivos odbc.ini y odbcinst.ini de muestra. Puede utilizar estos archivos como ejemplos para configurar el controlador ODBC de Amazon Redshift y el nombre del origen de datos (DSN).

No le recomendamos utilizar el directorio de instalación del controlador ODBC de Amazon Redshift para los archivos de configuración. Los archivos de muestra del directorio instalados se presentan únicamente como ejemplo. Si vuelve a instalar el controlador ODBC de Amazon Redshift más adelante o actualiza a una versión más reciente, se sobrescribe el directorio de instalación. Perderá los cambios que haya realizado en los archivos del directorio de instalación.

Para evitarlo, copie el archivo amazon.redshiftodbc.ini en un directorio distinto al directorio de instalación. Si copia este archivo en el directorio principal del usuario, agregue un punto (.) al principio del nombre del archivo para convertirlo en un archivo oculto.

Para los archivos odbc.ini y odbcinst.ini, utilice los archivos de configuración en el directorio principal del usuario o cree nuevas versiones en otro directorio. De manera predeterminada, su sistema operativo Linux debe tener un archivo odbc.ini y un archivo odbcinst.ini en el directorio de inicio del usuario (/home/$USER o ~/.). Estos archivos predeterminados son archivos ocultos, que se indica con el punto (.) delante de cada nombre de archivo. Estos archivos solo se muestran cuando se utiliza el indicador -a para enumerar el contenido del directorio.

Cualquiera que sea la opción que elija para los archivos odbc.ini y odbcinst.ini, modifique los archivos para agregar información de configuración del controlador y DSN. Si selecciona crear archivos nuevos, también deberá configurar variables de entorno para especificar la ubicación de estos archivos de configuración.

De manera predeterminada, los administradores de controladores ODBC están configurados para utilizar versiones ocultas de los archivos de configuración odbc.ini y odbcinst.ini (denominados .odbc.ini y .odbcinst.ini) ubicados en el directorio de inicio. También están configurados para utilizar el archivo amazon.redshiftodbc.ini en el directorio de instalación del controlador. Si almacena estos archivos de configuración en otro lugar, establezca las variables de entorno que se describen a continuación para que el administrador de controladores pueda localizar los archivos.

Si utiliza UnixODBC, haga lo siguiente:

- Configure ODBCINI en la ruta completa y el nombre del archivo odbc.ini.
- Configure ODBCSYSINI en la ruta completa del directorio que contiene el archivo odbcinst.ini.

- Configure `AMAZONREDSHIFTODBCINI` en la ruta completa y el nombre del archivo `amazon.redshiftodbc.ini`.

A continuación, se muestra un ejemplo de cómo configurar los valores anteriores:

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftodbc.ini
```

Configuración de una conexión mediante un nombre de origen de datos (DSN) en Linux

Cuando se conecte al almacenamiento de datos mediante un nombre de origen de datos (DSN), configure el archivo `odbc.ini` para definir los nombres de origen de datos (DSN). Establezca las propiedades del archivo `odbc.ini` para crear un DSN que especifique la información de conexión para el almacén de datos.

En los sistemas operativos Linux, utilice el siguiente formato:

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbc.ini` con el controlador ODBC de 64 bits para sistemas operativos Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
```

```
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932Database=dev
locale=en-US
```

Configuración de una conexión sin un DSN en Linux

Para conectarse al almacén de datos a través de una conexión que no tenga DSN, defina el controlador en el archivo `odbcinst.ini`. A continuación, proporcione una cadena de conexión sin DSN en su aplicación.

En los sistemas operativos Linux, utilice el siguiente formato:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbcinst.ini` con el controlador ODBC de 64 bits para sistemas operativos Linux.

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbcx64/librsodbc64.so
```

Configuración de la autenticación

Con el fin de proteger los datos contra accesos no autorizados, los almacenes de datos de Amazon Redshift requieren la autenticación de todas las conexiones mediante credenciales de usuario.

En la siguiente tabla, se ilustran las opciones de conexión obligatorias y opcionales para cada método de autenticación que se puede utilizar para conectarse al controlador ODBC de Amazon Redshift versión 2.x:

Opciones de conexión obligatorias y opcionales del método de autenticación ODBC

Método de autenticación	Obligatoria	Opcional
Estándar	• Host • Puerto • Base de datos • UID • Password	
Perfil de IAM	• Host • Puerto • Base de datos • IAM • Perfil	• ID del clúster • Región • AutoCreate • EndpointURL • StsEndpointURL • InstanceProfile **Note** ClusterID y Region se deben configurar en el Host si no se configura n por separado.
Credenciales de IAM	• Host • Puerto • Base de datos • IAM • AccessKeyID • SecretAccessKey	• ID del clúster • Región • AutoCreate • EndpointURL • StsEndpointURL • SessionToken

Método de autenticación	Obligatoria	Opcional
		• UID **Note** ClusterID y Region se deben configurar en el Host si no se configuran por separado.
AD FS	• Host • Puerto • Base de datos • IAM • plugin_name • UID • Password • IdP_Host • IdP_Port	• ID del clúster • Región • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • loginToRp • SSL_Insecure **Note** ClusterID y Region se deben configurar en el Host si no se configuran por separado.

Método de autenticación	Obligatoria	Opcional
Azure AD	• Host • Puerto • Base de datos • IAM • plugin_name • UID • Password • IdP_Tenant • Client_ID • Client_Secret	• ID del clúster • Región • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter **Note** ClusterID y Region se deben configurar en el Host si no se configura n por separado.
JWT	• Host • Puerto • Base de datos • IAM • plugin_name • web_identity_token	• provider_name

Método de autenticación	Obligatoria	Opcional
Okta	• Host • Puerto • Base de datos • IAM • plugin_name • UID • Password • IdP_Host • App_Name • App_ID	• ID del clúster • Región • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role **Note** ClusterID y Region se deben configurar en el Host si no se configuran por separado.
Ping Federate	• Host • Puerto • Base de datos • IAM • plugin_name • UID • Password • IdP_Host • IdP_Port	• ID del clúster • Región • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • SSL_Insecure • partner_spid **Note** ClusterID y Region se deben configurar en el Host si no se configuran por separado.

Método de autenticación	Obligatoria	Opcional
Browser Azure AD	• Host • Puerto • Base de datos • IAM • plugin_name • IdP_Tenant • Client_ID • UID	• ID del clúster • Región • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port **Note** ClusterID y Region se deben configurar en el Host si no se configura n por separado.

Método de autenticación	Obligatoria	Opcional
Browser SAML	• Host • Puerto • Base de datos • IAM • plugin_name • login_url • UID	• ID del clúster • Región • AutoCreate • EndpointUrl • StsEndpointUrl • Preferred_Role • dbgroups_filter • IdP_Response_Timeout • listen_port **Note** ClusterID y Region se deben configurar en el Host si no se configura n por separado.
Perfil de autenticación	• Host • Puerto • Base de datos • AccessKeyID • SecretAccessKey	

Método de autenticación	Obligatoria	Opcional
Browser Azure AD OAUTH2	• Host • Puerto • Base de datos • IAM • plugin_name • IdP_Tenant • Client_ID • UID	• ID del clúster • Región • EndpointUrl • IdP_Response_Timeout • listen_port • scope • provider_name **Note** ClusterID y Region se deben configurar en el Host si no se configura n por separado.

Uso de un servicio de credenciales externo

Además de la compatibilidad integrada con AD FS, Azure AD y Okta, la versión para Windows del controlador ODBC de Amazon Redshift también admite otros servicios de credenciales. El controlador puede autenticar las conexiones mediante cualquier complemento de proveedor de credenciales basado en SAML de su elección.

Para configurar un servicio de credenciales externo en Windows:

1. Cree un perfil de IAM que especifique el complemento del proveedor de credenciales y otros parámetros de autenticación según sea necesario. El perfil debe estar codificado en ASCII y debe contener el siguiente par clave-valor, en el que `PluginPath` es la ruta completa a la aplicación del complemento:

   ```
   plugin_name = PluginPath
   ```

   Por ejemplo:

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

Para obtener más información sobre cómo crear un perfil, consulte Uso de un perfil de configuración en la Guía de administración de clústeres de Amazon Redshift.

2. Configure el controlador para que utilice este perfil. El controlador detecta y utiliza la configuración de autenticación especificada en el perfil.

Conversión de tipos de datos

El controlador ODBC versión 2.x de Amazon Redshift admite varios formatos de datos frecuentes, por lo que permite la conversión entre los tipos de datos de Amazon Redshift y SQL.

En la siguiente tabla, se enumeran los mapeos de tipos de datos admitidos.

Tipo de Amazon Redshift	Tipo de SQL
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
FECHA	SQL_TYPE_DATE
DECIMAL	SQL_NUMERIC
DOUBLE PRECISION	SQL_DOUBLE
GEOGRAPHY	SQL_ LONGVARBINARY
GEOMETRY	SQL_ LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR

Tipo de Amazon Redshift	Tipo de SQL
TEXT	SQL_LONGVARCHAR
TIME	SQL_TYPE_TIME
TIMETZ	SQL_TYPE_TIME
TIMESTAMP	SQL_TYPE_ TIMESTAMP
TIMESTAMPTZ	SQL_TYPE_ TIMESTAMP
VARBYTE	SQL_LONGVARBINARY
VARCHAR	SQL_VARCHAR

Configuración de las opciones del controlador ODBC

Puede utilizar las opciones de configuración del controlador para controlar el comportamiento del controlador ODBC de Amazon Redshift. Las opciones del controlador no distinguen entre mayúsculas y minúsculas.

En Microsoft Windows, por lo general, las opciones del controlador se configuran cuando configura un nombre de origen de datos (DSN). También puede establecer opciones de controlador en la cadena de conexión cuando se conecta mediante programación o agregando o cambiando claves del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Para obtener más información acerca de la configuración de un DSN, consulte Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.

En Linux, se establecen las opciones de configuración del controlador en los archivos `odbc.ini` y `amazon.redshiftodbc.ini`, como se describe en Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X. Las opciones de configuración establecidas en un archivo `amazon.redshiftodbc.ini` se aplican a todas las conexiones. No obstante, las opciones de configuración establecidas en un archivo `odbc.ini` son específicas de una conexión. Las opciones de configuración establecidas en `odbc.ini` tienen prioridad sobre las opciones de configuración establecidas en `amazon.redshiftodbc.ini`.

A continuación, se muestran las descripciones relativas a las opciones que puede especificar para la versión 2.x del controlador ODBC de Amazon Redshift:

AccessKeyID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave de acceso de IAM para el usuario o el rol. Si establece este parámetro, también debe especificar SecretAccessKey.

Este parámetro es opcional.

app_id

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID único proporcionado por Okta que se asocia a su aplicación de Amazon Redshift.

Este parámetro es opcional.

app_name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de la aplicación Okta que utiliza en la autenticación de la conexión con Amazon Redshift.

Este parámetro es opcional.

AuthProfile

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El perfil de autenticación utilizado para administrar la configuración de la conexión. Si establece este parámetro, también debe establecer AccessKeyID y SecretAccessKey.

Este parámetro es opcional.

AuthType

- Valor predeterminado: estándar
- Tipo de datos: cadena

Esta opción especifica el modo de autenticación que el controlador utiliza al configurar un DSN mediante el cuadro de diálogo Configuración de DSN del controlador ODBC de Amazon Redshift:

- Estándar: autenticación estándar mediante su nombre de usuario y contraseña de Amazon Redshift.
- Perfil de AWS: autenticación de IAM mediante un perfil.
- Credenciales de AWS IAM: autenticación de IAM mediante credenciales de IAM.
- Proveedor de identidades: AD FS: autenticación de IAM mediante Active Directory Federation Services (AD FS).
- Proveedor de identidad: complemento de autenticación: complemento de autorización que acepta un token de Identity Center (IdC) o token de identidad basados en JSON (JWT) de OpenID Connect (OIDC) de cualquier proveedor de identidad web vinculado al IdC.
- Proveedor de identidades: Azure AD: autenticación de IAM mediante un portal de Azure AD.
- Proveedor de identidades: JWT: autenticación de IAM mediante un JSON Web Token (JWT).
- Proveedor de identidades: Okta: autenticación de IAM mediante Okta.
- Proveedor de identidades: PingFederate: autenticación de IAM mediante PingFederate.

Esta opción solo está disponible cuando configura un DSN mediante el cuadro de diálogo Configuración de DSN del controlador ODBC de Amazon Redshift en el controlador de Windows. Al configurar una conexión mediante una cadena de conexión o una máquina que no sea de Windows, el controlador determina automáticamente si se debe usar la autenticación estándar, de perfil de AWS o de credenciales de AWS IAM según las credenciales especificadas. Para utilizar un proveedor de identidades, debe configurar la propiedad plugin_name.

Este parámetro es obligatorio.

AutoCreate

- Valor predeterminado: 0
- Tipos de datos: booleano

Un booleano que especifica si el controlador crea un usuario nuevo cuando el usuario especificado no existe.

- 1 | TRUE: si el usuario especificado por el UID no existe, el controlador crea un usuario nuevo.
- 0 | FALSE: el controlador no crea un usuario nuevo. Si el usuario especificado no existe, se produce un error en la autenticación.

Este parámetro es opcional.

CaFile

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La ruta de acceso al archivo de certificado de CA que se utiliza para algunas formas de autenticación de IAM.

Este parámetro solo está disponible en Linux.

Este parámetro es opcional.

client_id

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de cliente asociado a la aplicación de Amazon Redshift en Azure AD.

Este parámetro es necesario si la autenticación se realiza a través del servicio Azure AD.

client_ secret

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave secreta asociada a la aplicación de Amazon Redshift en Azure AD.

Este parámetro es necesario si la autenticación se realiza a través del servicio Azure AD.

ClusterId

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del clúster de Amazon Redshift al que desea conectarse. Se utiliza en la autenticación de IAM. El ID de clúster no se especifica en el parámetro Server (Servidor).

Este parámetro es opcional.

compression

- Valor predeterminado: desconectado
- Tipo de datos: cadena

Método de compresión utilizado para la comunicación mediante protocolo de conexión entre el servidor de Amazon Redshift y el cliente o el controlador.

Puede especificar los valores siguientes:

- lz4: establece el método de compresión utilizado para la comunicación mediante protocolo de conexión con Amazon Redshift a `lz4`.
- zstd: establece el método de compresión utilizado para la comunicación mediante protocolo de conexión con Amazon Redshift a `zstd`.
- off: no utiliza la compresión para la comunicación mediante protocolo de conexión con Amazon Redshift.

Este parámetro es opcional.

Base de datos

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de la base de datos de Amazon Redshift a la que desea obtener acceso.

Este parámetro es obligatorio.

DatabaseMetadataCurrentDbOnly

- Valor predeterminado: 1
- Tipos de datos: booleano

Un booleano que especifica si el controlador devuelve metadatos de varias bases de datos y clústeres.

- 1 | TRUE: el controlador solo devuelve metadatos de la base de datos actual.
- 0 | FALSE. El controlador devuelve metadatos de varios clústeres y bases de datos de Amazon Redshift.

Este parámetro es opcional.

dbgroups_filter

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La expresión regular que puede especificar para filtrar DbGroups que se reciben de la respuesta SAML a Amazon Redshift cuando se utilizan los tipos de autenticación Azure, Browser Azure y Browser SAML.

Este parámetro es opcional.

Controlador

- Valor predeterminado: controlador ODBC de Amazon Redshift (x64)
- Tipo de datos: cadena

El nombre del controlador. El único valor admitido es Amazon Redshift ODBC Driver (x64) (Controlador ODBC de Amazon Redshift [x64]).

Este parámetro es necesario si no establece el DSN.

DSN

- Valor predeterminado: ninguno

- Tipo de datos: cadena

El nombre del origen de datos del controlador. La aplicación especifica el DSN en la API de SQLDriverConnect.

Este parámetro es necesario si no establece el Driver (Controlador).

EndpointUrl

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El punto de conexión de anulación que se utiliza para comunicarse con Amazon Redshift Coral Service para la autenticación de IAM.

Este parámetro es opcional.

ForceLowercase

- Valor predeterminado: 0
- Tipos de datos: booleano

Un valor booleano que especifica si el controlador escribe en minúsculas todos los DbGroups que se envían desde el proveedor de identidades a Amazon Redshift cuando se utiliza la autenticación de inicio de sesión único.

- 1 | TRUE: el controlador escribe en minúsculas todos los DbGroups que se envían desde el proveedor de identidades.
- 0 | FALSE: el controlador no modifica los DbGroups.

Este parámetro es opcional.

group_federation

- Valor predeterminado: 0
- Tipos de datos: booleano

Un valor booleano que especifica si la API `getClusterCredentialsWithIAM` se utiliza para obtener credenciales de clúster temporales en los clústeres aprovisionados. Esta opción permite a los usuarios de IAM integrarse con los roles de base de datos de Redshift en los clústeres aprovisionados. Tenga en cuenta que esta opción no se aplica a los espacios de nombres de Redshift sin servidor.

- 1 | VERDADERO: el controlador utiliza la API `getClusterCredentialsWithIAM` para obtener credenciales de clúster temporales en los clústeres aprovisionados.
- 0 | FALSO: el controlador utiliza la API `getClusterCredentials` predeterminada para obtener credenciales de clúster temporales en los clústeres aprovisionados.

Este parámetro es opcional.

https_proxy_host

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de host o la dirección IP del servidor proxy a través del cual desea pasar los procesos de autenticación de IAM.

Este parámetro es opcional.

https_proxy_password

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La contraseña que utiliza para obtener acceso al servidor proxy. Se utiliza para la autenticación de IAM.

Este parámetro es opcional.

https_proxy_port

- Valor predeterminado: ninguno
- Tipo de datos: entero

El número del puerto que el servidor proxy utiliza para escuchar las conexiones del cliente. Se utiliza para la autenticación de IAM.

Este parámetro es opcional.

https_proxy_username

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de usuario que utiliza para obtener acceso al servidor proxy. Se utiliza para la autenticación de IAM.

Este parámetro es opcional.

IAM

- Valor predeterminado: 0
- Tipos de datos: booleano

Un booleano que especifica si el controlador utiliza un método de autenticación de IAM para autenticar la conexión.

- 1 | TRUE: el controlador utiliza uno de los métodos de autenticación de IAM (mediante un par de clave de acceso y clave secreta, un perfil o un servicio de credenciales).
- 0 | FALSE. El controlador utiliza la autenticación estándar (con el nombre de usuario y la contraseña de la base de datos).

Este parámetro es opcional.

identity_namespace

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Es el espacio de nombres de identidad que se utiliza al autenticarse con IdpTokenAuthPlugin. Ayuda a Redshift a determinar qué instancia de IAM Identity Center utilizar.

Si solo hay una instancia del IAM Identity Center o si se ha establecido el espacio de nombres de identidad predeterminado, este parámetro es opcional; de lo contrario, es obligatorio.

idp_host

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El alojamiento del IdP (proveedor de identidad) que utiliza para la autenticación en Amazon Redshift.

Este parámetro es opcional.

idp_port

- Valor predeterminado: ninguno
- Tipo de datos: entero

El puerto del IdP (proveedor de identidades) que utiliza para la autenticación en Amazon Redshift. Según el puerto que haya seleccionado al crear, modificar o migrar el clúster, se permitirá el acceso al puerto seleccionado.

Este parámetro es opcional.

Idp_response_timeout

- Valor predeterminado: 120
- Tipo de datos: entero

La cantidad de segundos que el controlador espera para obtener la respuesta SAML del proveedor de identidades cuando se utilizan los servicios Azure AD o SAML a través de un complemento del navegador.

Este parámetro es opcional.

idp_tenant

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El ID de inquilino de Azure AD asociado a la aplicación de Amazon Redshift.

Este parámetro es necesario si la autenticación se realiza a través del servicio Azure AD.

idp_use_https_proxy

- Valor predeterminado: 0
- Tipos de datos: booleano

Un booleano que especifica si el controlador pasa los procesos de autenticación de los proveedores de identidades (IdP) a través de un servidor proxy.

- 1 | TRUE: el controlador pasa los procesos de autenticación de los IdP a través de un servidor proxy.
- 0 | FALSE. El controlador no pasa los procesos de autenticación de los IdP a través de un servidor proxy.

Este parámetro es opcional.

InstanceProfile

- Valor predeterminado: 0
- Tipos de datos: booleano

Un booleano que especifica si el controlador utiliza el perfil de instancia de Amazon EC2 cuando está configurado para usar un perfil para la autenticación.

- 1 | TRUE: el controlador utiliza el perfil de instancia de Amazon EC2.
- 0 | FALSE. El controlador utiliza el perfil de roles encadenados especificado en la opción Nombre de perfil (Profile [Perfil]) en su lugar.

Este parámetro es opcional.

KeepAlive

- Valor predeterminado: 1
- Tipos de datos: booleano

Un booleano que especifica si el controlador utiliza keepalives de TCP para evitar que se agote el tiempo de espera en las conexiones.

- 1el controlador utiliza keepalives de TCP para evitar que se agote el tiempo de espera en las conexiones.
- 0 | FALSE. El controlador no utiliza keepalives de TCP.

Este parámetro es opcional.

KeepAliveCount

- Valor predeterminado: 0
- Tipo de datos: entero

La cantidad de paquetes keepalive de TCP que se pueden perder antes de que se considere que se interrumpió la conexión. Cuando este parámetro está establecido en 0, el controlador utiliza el valor predeterminado del sistema para esta configuración.

Este parámetro es opcional.

KeepAliveInterval

- Valor predeterminado: 0
- Tipo de datos: entero

La cantidad de segundos entre cada retransmisión de keepalive de TCP. Cuando este parámetro está establecido en 0, el controlador utiliza el valor predeterminado del sistema para esta configuración.

Este parámetro es opcional.

KeepAliveTime

- Valor predeterminado: 0
- Tipo de datos: entero

La cantidad de segundos de inactividad antes de que el controlador envíe un paquete keepalive de TCP. Cuando este parámetro está establecido en 0, el controlador utiliza el valor predeterminado del sistema para esta configuración.

Este parámetro es opcional.

listen_port

- Valor predeterminado: 7890
- Tipo de datos: entero

El puerto que utiliza el controlador para obtener la respuesta SAML del proveedor de identidades cuando se usan los servicios SAML o Azure AD a través de un complemento del navegador.

Este parámetro es opcional.

login_url

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La dirección URL del recurso en el sitio web del proveedor de identidades cuando se utiliza el complemento de navegador SAML genérico.

Este parámetro es necesario si la autenticación se realiza con el servicio Azure AD o SAML a través de un complemento del navegador.

loginToRp

- Valor predeterminado: urn:amazon:webservices
- Tipo de datos: cadena

La relación de confianza para usuario autenticado que desea utilizar para el tipo de autenticación de AD FS.

Esta cadena es opcional.

LogLevel

- Valor predeterminado: 0

- Tipo de datos: entero

Utilice esta propiedad para habilitar o deshabilitar el registro en el controlador y especificar la cantidad de detalles incluidos en los archivos de registro. Le recomendamos que habilite el registro solo durante el tiempo suficiente para detectar un problema, ya que el registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Establezca la propiedad en uno de los siguientes valores:

- 0: OFF. Desactive todos los registros.
- 1: ERROR. Registra eventos de errores que podrían hacer que el controlador continúe ejecutándose, pero genere un error.
- 2: API_CALL. Registra las llamadas a funciones de la API ODBC con valores de argumento de función.
- 3: INFO. Registra información general que describe el progreso del controlador.
- 4: MSG_PROTOCOL. Registra información detallada del protocolo de mensajes del controlador.
- 5: DEBUG. Registra toda la actividad del controlador.
- 6: DEBUG_APPEND. Siga agregando registros de todas las actividades del controlador.

Cuando se habilita el registro, el controlador crea los siguientes archivos de registro en la ubicación que especifica en la propiedad LogPath:

- Un archivo `redshift_odbc.log.1` que registra la actividad del controlador que tiene lugar durante el protocolo de enlace de una conexión.
- Un archivo `redshift_odbc.log` para todas las actividades del controlador después de establecer una conexión a la base de datos.

Este parámetro es opcional.

LogPath

- Valor predeterminado: el directorio TEMP específico del sistema operativo
- Tipo de datos: cadena

La ruta completa a la carpeta en la que el controlador guarda los archivos de registro cuando LogLevel es superior a 0.

Este parámetro es opcional.

Min_TLS

- Valor predeterminado: el valor mínimo.
- Tipo de datos: cadena

La versión mínima de TLS/SSL que el controlador permite que el almacén de datos utilice para cifrar las conexiones. Por ejemplo, si se especifica TLS 1.3, no se puede utilizar TLS 1.2 para cifrar las conexiones.

Min_TLS acepta los valores siguientes:

- 1.2: La conexión debe utilizar al menos TLS 1.2. Esta es la versión de TLS mínima requerida para las conexiones de Amazon Redshift.
- 1.3: La conexión debe utilizar al menos TLS 1.3. Nosotros recomendamos TLS 1.3.

Este parámetro es opcional.

partner_spid

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El valor del SPID (ID del proveedor de servicios) del socio que se utilizará cuando se autentique la conexión mediante el servicio PingFederate.

Este parámetro es opcional.

Contraseña | PWS

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La contraseña correspondiente al nombre de usuario proporcionado en el campo Usuario (UID | Usuario | LogonID).

Este parámetro es opcional.

plugin_name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del complemento del proveedor de credenciales que desea utilizar para la autenticación.

Se admiten los siguientes valores:

- `ADFS`: utilice Active Federation Services para la autenticación.
- `AzureAD`: utilice el servicio de Microsoft Azure Active Directory (AD) para la autenticación.
- `BrowserAzureAD`: utilice un complemento del navegador del servicio de Microsoft Azure Active Directory (AD) para la autenticación.
- `BrowserSAML`: utilice un complemento del navegador de los servicios SAML, como Okta o Ping, para la autenticación.
- `IdpTokenAuthPlugin`: complemento de autorización que acepta un token de Identity Center (IdC) o token de identidad basados en JSON (JWT) de OpenID Connect (OIDC) de cualquier proveedor de identidad web vinculado al IdC.
- `JWT`: utilice un JSON Web Token (JWT) para la autenticación.
- `Ping`: utilice el servicio PingFederate para la autenticación.
- `Okta`: utilice el servicio Okta para la autenticación.

Este parámetro es opcional.

Puerto | PortNumber

- Valor predeterminado: 5439
- Tipo de datos: entero

El número del puerto TCP que el servidor de Amazon Redshift utiliza para escuchar las conexiones del cliente.

Este parámetro es opcional.

preferred_role

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El rol que desea asumir durante la conexión a Amazon Redshift. Se utiliza para la autenticación de IAM.

Este parámetro es opcional.

Perfil

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre del perfil de usuario de AWS utilizado para autenticarse en Amazon Redshift.

- Si Usar el parámetro del perfil de instancia (la propiedad InstanceProfile) se establece en 1 | TRUE, esa configuración tiene prioridad y el controlador utiliza el perfil de instancia de Amazon EC2 en su lugar.
- La ubicación predeterminada del archivo de credenciales que contiene los perfiles es `~/.aws/Credentials`. La variable de entorno `AWS_SHARED_CREDENTIALS_FILE` se puede utilizar para apuntar a un archivo de credenciales diferente.

Este parámetro es opcional.

provider_name

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El proveedor de autenticación creado por el usuario mediante la consulta CREATE IDENTITY PROVIDER. Se utiliza en la autenticación nativa de Amazon Redshift.

Este parámetro es opcional.

ProxyHost

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de host o la dirección IP del servidor proxy a través del que desea conectarse.

Este parámetro es opcional.

ProxyPort

- Valor predeterminado: ninguno
- Tipo de datos: entero

El número del puerto que el servidor proxy utiliza para escuchar las conexiones del cliente.

Este parámetro es opcional.

ProxyPwd

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La contraseña que utiliza para obtener acceso al servidor proxy.

Este parámetro es opcional.

ProxyUid

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de usuario que utiliza para obtener acceso al servidor proxy.

Este parámetro es opcional.

ReadOnly

- Valor predeterminado: 0

- Tipos de datos: booleano

Un booleano que especifica si el controlador se encuentra en modo de solo lectura.

- 1l | TRUE: a conexión se encuentra en modo de solo lectura y no se puede escribir en el almacén de datos.
- 0la conexión no se encuentra en modo de solo lectura y se puede escribir en el almacén de datos.

Este parámetro es opcional.

región

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La región de AWS en la que se encuentra el clúster.

Este parámetro es opcional.

SecretAccessKey

- Valor predeterminado: ninguno
- Tipo de datos: cadena

La clave secreta de IAM para el usuario o el rol. Si establece este parámetro, también debe establecer AccessKeyID.

Este parámetro es opcional.

SessionToken

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El token de sesión temporal de IAM asociado con el rol de IAM que se está utilizando para la autenticación.

Este parámetro es opcional.

Servidor | HostName | Host

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El servidor de punto de conexión al que desea conectarse.

Este parámetro es obligatorio.

ssl_insecure

- Valor predeterminado: 0
- Tipos de datos: booleano

Un booleano que especifica si el controlador verifica la autenticidad del certificado de servidor del IdP.

- 1 | TRUE: el controlador no verifica la autenticidad del certificado de servidor del IdP.
- 0 | FALSE: el controlador verifica la autenticidad del certificado de servidor del IdP.

Este parámetro es opcional.

SSLMode

- Valor predeterminado: `verify-ca`
- Tipo de datos: cadena

El modo de verificación del certificado SSL que se utiliza para establecer la conexión a Amazon Redshift. Se admiten los siguientes valores:

- `verify-full`: conéctese solo con SSL, una entidad de certificación de confianza y un nombre de servidor que coincida con el certificado.
- `verify-ca`: conéctese solo con SSL y una entidad de certificación de confianza.
- `require`: conéctese solo con SSL.
- `prefer`: conéctese con SSL, si está disponible. De lo contrario, conéctese sin utilizar SSL.
- `allow`: de forma predeterminada, conéctese sin usar SSL. Si el servidor requiere conexiones SSL, utilice SSL.

- `disable`: conéctese sin utilizar SSL.

Este parámetro es opcional.

StsConnectionTimeout

- Valor predeterminado: 0
- Tipo de datos: entero

El tiempo de espera máximo de las conexiones de IAM, en segundos. Si se establece en 0 o no se especifica, el controlador espera 60 segundos para cada llamada a AWS STS.

Este parámetro es opcional.

StsEndpointUrl

- Valor predeterminado: ninguno
- Tipo de datos: cadena

Esta opción especifica el punto de conexión de anulación que se utiliza para comunicarse con AWS Security Token Service (AWS STS).

Este parámetro es opcional.

UID | Usuario | LogonID

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El nombre de usuario que utiliza para obtener acceso al servidor de Amazon Redshift.

Este parámetro es necesario si utiliza la autenticación de base de datos.

web_identity_token

- Valor predeterminado: ninguno
- Tipo de datos: cadena

El token de OAUTH proporcionado por el proveedor de identidades. Se utiliza en el complemento JWT.

Este parámetro es necesario si establece el parámetro plugin_name en BasicJwtCredentialsProvider.

Versiones anteriores del controlador ODBC

Descargue una versión anterior del controlador ODBC versión 2.x de Amazon Redshift solo si su herramienta requiere una versión específica del controlador.

Usar versiones anteriores del controlador ODBC para Microsoft Windows

A continuación, se muestran las versiones anteriores del controlador ODBC versión 2.x de Amazon Redshift para Microsoft Windows:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC64-2.0.1.0.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC64-2.0.0.11.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC64-2.0.0.9.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC64-2.0.0.8.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC64-2.0.0.7.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC64-2.0.0.6.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC64-2.0.0.5.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC64-2.0.0.3.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.msi

Usar versiones anteriores del controlador ODBC para Linux

A continuación, se muestran las versiones anteriores del controlador ODBC versión 2.x de Amazon Redshift para Linux:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC-64-bit-2.0.1.0.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC-64-bit-2.0.0.11.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC-64-bit-2.0.0.9.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC-64-bit-2.0.0.8.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC-64-bit-2.0.0.7.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC-64-bit-2.0.0.6.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC-64-bit-2.0.0.5.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC-64-bit-2.0.0.3.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC-64-bit-2.0.0.1.x86_64.rpm

Configuración de una conexión ODBC

Puede utilizar una conexión ODBC para conectarse a su clúster de Amazon Redshift desde distintas aplicaciones y herramientas de cliente SQL de terceros. Para hacerlo, configure la conexión en su equipo cliente o en una instancia de Amazon EC2. Si su equipo cliente es compatible con JDBC, puede elegir utilizar ese tipo de conexión, en lugar de una conexión ODBC ya que JDBC es más fácil de configurar. No obstante, si su herramienta de cliente no es compatible con JDBC, siga los pasos de esta sección para configurar una conexión ODBC.

Amazon Redshift proporciona controladores ODBC de 64 bit para los sistemas operativos Linux, Windows y macOS X. Los controladores ODBC de 32 bits se suspenden. No se publicarán más actualizaciones, excepto las revisiones de seguridad urgentes.

Para obtener la información más reciente acerca de la funcionalidad del controlador ODBC y los requisitos previos, consulte Notas de la versión del controlador ODBC de Amazon Redshift.

Para obtener información acerca de la instalación y la configuración de los controladores ODBC de Amazon Redshift, consulte la Guía de instalación y configuración de controladores ODBC de Amazon Redshift.

Si desea utilizar una conexión ODBC, siga los pasos siguientes.

Temas

- Obtención del URL de ODBC para su clúster
- Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows
- Instalación del controlador ODBC de Amazon Redshift en Linux
- Instalación del controlador ODBC de Amazon Redshift en macOS X
- Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X
- Configurar las opciones del controlador ODBC
- Versiones anteriores del controlador ODBC

Obtención del URL de ODBC para su clúster

Amazon Redshift muestra la URL de ODBC de su clúster en la consola de Amazon Redshift. Esta dirección URL contiene la información que necesita para configurar la conexión entre su equipo cliente y la base de datos.

Una URL de ODBC tiene el siguiente formato:

```
Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=passwor
```

Los campos del formato mostrado anteriormente tienen los siguientes valores.

Campo	Valor
`Driver`	Nombre del controlador ODBC de 64 bits que se va a utilizar: Amazon Redshift (x64). Nombre del controlador ODBC de 32 bits: Amazon Redshift (x86).
`Server`	El punto de conexión del clúster de Amazon Redshift.
`Database`	Base de datos que creó para su clúster.

Campo	Valor
UID	Nombre de usuario de una cuenta de usuario que tiene permiso para conectarse a la base de datos. Este valor es un permiso de la base de datos, no un permiso de Amazon Redshift, aunque puede utilizar la cuenta de usuario administrador que configuró cuando lanzó el clúster.
PWD	Contraseña de la cuenta de usuario para conectarse a la base de datos.
Port	Número de puerto que especificó cuando lanzó el clúster. Si tiene un firewall, asegúrese de que este puerto esté abierto para poder usarlo.

Los campos de las tablas anteriores pueden contener los siguientes caracteres especiales:

```
[]{}(),;?*=!@
```

Si utiliza estos caracteres especiales, debe incluir el valor entre llaves. Por ejemplo, el valor de contraseña `Your;password123` en una cadena de conexión se representa como `PWD={Your;password123};`.

Como los pares `Field=value` están separados por punto y coma, la combinación de `}` y `;` con cualquier número de espacios intermedios se considera el final de un par `Field={value};`. Le recomendamos que evite la secuencia `};` en los valores de campo. Por ejemplo, si establece el valor de su contraseña a `PWD={This is a passwor} ;d};`, su contraseña sería `This is a passwor} ;` y la URL generaría un error.

A continuación, se muestra un ejemplo de la URL de ODBC.

```
Driver={Amazon Redshift (x64)};
                    Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com;
                    Database=dev;
                    UID=adminuser;
                    PWD=insert_your_admin_user_password_here;
                    Port=5439
```

Para obtener información acerca de cómo crear su propia conexión ODBC, consulte Obtención de la cadena de conexión a su clúster.

Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows

Requisitos del sistema

Debe instalar el controlador ODBC de Amazon Redshift en los equipos cliente que tienen acceso a un almacenamiento de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir una lista de requisitos mínimos de sistema: Para obtener información acerca de los requisitos mínimos del sistema, consulte la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Instalación del controlador de Amazon Redshift en sistemas operativos Windows

Utilice el procedimiento siguiente para descargar los controladores ODBC de Amazon Redshift para los sistemas operativos Windows. Utilice un controlador diferente solo si está ejecutando una aplicación de terceros que está certificada para usarse con Amazon Redshift y que requiere un controlador específico.

Pasos para instalar el controlador ODBC de

1. Descargue alguno de los siguientes controladores, según la arquitectura de sistema de su aplicación o su herramienta de cliente SQL:

   - Versión 1.5.9 del controlador ODBC de 64 bits

     El nombre de este controlador es Amazon Redshift (x64).
   - Versión 1.4.52 del controlador ODBC de 32 bits

     El nombre de este controlador es Amazon Redshift (x86). Los controladores ODBC de 32 bits se suspenden. No se publicarán más actualizaciones, excepto las revisiones de seguridad urgentes.

   > **Note**
   >
   > Descargue el paquete MSI que corresponde a la arquitectura de sistema de su aplicación o su herramienta de cliente SQL. Por ejemplo, si su herramienta de cliente SQL es de 64 bits, instale el controlador de 64 bits.

A continuación, descargue y revise el Acuerdo de licencia del controlador ODBC y JDBC de Amazon Redshift.

2. Haga doble clic en el archivo .msi y, luego, siga los pasos en el asistente para instalar el controlador.

Creación de una entrada de sistema DSN para una conexión ODBC en Microsoft Windows

Después de descargar e instalar el controlador ODBC, agregue una entrada de nombre de origen de datos (DSN) al equipo cliente o a la instancia de Amazon EC2. Las herramientas de cliente SQL utilizan este origen de datos para conectarse a la base de datos de Amazon Redshift.

Se recomienda crear un DSN del sistema en lugar de un DSN de usuario. Algunas aplicaciones cargan los datos con una cuenta de usuario diferente. Es posible que estas aplicaciones no puedan detectar DSN de usuario que se crean en otra cuenta de usuario.

> **Note**
>
> Para la autenticación con credenciales de AWS Identity and Access Management (IAM) o credenciales de proveedor de identidad (IdP), se requieren pasos adicionales. Para obtener más información, consulte Configurar una conexión JDBC u ODBC para usar credenciales de IAM.

Para obtener información acerca de cómo crear una entrada DSN del sistema, consulte la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Para crear una entrada DSN del sistema para una conexión ODBC en Windows

1. En el menú Start (Inicio), abra ODBC Data Sources (Orígenes de datos ODBC).

   Asegúrese de elegir el Administrador de orígenes de datos ODBC que tenga el mismo valor de bits que la aplicación cliente que está utilizando para conectarse a Amazon Redshift.
2. En el Administrador de orígenes de datos ODBC, elija la pestaña Driver (Controlador) y busque la carpeta del controlador:

   - Controlador ODBC de Amazon Redshift (64 bits)
   - Controlador ODBC de Amazon Redshift (32 bits)

3. Elija la pestaña System DSN (DSN de sistema) para configurar el controlador para todos los usuarios del equipo o la pestaña User DSN (DSN de usuario) si para configurar solamente el controlador para la cuenta de usuario.
4. Elija Añadir. Se abrirá la ventana Create New Data Source (Crear nuevo origen de datos).
5. Elija el controlador ODBC de Amazon Redshift y, a continuación, elija Finish (Finalizar). Se abrirá la ventana Amazon Redshift ODBC Driver DSN Setup (Configuración de DSN del controlador ODBC de Amazon Redshift).
6. En Connection Settings (Configuración de conexión), escriba la siguiente información:

   Nombre de origen de datos

   Escriba un nombre para el origen de datos. Puede usar cualquier nombre que desee para identificar el origen de datos más adelante cuando cree la conexión al clúster. Por ejemplo, si siguió la Guía de introducción a Amazon Redshift, podría escribir `examplecluserdsn` para que le sea más fácil recordar el clúster que asocia a este DSN.

   Server

   Especifique el punto de conexión para su clúster de Amazon Redshift. Puede encontrar esta información en la consola de Amazon Redshift en la página de detalles del clúster. Para obtener más información, consulte Configuración de conexiones en Amazon Redshift.

   Puerto

   Escriba el número de puerto que usa la base de datos. Utilice el puerto que se configuró para el clúster en el momento del lanzamiento o la modificación.

   Base de datos

   Introduzca el nombre de la base de datos de Amazon Redshift. Si ha lanzado el clúster sin especificar un nombre de base de datos, escriba *dev*. De lo contrario, utilice el nombre que eligió durante el proceso de inicio. Si siguió la Guía de introducción a Amazon Redshift, ingrese *dev*.
7. En Authentication (Autenticación), especifique las opciones de configuración para configurar la autenticación de IAM o estándar. Para obtener información acerca de las opciones de autenticación, consulte “Configuración de la autenticación en Windows” en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.
8. En SSL Settings (Configuración de SSL), especifique un valor para el siguiente campo:

Autenticación SSL

Elija un modo para controlar la Capa de conexión segura (SSL). En un entorno de prueba, podría usar `prefer`. No obstante, para entornos de producción y cuando se requiera un intercambio seguro de datos, use `verify-ca` o `verify-full`. Para obtener más información acerca del uso de SSL en Windows, consulte “Configuración de la verificación SSL en Windows” en la Guía de instalación y configuración de conectores de ODBC de Amazon Redshift.

9. En Additional Options (Opciones adicionales), especifique las opciones sobre cómo devolver los resultados de la consulta a la herramienta o aplicación cliente SQL. Para obtener más información, consulte “Configuración de opciones adicionales en Windows” en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.
10. En Logging Options (Opciones de registro), especifique valores para la opción de registro. Para obtener más información, consulte “Configuración de opciones de registro en Windows” en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

    A continuación, seleccione OK (Aceptar).
11. En Data Type Options (Opciones de tipo de datos), especifique valores para los tipos de datos. Para obtener más información, consulte “Configuración de opciones de tipos de datos en Windows” en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

    A continuación, seleccione OK (Aceptar).
12. Seleccione Probar. Si el equipo cliente puede conectarse a la base de datos de Amazon Redshift, verá el siguiente mensaje: Connection successful (Conexión realizada correctamente).

    Si el equipo cliente no puede conectarse a la base de datos, puede solucionar los posibles problemas. Para obtener más información, consulte Solución de problemas de conexión en Amazon Redshift.
13. Configure las conexiones keepalive de TCP en Windows para evitar que se agote el tiempo de espera en las conexiones. Para obtener información acerca de cómo configurar keepalives de TCP en Windows, consulte la Guía de instalación y configuración de conectores de ODBC de Amazon Redshift.
14. Para ayudar a solucionar problemas, configure el registro. Para obtener información acerca de cómo configurar los registros en Windows, consulte la Guía de instalación y configuración de conectores de ODBC de Amazon Redshift.

Instalación del controlador ODBC de Amazon Redshift en Linux

Requisitos del sistema

Debe instalar el controlador ODBC de Amazon Redshift en los equipos cliente que tienen acceso a un almacenamiento de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir una lista de requisitos mínimos de sistema: Para obtener información acerca de los requisitos mínimos del sistema, consulte la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Instalación del controlador de Amazon Redshift en sistemas operativos Linux

Siga los pasos en esta sección para descargar e instalar los controladores ODBC de Amazon Redshift en una distribución Linux compatible. El proceso de instalación instala los archivos del controlador en los siguientes directorios:

- `/opt/amazon/redshiftodbc/lib/64` (para el controlador de 64 bits)
- `/opt/amazon/redshiftodbc/ErrorMessages`
- `/opt/amazon/redshiftodbc/Setup`
- `/opt/amazon/redshiftodbc/lib/32` (para el controlador de 32 bits)

Para instalar el controlador ODBC de Amazon Redshift

1. Descargue alguno de los siguientes controladores, según la arquitectura de sistema de su aplicación o su herramienta de cliente SQL:

   - Versión 1.5.9 del controlador RPM de 64 bits
   - Versión 1.5.9 del controlador Debian de 64 bits
   - Versión 1.4.52 del controlador RPM de 32 bits
   - Versión 1.4.52 del controlador Debian de 32 bits

   El nombre de cada uno de estos controladores es el controlador ODBC de Amazon Redshift. Los controladores ODBC de 32 bits se suspenden. No se publicarán más actualizaciones, excepto las revisiones de seguridad urgentes.

> **Note**
>
> Descargue el paquete que corresponde a la arquitectura de sistema de su aplicación o su herramienta de cliente SQL. Por ejemplo, si su herramienta de cliente es de 64 bits, instale un controlador de 64 bits.

A continuación, descargue y revise el Acuerdo de licencia del controlador ODBC y JDBC de Amazon Redshift.

2. Vaya a la ubicación en la que descargó el paquete y, a continuación, ejecute alguno de los siguientes comandos. Utilice el comando que corresponda a su distribución Linux.

   - En los sistemas operativos RHEL y CentOS , ejecute el siguiente comando.

     ```
     yum --nogpgcheck localinstall RPMFileName
     ```

     Reemplace *RPMFileName* por el nombre de archivo del paquete RPM. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 64 bits.

     ```
     yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
     ```

   - En SLES, ejecute el siguiente comando.

     ```
     zypper install RPMFileName
     ```

     Reemplace *RPMFileName* por el nombre de archivo del paquete RPM. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 64 bits.

     ```
     zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
     ```

   - En Debian, ejecute el siguiente comando.

     ```
     sudo apt install ./DEBFileName.deb
     ```

     Sustituya *DEBFileName.deb* por el nombre del archivo del paquete Debian. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 64 bits.

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

> **Important**
>
> Cuando haya terminado de instalar los controladores, configúrelos para usarlos en su sistema. Para obtener más información acerca de la configuración de los controladores, consulte Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X.

Instalación del controlador ODBC de Amazon Redshift en macOS X

Requisitos del sistema

Debe instalar el controlador en los equipos cliente que tienen acceso a un almacenamiento de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir una lista de requisitos mínimos de sistema: Para obtener información acerca de los requisitos mínimos del sistema, consulte la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Instalación del controlador ODBC de Amazon Redshift en macOS X

Siga los pasos de esta sección para descargar e instalar el controlador ODBC de Amazon Redshift en una versión compatible con macOS X. Con el proceso de instalación, se instalan los archivos del controlador en los siguientes directorios:

- `/opt/amazon/redshift/lib/universal`
- `/opt/amazon/redshift/ErrorMessages`
- `/opt/amazon/redshift/Setup`

Para instalar el controlador ODBC de Amazon Redshift en macOS X

1. Si el sistema macOS X utiliza la arquitectura Intel, descargue el controlador Intel para macOS X versión 1.5.9. Si el sistema usa la arquitectura ARM, descargue el controlador ARM para macOS X versión 1.5.9. En ambos casos, el nombre de este controlador es el controlador ODBC de Amazon Redshift.

A continuación, descargue y revise el Acuerdo de licencia del controlador ODBC y JDBC de Amazon Redshift.

2. Haga doble clic en AmazonRedshiftODBC.dmg para montar la imagen del disco.
3. Haga doble clic en AmazonRedshiftODBC.pkg para ejecutar el instalador.
4. Siga los pasos del instalador para completar el proceso de instalación del controlador. Para llevar a cabo la instalación, acepte los términos del acuerdo de licencia.

> **Important**
>
> Cuando haya terminado de instalar el controlador, configúrelo para usarlo en su sistema. Para obtener más información acerca de la configuración de los controladores, consulte Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X.

Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X

En los sistemas operativos Linux y Mac OS X, debe utilizar un administrador de controlador ODBC para configurar la conexión ODBC. Los administradores del controlador ODBC usan archivos de configuración para definir y configurar los controladores y el origen de datos de ODBC. El administrador del controlador ODBC que utiliza depende del sistema operativo que usa:

- administrador de controladores unixODBC (para sistemas operativos Linux)
- administrador de controladores iODBC (para el sistema operativo macOS X)

Para obtener más información acerca de los administradores de controladores ODBC compatibles que se utilizan para configurar los controladores ODBC de Amazon Redshift, consulte Requisitos del sistema para sistemas operativos Linux y Requisitos del sistema para sistemas operativos macOS X. Asimismo, consulte "Especificación de administradores de controladores ODBC en máquinas que no sean de Windows" en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Se necesitan tres archivos para configurar el controlador ODBC de Amazon Redshift: `amazon.redshiftodbc.ini`, `odbc.ini` y `odbcinst.ini`.

Si instaló el controlador en la ubicación predeterminada, el archivo de configuración `amazon.redshiftodbc.ini` se encuentra en alguno de los siguientes directorios:

- `/opt/amazon/redshiftodbc/lib/64` (para el controlador de 64 bits en sistemas operativos Linux)
- `/opt/amazon/redshiftodbc/lib/32` (para el controlador de 32 bits en sistemas operativos Linux)
- `/opt/amazon/redshift/lib` (para el controlador en Mac OS X)

Además, `/opt/amazon/redshiftodbc/Setup` en Linux o /opt/amazon/redshift/setup en Mac OS X, hay archivos `odbc.ini` y `odbcinst.ini` de ejemplo. Puede utilizar estos archivos como ejemplos para configurar el controlador ODBC de Amazon Redshift y el nombre del origen de datos (DSN).

No le recomendamos utilizar el directorio de instalación del controlador ODBC de Amazon Redshift para los archivos de configuración. Los archivos de muestra del directorio `Setup` son solo con fines de ejemplo. Si vuelve a instalar el controlador ODBC de Amazon Redshift más adelante o actualiza a una versión más reciente, se sobrescribe el directorio de instalación. A continuación, perderá los cambios que haya realizado en esos archivos.

Para evitarlo, copie el archivo `amazon.redshiftodbc.ini` en un directorio distinto al directorio de instalación. Si copia este archivo en el directorio principal del usuario, agregue un punto (.) al principio del nombre del archivo para convertirlo en un archivo oculto.

Para los archivos `odbc.ini` y `odbcinst.ini`, utilice los archivos de configuración en el directorio principal del usuario o cree nuevas versiones en otro directorio. De manera predeterminada, su sistema operativo Linux o Mac OS X debe tener un archivo `odbc.ini` y un archivo `odbcinst.ini` en el directorio de inicio del usuario (`/home/$USER` o `~/`). Estos archivos predeterminados son archivos ocultos, que se indica con el punto (.) delante de cada nombre de archivo. Estos archivos solo se muestran cuando se utiliza el indicador `-a` para enumerar el contenido del directorio.

Cualquiera que sea la opción que elija para los archivos `odbc.ini` y `odbcinst.ini`, modifique los archivos para agregar información de configuración del controlador y DSN. Si selecciona crear archivos nuevos, también deberá configurar variables de entorno para especificar la ubicación de estos archivos de configuración.

De manera predeterminada, los administradores de controladores ODBC están configurados para usar versiones ocultas de los archivos de configuración `odbc.ini` y `odbcinst.ini`

(denominados `.odbc.ini` y `.odbcinst.ini`) ubicados en el directorio de inicio. También están configurados para utilizar el archivo `amazon.redshiftodbc.ini` en la subcarpeta `/lib` del directorio de instalación del controlador. Si almacena estos archivos de configuración en otro lugar, establezca las variables de entorno que se describen a continuación para que el administrador de controladores pueda localizar los archivos. Para obtener más información, consulte "Especificación de las ubicaciones de los archivos de configuración del controlador" en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Creación de un nombre de origen de datos en sistemas operativos Linux y Mac OS X

Cuando se conecte al almacenamiento de datos mediante un nombre de origen de datos (DSN), configure el archivo `odbc.ini` para definir los DSN. Establezca las propiedades del archivo `odbc.ini` para crear un DSN que especifique la información de conexión para el almacén de datos.

Para obtener información acerca de cómo configurar el archivo `odbc.ini`, consulte "Creación de un nombre de origen de datos en una máquina que no sea de Windows" en la Guía de instalación y configuración del conector ODBC de Amazon Redshift

Utilice el siguiente formato en sistemas operativos Linux:

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

En el siguiente ejemplo, se muestra la configuración del archivo odbc.ini con el controlador ODBC de 64 bits para sistemas operativos Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
```

```
Database=dev
locale=en-US
```

En el siguiente ejemplo, se muestra la configuración del archivo odbc.ini con el controlador ODBC de 32 bits para sistemas operativos Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x32=Amazon Redshift (x86)

[Amazon Redshift (x86)]
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Utilice el siguiente formato en sistemas operativos Mac OS X:

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/lib/amazonredshiftodbc.dylib

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbc.ini` en sistemas operativos Mac OS X.

```
[ODBC Data Sources]
Amazon_Redshift_dylib=Amazon Redshift DSN for macOS X

[Amazon Redshift DSN for macOS X]
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
```

```
locale=en-US
```

Configuración de una conexión sin DSN en sistemas operativos Linux y Mac OS X

Para conectarse al almacén de datos a través de una conexión que no tenga DSN, defina el controlador en el archivo `odbcinst.ini`. A continuación, proporcione una cadena de conexión sin DSN en su aplicación.

Para obtener información acerca de cómo configurar el archivo `odbcinst.ini` en este caso, consulte "Configuración de una conexión sin DSN en una máquina que no sea de Windows" en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Utilice el siguiente formato en sistemas operativos Linux:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file

...
```

En el siguiente ejemplo, se muestra la configuración de `odbcinst.ini` para los controladores de 64 bits que se instalan en los directorios predeterminados en sistemas operativos Linux.

```
[ODBC Drivers]
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

En el siguiente ejemplo, se muestra la configuración de `odbcinst.ini` para los controladores de 32 bits que se instalan en los directorios predeterminados en sistemas operativos Linux.

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed
```

```
[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```

Utilice el siguiente formato en sistemas operativos Mac OS X:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib

...
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbcinst.ini` para el controlador que se instala en el directorio predeterminado en sistemas operativos Mac OS X.

```
[ODBC Drivers]
Amazon RedshiftODBC DSN=Installed

[Amazon RedshiftODBC DSN]
Description=Amazon Redshift ODBC Driver for macOS X
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

Configuración de variables de entorno

Utilice el administrador de controladores ODBC correcto para cargar el controlador correcto. Para ello, configure la variable de entorno de ruta de biblioteca. Para obtener más información, consulte "Especificación de administradores de controladores ODBC en máquinas que no sean de Windows" en la Guía de instalación y configuración de controladores ODBC de Amazon Redshift.

De manera predeterminada, los administradores de controladores ODBC están configurados para usar versiones ocultas de los archivos de configuración `odbc.ini` y `odbcinst.ini` (denominados `.odbc.ini` y `.odbcinst.ini`) ubicados en el directorio de inicio. También están configurados para utilizar el archivo `amazon.redshiftodbc.ini` en la subcarpeta `/lib` del directorio de instalación del controlador. Si almacena estos archivos de configuración en otro lugar, las variables de entorno para que el administrador de controladores pueda localizar los archivos.

Para obtener más información, consulte “Especificación de las ubicaciones de los archivos de configuración del controlador” en la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Configuración de las características de conexión

Puede configurar las siguientes características de conexión para la configuración de ODBC:

- Configure el controlador ODBC para proporcionar credenciales y autenticar la conexión a la base de datos de Amazon Redshift.
- Configure el controlador ODBC para conectarse a un socket habilitado con la capa de conexión segura (SSL), si se está conectando a un servidor de Amazon Redshift que tiene SSL habilitado.
- Configure el controlador ODBC para conectarse a Amazon Redshift a través de un servidor proxy.
- Configure el controlador ODBC para utilizar un modo de procesamiento de consultas para evitar que las consultas consuman demasiada memoria.
- Configure el controlador ODBC para que transfiera los procesos de autenticación de IAM a través de un servidor proxy.
- Configure el controlador ODBC para que utilice conexiones keepalive de TCP para evitar que se agote el tiempo de espera en las conexiones.

Para obtener información acerca de estas características de conexión, consulte la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Configurar las opciones del controlador ODBC

Puede utilizar las opciones de configuración para controlar el comportamiento del controlador ODBC de Amazon Redshift.

En Microsoft Windows, por lo general, las opciones del controlador se configuran cuando configura un nombre de origen de datos (DSN). También puede establecer opciones de controlador en la cadena de conexión cuando se conecta mediante programación o agregando o cambiando claves del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\`*`your_DSN`*. Para obtener más información acerca de la configuración de un DSN, consulte Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.

En Linux y Mac OS X, se establecen las opciones de configuración del controlador en los archivos `odbc.ini` y `amazon.redshiftodbc.ini`, como se describe en Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X.

Las opciones de configuración establecidas en un archivo `amazon.redshiftodbc.ini` se aplican a todas las conexiones. No obstante, las opciones de configuración establecidas en un archivo `odbc.ini` son específicas de una conexión. Las opciones de configuración establecidas en `odbc.ini` tienen prioridad sobre las opciones de configuración establecidas en `amazon.redshiftodbc.ini`.

Para obtener información acerca de cómo configurar las opciones de configuración de controladores ODBC, consulte la Guía de instalación y configuración de conectores ODBC de Amazon Redshift.

Versiones anteriores del controlador ODBC

Descargue una versión anterior del controlador ODBC de Amazon Redshift solo si su herramienta requiere una versión específica de este.

Usar versiones anteriores del controlador ODBC para Windows

Los siguientes son los controladores de 64 bits:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC64-1.5.7.1007.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC64-1.4.65.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC64-1.4.62.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC64-1.4.59.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC64-1.4.56.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/AmazonRedshiftODBC64-1.4.53.1000.msi
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC64-1.4.52.1000.msi

Los controladores de 32 bits se suspenden y no se admiten versiones anteriores.

Usar versiones anteriores del controlador ODBC para Linux

Las siguientes son las versiones del controlador de 64 bits:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-64-bit-1.5.7.1007-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-64-bit-1.4.65.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-64-bit-1.4.62.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.deb
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.rpm
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.deb

Los controladores de 32 bits se suspenden y no se admiten versiones anteriores.

Usar versiones anteriores del controlador ODBC para Mac OS X

A continuación, se muestran las versiones del controlador ODBC de Amazon Redshift para macOS X:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-1.5.7.1007.x86_64.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-1.4.65.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-1.4.62.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-1.4.59.1000.dmg

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-1.4.56.1000.dmg
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-1.4.52.1000.dmg

Configuración de las opciones de seguridad para las conexiones

Amazon Redshift admite las conexiones de capa de conexión segura (SSL) para cifrar datos y los certificados de servidor para validar el certificado del servidor al que se conecta el cliente.

Conexión mediante una SSL

Para admitir las conexiones SSL, Amazon Redshift crea e instala un certificado SSL emitido por AWS Certificate Manager (ACM) en cada clúster. La mayoría de los sistemas operativos, navegadores web y clientes confían públicamente en los certificados ACM. No obstante, este cambio lo afectará en caso de que sus clientes o aplicaciones SQL se conectan a Amazon Redshift mediante SSL con el conjunto de opciones de conexión `sslmode` establecido como `require`, `verify-ca` o `verify-full`. Si su cliente necesita un certificado, Amazon Redshift proporciona un certificado de paquete de la siguiente manera:

- Descargue el paquete desde https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt.
  - El número de suma de comprobación MD5 esperado es 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - El número de suma de comprobación sha256 es 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  No utilice el paquete de certificados anterior que se encontraba en`https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.
- En la Región de AWS China, descargue el paquete desde https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt.
  - El número de suma de comprobación MD5 esperado es 418dea9b6d5d5de7a8f1ac42e164cdcf.
  - El número de suma de comprobación sha256 es 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

  No utilice los paquetes de certificados anteriores que se encontraban en `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` y

```
https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-
ssl-ca-cert.pem
```

> **Important**
>
> Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte Migración a certificados de ACM para las conexiones SSL.

De manera predeterminada, las bases de datos del clúster aceptan una conexión, independientemente de que use una SSL o no. Para configurar que su clúster requiera una conexión SSL, establezca el parámetro `require_SSL` en `true` en el grupo de parámetros asociado al clúster.

Amazon Redshift admite un modo SSL conforme con el Estándar de procesamiento de la información federal (FIPS, Federal Information Processing Standard) 140-2. El modo SSL compatible con FIPS está deshabilitado de manera predeterminada.

> **Important**
>
> Habilite el modo SSL compatible con FIPS solo si el sistema debe ser compatible con FIPS.

Para habilitar el modo SSL compatible con FIPS, establezca tanto el parámetro `use_fips_ssl` como `require_SSL` en `true` en el grupo de parámetros asociado al clúster. Para obtener información acerca de cómo modificar un grupo de parámetros, consulte Grupos de parámetros de Amazon Redshift.

Amazon Redshift es compatible con el protocolo de acuerdo de clave de Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Con ECDHE, tanto el cliente como el servidor tienen un par de claves pública-privada de curva elíptica que se usa para establecer un código secreto compartido sobre un canal inseguro. No es necesario que configure nada en Amazon Redshift para habilitar ECDHE. Si se conecta desde una herramienta de cliente SQL que usa ECDHE para cifrar la comunicación entre el cliente y el servidor, Amazon Redshift usará la lista de cifrado proporcionada para realizar la conexión adecuada. Para obtener más información, consulte Elliptic Curve Diffie-Hellman en Wikipedia y Ciphers en el sitio web de OpenSSL.

Uso de certificados SSL y de entidad de certificación de confianza en ODBC

Si se conecta usando los controladores ODBC de Amazon Redshift más recientes (versión 1.3.7.1000 o posterior), puede omitir esta sección. Para descargar los controladores más recientes, consulte Configuración de una conexión ODBC.

Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte Conexión mediante una SSL.

Puede verificar que el certificado que descargó concuerda con el número de suma de comprobación MD5 esperado. Para hacer esto, puede usar el programa Md5sum en sistemas operativos Linux u otra herramienta en sistemas operativos Windows y Mac OS X.

Los DSN de ODBC contienen un valor `sslmode` que determina cómo se va a administrar el cifrado en las conexiones cliente y la verificación del certificado del servidor. Amazon Redshift admite los siguientes valores `sslmode` de la conexión de cliente:

- `disable`

  SSL está deshabilitada y la conexión no está cifrada.
- `allow`

  Se utiliza SSL si el servidor lo requiere.
- `prefer`

  Se utiliza SSL si el servidor lo admite. Amazon Redshift es compatible con SSL y, por lo tanto, se utiliza cuando se establece `sslmode` en `prefer`.
- `require`

  SSL es obligatoria.
- `verify-ca`

  Se debe utilizar SSL y se debe comprobar el certificado de servidor.
- `verify-full`

  Se debe utilizar SSL. Se debe comprobar el certificado de servidor y el nombre del host debe coincidir con el atributo del nombre de host del certificado.

Puede determinar si se utiliza SSL y si se verifican los certificados del servidor en una conexión entre el cliente y el servidor. Para ello, debe revisar la configuración de `sslmode` para su DSN de ODBC en el cliente y la configuración de `require_SSL` para el clúster de Amazon Redshift en el servidor. En la tabla a continuación, se describe el resultado del cifrado para diferentes combinaciones de configuraciones de clientes y servidores:

sslmode (cliente)	require_SSL (servidor)	Resultado
`disable`	`false`	La conexión no está cifrada.
`disable`	`true`	No se puede establecer la conexión porque el servidor requiere SSL y el cliente tiene SSL deshabilitado para la conexión.
`allow`	`true`	La conexión está cifrada.
`allow`	`false`	La conexión no está cifrada.
`prefer` o `require`	`true`	La conexión está cifrada.
`prefer` o `require`	`false`	La conexión está cifrada.
`verify-ca`	`true`	La conexión está cifrada y se comprueba el certificado de servidor.
`verify-ca`	`false`	La conexión está cifrada y se comprueba el certificado de servidor.
`verify-full`	`true`	La conexión está cifrada y se comprueba el certificado de servidor y el nombre de host.
`verify-full`	`false`	La conexión está cifrada y se comprueba el certificado de servidor y el nombre de host.

Conexión a través del certificado de servidor con ODBC en Microsoft Windows

Si desea conectarse al clúster mediante SSL y el certificado de servidor, descargue primero el certificado en el equipo cliente o la instancia de Amazon EC2. A continuación, configure el DSN ODBC.

1. Descargue el paquete de entidades de certificación de Amazon Redshift en la computadora cliente, en la carpeta `lib` del directorio de instalación del controlador, y guarde el archivo como `root.crt`. Para obtener información sobre la descarga, consulte Conexión mediante una SSL.
2. Abra ODBC Data Source Administrator (Administrador de orígenes de datos de ODBC) y agregue o edite la entrada DSN del sistema de su conexión ODBC. En SSL Mode (Modo SSL), seleccione `verify-full` a menos que use un alias DNS. Si usa un alias DNS, seleccione `verify-ca`. A continuación, elija Guardar.

   Para obtener más información acerca de la configuración del DSN de ODBC, consulte Configuración de una conexión ODBC.

Uso de certificados SSL y de servidor en Java

SSL proporciona una capa de seguridad al cifrar los datos que se mueven entre su cliente y el clúster. El uso de un certificado de servidor proporciona una capa adicional de seguridad, ya que comprueba que el clúster sea un clúster de Amazon Redshift. La validación la hace comprobando que el certificado de servidor se instale automáticamente en todos los clústeres que usted aprovisiona. Para obtener más información acerca del uso de certificados de servidor con JDBC, visite Configuring the Client en la documentación de PostgreSQL.

Conexión mediante certificados de entidad de certificación en Java

> **Important**
>
> Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte Conexión mediante una SSL.

Para conectarse mediante certificados de CA de confianza

Puede usar el archivo `redshift-keytool.jar` para importar los certificados de entidad de certificación del paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java o en su TrustStore privado.

1. Si usa la opción `-Djavax.net.ssl.trustStore` de la línea de comandos de Java, elimínela de la línea de comandos, si es posible.
2. Descargue redshift-keytool.jar.
3. Realice una de las acciones siguientes:

   - Para importar el paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java, ejecute el siguiente comando.

     ```
     java -jar redshift-keytool.jar -s
     ```

   - Para importar el paquete de entidades de certificación de Amazon Redshift en su TrustStore privado, ejecute el siguiente comando:

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Migración a certificados de ACM para las conexiones SSL

Amazon Redshift está sustituyendo los certificados SSL en sus clústeres con certificados emitidos por AWS Certificate Manager (ACM). ACM en una entidad de certificación (CA) pública de confianza en la que confían la mayoría de los sistemas actuales. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL.

Este cambio solo le afecta si se dan las siguientes circunstancias:

- Sus clientes SQL o aplicaciones se conectan a clústeres de Amazon Redshift mediante SSL con el conjunto de opciones de conexión `sslMode` establecido en la opción de configuración `require`, `verify-ca` o `verify-full`.
- No utiliza los controladores ODBC o JDBC de Amazon Redshift ODBC, o bien utiliza controladores de Amazon Redshift anteriores a ODBC versión 1.3.7.1000 o JDBC versión 1.2.8.1005.

Si este cambio lo afecta en las regiones comerciales de Amazon Redshift, debe actualizar sus certificados de entidad de certificación raíz actuales antes del 23 de octubre de 2017. Amazon Redshift migrará sus clústeres para usar certificados de ACM entre la fecha actual y el 23 de octubre de 2017. El cambio apenas debería tener efecto en el rendimiento o la disponibilidad de sus clústeres.

Si este cambio lo afecta en las regiones de AWS GovCloud (US) (EE. UU.), debe actualizar los certificados de entidad de certificación raíz de confianza actuales antes del 1 de abril de 2020 para evitar la interrupción del servicio. A partir de esta fecha, los clientes que se conectan a clústeres de Amazon Redshift mediante conexiones cifradas SSL necesitan una entidad de certificación (CA) de confianza adicional. Los clientes utilizan entidades de certificación de confianza para confirmar la identidad del clúster de Amazon Redshift cuando se conectan a él. Su acción es necesaria para actualizar los clientes y aplicaciones SQL para utilizar un paquete de certificados actualizado que incluya la nueva entidad de certificación de confianza.

> **Important**
>
> A partir del 5 de enero de 2021, en las regiones de China, Amazon Redshift reemplazará los certificados SSL de sus clústeres por certificados emitidos por AWS Certificate Manager (ACM). Si este cambio lo afecta en la región China (Pekín) o en la región China (Ningxia), debe actualizar sus certificados de entidad de certificación raíz de confianza actuales antes del 5 de enero de 2021 para evitar la interrupción del servicio. A partir de esta fecha, los clientes que se conectan a clústeres de Amazon Redshift mediante conexiones cifradas SSL necesitan una entidad de certificación (CA) de confianza adicional. Los clientes utilizan entidades de certificación de confianza para confirmar la identidad del clúster de Amazon Redshift cuando se conectan a él. Su acción es necesaria para actualizar los clientes y aplicaciones SQL para utilizar un paquete de certificados actualizado que incluya la nueva entidad de certificación de confianza.

- Uso de los controladores ODBC o JDBC de Amazon Redshift más recientes
- Uso de controladores ODBC o JDBC de Amazon Redshift anteriores
- Uso de otros tipos de conexión SSL

Uso de los controladores ODBC o JDBC de Amazon Redshift más recientes

El método preferido es usar los controladores ODBC o JDBC de Amazon Redshift más recientes. Los controladores ODBC de Amazon Redshift a partir de la versión 1.3.7.1000 y JDBC a partir de la versión 1.2.8.1005 realizan la migración automáticamente desde un certificado autofirmado de Amazon Redshift a un certificado de ACM. Para descargar los controladores más recientes, consulte Configuración de una conexión ODBC o Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.

Si usa el controlador JDBC de Amazon Redshift más reciente, es aconsejable que no use `-Djavax.net.ssl.trustStore` en las opciones de JVM. Si debe usar `-Djavax.net.ssl.trustStore`, importe el paquete de entidades de certificación de Redshift en el TrustStore al que apunta. Para obtener información sobre la descarga, consulte Conexión mediante una SSL. Para obtener más información, consulte Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore.

Uso de controladores ODBC o JDBC de Amazon Redshift anteriores

- Si el DSN de ODBC está configurado con `SSLCertPath`, sobrescriba el archivo de certificado en la ruta especificada.
- Si `SSLCertPath` no está establecido, sobrescriba el archivo de certificado `root.crt` en la ubicación de la DLL del controlador.

Si debe usar un controlador JDBC de Amazon Redshift anterior a la versión 1.2.8.1005, proceda de una de las siguientes maneras:

- Si la cadena de conexión de JDBC usa la opción `sslCert`, elimine la opción `sslCert`. A continuación, importe el Paquete de entidades de certificación de Redshift en su TrustStore de Java. Para obtener información sobre la descarga, consulte Conexión mediante una SSL. Para obtener más información, consulte Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore.
- Si usa la opción `-Djavax.net.ssl.trustStore` de la línea de comandos de Java, elimínela de la línea de comandos, si es posible. A continuación, importe el Paquete de entidades de certificación de Redshift en su TrustStore de Java. Para obtener información sobre la descarga, consulte Conexión mediante una SSL. Para obtener más información, consulte Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore.

Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore

Puede usar `redshift-keytool.jar` para importar los certificados de entidad de certificación del paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java o en su TrustStore privado.

Para importar el paquete de entidades de certificación de Amazon Redshift en un TrustStore

1. Descargue redshift-keytool.jar.
2. Realice una de las acciones siguientes:
   - Para importar el paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java, ejecute el siguiente comando.

     ```
     java -jar redshift-keytool.jar -s
     ```
   - Para importar el paquete de entidades de certificación de Amazon Redshift en su TrustStore privado, ejecute el siguiente comando:

     ```
     java -jar redshift-keytool.jar -k <your_private_trust_store> -
     p <keystore_password>
     ```

Uso de otros tipos de conexión SSL

Siga los pasos de esta sección si se conecta mediante alguno de los métodos siguientes:

- Controlador ODBC de código abierto
- Controlador JDBC de código abierto
- La interfaz de línea de comandos de Amazon Redshift RSQL
- Alguna conexión de lenguaje de programación basada en libpq, como psycopg2 (Python) y ruby-pg (Ruby)

Para usar certificados de ACM con otros tipos de conexión SSL:

1. Descargue el paquete de entidades de certificación de Amazon Redshift. Para obtener información sobre la descarga, consulte Conexión mediante una SSL.
2. Coloque los certificados del paquete en su archivo `root.crt`.

- En los sistemas operativos Linux y Mac OS X, el archivo es `~/.postgresql/root.crt`
- En Microsoft Windows, el archivo es `%APPDATA%\postgresql\root.crt`

Conexión desde herramientas y código cliente

Amazon Redshift proporciona el editor de consultas de Amazon Redshift v2 para conectarse a sus clústeres y grupos de trabajo. Para obtener más información, consulte Consulta de una base de datos mediante el editor de consultas v2 de Amazon Redshift.

En esta sección, se proporcionan algunas opciones para la conexión de herramientas de terceros. Además, se describe cómo conectarse a su clúster mediante programación.

Temas

- Conexión con Amazon Redshift RSQL
- Conexión a un clúster con Amazon Redshift RSQL
- Metacomandos de Amazon Redshift RSQL
- Variables de Amazon Redshift RSQL
- Códigos de error de Amazon Redshift RSQL
- Variables de entorno de Amazon Redshift RSQL

Conexión con Amazon Redshift RSQL

Amazon Redshift RSQL es un cliente de línea de comandos para interactuar con clústeres y bases de datos de Amazon Redshift. Puede conectarse a un clúster de Amazon Redshift, describir objetos de base de datos, consultar datos y ver los resultados de las consultas en varios formatos de salida.

Amazon Redshift RSQL admite las capacidades de la herramienta de línea de comandos psql de PostgreSQL con un conjunto adicional de capacidades específicas de Amazon Redshift. Estos incluyen los siguientes:

- Puede utilizar la autenticación de inicio de sesión único mediante ADFS, PingIdentity, Okta, Azure AdM u otros proveedores de identidades basados en SAML/JWT. También puede utilizar proveedores de identidades SAML basados en navegador para la autenticación multifactor (MFA).
- Puede describir las propiedades o los atributos de los objetos de Amazon Redshift, tales como claves de distribución de tablas, claves de clasificación de tablas, vistas de enlace tardío (LBV)

y vistas materializadas. También puede describir las propiedades o los atributos de las tablas externas en un catálogo AWS Glue o Apache Hive Metastore, bases de datos externas en Amazon RDS for PostgreSQL, edición compatible con PostgreSQL de Amazon Aurora, RDS para MySQL (versión preliminar) y edición compatible con MySQL de Amazon Aurora (versión preliminar), y tablas compartidas mediante el uso compartido de datos de Amazon Redshift.

- También puede utilizar comandos de flujo de control mejorados, como `IF` (`\ELSEIF`, `\ELSE`, `\ENDIF`), `\GOTO` y `\LABEL`.

Con el modo por lotes de Amazon Redshift RSQL, que ejecuta un script pasado como parámetro de entrada, puede ejecutar scripts que incluyan SQL y lógica empresarial compleja. Si ya tiene almacenamientos de datos autoadministrados en las instalaciones, puede utilizar Amazon Redshift RSQL para reemplazar los scripts de extracción, transformación, carga (ETL) y automatización existentes, como los scripts BTEQ de Teradata. El uso de RSQL lo ayuda a evitar la reimplementación manual de scripts en un lenguaje de procedimiento.

Amazon Redshift RSQL está disponible para los sistemas operativos Linux, Windows y macOS X.

Para informar de problemas de Amazon Redshift RSQL, escriba `a<redshift-rsql-support@amazon.com>`.

Temas

- Introducción a Amazon Redshift RSQL
- Registro de cambios de Amazon Redshift RSQL

Introducción a Amazon Redshift RSQL

Instale Amazon Redshift RSQL en una computadora con un sistema operativo Linux, macOS o Microsoft Windows.

Descarga de RSQL

- RPM de Linux de 64 bits: versión 1.0.8 de RSQL
- DMG de Mac OS de 64 bits: versión 1.0.8 de RSQL
- MSI de Windows de 64 bits: versión 1.0.8 de RSQL

Consulte el registro de cambios y las descargas de versiones anteriores en Registro de cambios de Amazon Redshift RSQL.

Instalación de RSQL para Linux

Siga los pasos que se indican a continuación para instalar RSQL para Linux.

1. Instale el administrador de controladores con el siguiente comando:

   ```
   sudo yum install unixODBC openssl
   ```

   OpenSSL es necesario para las distribuciones de Linux. La biblioteca de OpenSSL se encuentra en el repositorio Linux OpenSSL de Github. Para obtener más información acerca de OpenSSL, consulte OpenSSL.

2. Instale el controlador ODBC: Instalación del controlador de Amazon Redshift en sistemas operativos Linux.

3. Copie el archivo ini en el directorio de inicio.

   ```
   cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
   ```

4. Establezca las variables de entorno para que apunten a la ubicación del archivo:

   ```
   export ODBCINI=~/.odbc.ini
       export ODBCSYSINI=/opt/amazon/redshiftodbc/Setup
       export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/
   amazon.redshiftodbc.ini
   ```

   Para obtener más información sobre cómo configurar variables de entorno de ODBC, consulte Configuración de variables de entorno.

5. Ahora puede instalar RSQL si ejecuta el siguiente comando.

   ```
   sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
   ```

Instalación de RSQL para Mac

Siga los pasos que se indican a continuación para instalar RQL para Mac OSX.

1. Instale el administrador de controladores con el siguiente comando:

   ```
   brew install unixodbc openssl@1.1 --build-from-source
   ```

2. Instale el controlador ODBC: Instalación del controlador ODBC de Amazon Redshift en macOS X.
3. Copie el archivo ini en el directorio de inicio.

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. Establezca las variables de entorno para que apunten a la ubicación del archivo:

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshift/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftodbc.ini
```

   Para obtener más información sobre cómo configurar variables de entorno de ODBC, consulte Configuración de variables de entorno.
5. Establezca `DYLD_LIBRARY_PATH` en la ubicación de su libodbc.dylib si no está en `/usr/local/lib`.

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

6. Haga doble clic en el archivo dmg para montar la imagen del disco.
7. Haga doble clic en el archivo pkg para ejecutar el instalador.
8. Siga los pasos de instalación para completar la instalación. Acepte los términos del acuerdo de licencia.

Instalación de RSQL para Windows

Siga las instrucciones en Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows para instalar el controlador. Windows no requiere administrador de controladores.

OpenSSL es necesario para Amazon Redshift RSQL en Windows. La biblioteca de OpenSSL de Windows se encuentra en el repositorio Windows OpenSSL de Github. Para obtener más información acerca de OpenSSL, consulte OpenSSL.

Haga doble clic en el archivo de descarga de RSQL para ejecutar el instalador y, a continuación, siga las indicaciones para completar la instalación.

Registro de cambios de Amazon Redshift RSQL

1.0.8 (2023-06-19)

Correcciones de errores

- Se ha solucionado un problema por el que la salida se truncaba con los comandos SHOW.
- Se ha agregado soporte a \de para describir flujos de Kinesis externos y temas de Kafka.

1.0.7 (2023-03-22)

Correcciones de errores

- Se corrigió un problema por el que RSQL no podía describir las vistas materializadas.
- Se corrigió el error de permiso denegado en stl_connection_log al usar Amazon Redshift sin servidor.
- Se corrigió el problema por el que RSQL podía procesar las etiquetas \GOTO de forma incorrecta.
- Se corrigió el problema por el que los mensajes SSL se imprimían en modo silencioso.
- Se corrigió el problema con los caracteres aleatorios que se mostraban al describir los procedimientos almacenados.
- Se corrigió el problema al imprimir mensajes ERROR/INFO duplicados.

New

- RSQL ahora obtiene la información de SSL directamente del controlador ODBC.

1.0.6 (2023-02-21)

Correcciones de errores

- Se corrigió un problema por el que \d genera el error de sintaxis de entrada no válida para el entero: “xid”, en Redshift revisión 1.0.46086 (P173).

New

- Se cambió el nombre de los archivos de instalación para reflejar la arquitectura compatible.

1.0.5 (27-06-2022)

Correcciones de errores

- Envíe mensajes de error SQL al error estándar (stderr).
- Se corrigió el problema con los códigos de salida al usar ON_ERROR_STOP. Ahora los scripts finalizan después de encontrar un error y devuelven los códigos de salida correctos.
- Maxerror ahora distingue entre mayúsculas y minúsculas.

New

- Se agregó compatibilidad para el controlador ODBC 2.x.

1.0.4 (2022-03-19)

- Agregue compatibilidad con la variable de entorno RSPASSWORD. Establezca una contraseña para conectarse a Amazon Redshift. Por ejemplo, `export RSPASSWORD=TestPassw0rd`.

1.0.3 (08-12-2021)

Correcciones de errores

- Se ha corregido el diálogo emergente al usar `\c` o `\logon` para cambiar entre bases de datos en el sistema operativo Windows.
- Se ha corregido el fallo al comprobar la información de SSL.

Versiones anteriores de Amazon Redshift RSQL

Elija uno de los enlaces para descargar la versión de Amazon Redshift RSQL que necesita, según su sistema operativo.

Archivo RPM de Linux de 64 bits

- Versión 1.0.7 de RSQL
- Versión 1.0.6 de RSQL
- Versión 1.0.5 de RSQL
- Versión 1.0.4 de RSQL

- RSQL, versión 1.0.3
- RSQL, versión 1.0.1

Archivo DMG de Mac OS de 64 bits

- Versión 1.0.7 de RSQL
- Versión 1.0.6 de RSQL
- RSQL, versión 1.0.5
- RSQL, versión 1.0.4
- RSQL, versión 1.0.3
- RSQL, versión 1.0.1

Archivo MSI de Windows de 64 bits

- Versión 1.0.7 de RSQL
- Versión 1.0.6 de RSQL
- Versión 1.0.5 de RSQL
- Versión 1.0.4 de RSQL
- RSQL, versión 1.0.3
- RSQL, versión 1.0.1

Conexión a un clúster con Amazon Redshift RSQL

Conexión sin un DSN

1. En la consola de Amazon Redshift, elija el clúster al que desea conectarse y anote el punto de conexión, la base de datos y el puerto.
2. En el símbolo del sistema, especifique la información de conexión usando los parámetros de línea de comando.

   ```
   rsql -h <endpoint> -U <username> -d <databasename> -p <port>
   ```

   A continuación, se aplica lo siguiente:

   - *<endpoint>* en el punto de conexión que registró en el paso anterior.

- *<username>* es el nombre de usuario con permisos para conectarse al clúster.
- *<databasename>* es el nombre de base de datos que registró en el paso anterior.
- *<port>* es el puerto que registró en el paso anterior. *<port>* es un parámetro opcional.

Ejemplo:

```
rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
```

3. Cuando se le solicite la contraseña, ingrese la contraseña del usuario *<username>*.

   Una respuesta de conexión exitosa tendría el siguiente aspecto.

```
% rsql -h testcluster.example.com -d dev -U user1 -p 5349
Password for user user1:
DSN-less Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

El comando de conexión tiene los mismos parámetros en Linux, Mac OS y Windows.

Conexión mediante un DSN

Puede conectar RSQL a Amazon Redshift utilizando un nombre de origen de datos (DSN) para simplificar la organización de las propiedades de conexión. Para obtener más información, consulte Configuración de las características de conexión. En este tema se incluyen instrucciones para la instalación del controlador ODBC y descripciones de las propiedades de DSN. Por ejemplo, en la siguiente sección, Instale y configure el controlador ODBC de Amazon Redshift en Microsoft Windows, se muestra cómo conectarse con un DSN mediante Windows.

Uso de una conexión DSN con contraseña

A continuación se muestra un ejemplo de configuración de conexión DSN que utiliza una contraseña. El `<path to driver>` predeterminado para Mac OSX es `/opt/amazon/redshift/lib/`

`libamazonredshiftodbc.dylib` y para Linux es `/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so`.

```
[testuser]
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<database port>
Database=<dbname>
UID=<username>
PWD=<password>
sslmode=prefer
```

El siguiente es el resultado de una conexión correcta.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

Uso de DSN de inicio de sesión único

Puede configurar un DSN para la autenticación de inicio de sesión único. A continuación se muestra un ejemplo de una configuración de conexión DSN que utiliza el inicio de sesión único de Okta.

```
[testokta]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
```

```
locale=en-US
iam=1
plugin_name=<plugin name>
uid=<okta username>
pwd=<okta password>
idp_host=<idp endpoint>
app_id=<app id>
app_name=<app name>
preferred_role=<role arn>
```

Salida de ejemplo de una conexión correcta.

```
% rsql -D testokta
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

A continuación se muestra un ejemplo de una configuración de conexión DSN que utiliza el inicio de sesión único de Azure.

```
[testazure]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<cluster port>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
locale=en-us
iam=1
plugin_name=<plugin name>
uid=<azure username>
pwd=<azure password>
idp_tenant=<Azure idp tenant uuid>
client_id=<Azure idp client uuid>
```

```
client_secret=<Azure idp client secret>
```

Uso de una conexión DSN con un perfil de IAM

Puede conectarse a Amazon Redshift mediante el perfil de IAM configurado. El perfil de IAM debe tener privilegios para llamar a `GetClusterCredentials`. En el siguiente ejemplo, se muestran las propiedades de DSN que se utilizarán. Los parámetros `ClusterID` y `Region` son obligatorios solo si el `Host` no es un punto de conexión proporcionado por Amazon como `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default
```

El valor de la clave `Profile` es el perfil con nombre que elija de sus credenciales de la AWS CLI. En este ejemplo, se muestran las credenciales del perfil denominado `default`.

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

A continuación se muestra la respuesta de conexión.

```
$ rsql -D testiam
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

Uso de una conexión DSN con un perfil de instancias

Puede conectarse a Amazon Redshift mediante su perfil de instancia de Amazon EC2. El perfil de instancias debe tener privilegios para llamar a `GetClusterCredentials`. Consulte el siguiente ejemplo para ver las propiedades de DSN que se van a utilizar. Los parámetros `ClusterID` y `Region` son obligatorios solo si el `Host` no es un punto de conexión proporcionado por Amazon como `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

A continuación se muestra la respuesta de conexión.

```
$ rsql -D testinstanceprofile
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

Uso de una conexión DSN con la cadena predeterminada de proveedores de credenciales

Para conectarse mediante la cadena predeterminada de proveedores de credenciales, especifique solo la propiedad de IAM; Amazon Redshift RSQL intentará adquirir las credenciales en el orden descrito en Uso de credenciales de AWS en el AWS SDK para Java. Al menos uno de los proveedores de la cadena debe tener el permiso `GetClusterCredentials`. Eso resulta útil para conectarse desde contenedores de ECS, por ejemplo.

```
[iamcredentials]
```

```
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
```

Metacomandos de Amazon Redshift RSQL

Los metacomandos de Amazon Redshift RSQL devuelven registros informativos sobre bases de datos u objetos de base de datos específicos. Los resultados pueden incluir varias columnas y metadatos. Otros comandos realizan acciones específicas. Estos comandos van precedidos de una barra invertida.

\d[S+]

Muestra las tablas creadas por el usuario local, las vistas regulares, las vistas de enlace tardío y las vistas materializadas. `\dS` también enumera tablas y vistas, como `\d`, pero los objetos del sistema se incluyen en los registros devueltos. Los resultados + en la columna de metadatos adicionales `description` para todos los objetos enumerados. A continuación se muestran los registros de ejemplo devueltos como resultado del comando.

```
List of relations
 schema |   name    | type  |  owner
--------+-----------+-------+---------
 public | category  | table | awsuser
 public | date      | table | awsuser
 public | event     | table | awsuser
 public | listing   | table | awsuser
 public | sales     | table | awsuser
 public | users     | table | awsuser
 public | venue     | table | awsuser
(7 rows)
```

\d[S+] NOMBRE

Describe una tabla, vista o índice. Incluye los nombres y tipos de columnas. También proporciona el estilo diststyle, la configuración de copias de seguridad, la fecha de creación (tablas creadas después de octubre de 2018) y las restricciones. Por ejemplo, `\dS+ sample` devuelve las

propiedades de objeto. Anexar S+ da como resultado columnas adicionales incluidas en los registros devueltos.

```
Table "public.sample"
 Column |            Type             |   Collation    | Nullable | Default Value |
 Encoding  | DistKey | SortKey
--------+-----------------------------+----------------+----------+---------------
+-----------+---------+---------
 col1   | smallint                    |                | NO       |               |
 none      | t       | 1
 col2   | character(100)              | case_sensitive | YES      |               |
 none      | f       | 2
 col3   | character varying(100)      | case_sensitive | YES      |               |
 text32k   | f       | 3
 col4   | timestamp without time zone |                | YES      |               |
 runlength | f       | 0
 col5   | super                       |                | YES      |               |
 zstd      | f       | 0
 col6   | bigint                      |                | YES      |               |
 az64      | f       | 0

Diststyle: KEY
Backup: YES
Created: 2021-07-20 19:47:27.997045
Unique Constraints:
    "sample_pkey" PRIMARY KEY (col1)
    "sample_col2_key" UNIQUE (col2)
Foreign-key constraints:
    "sample_col2_fkey" FOREIGN KEY (col2) REFERENCES lineitem(l_orderkey)
```

El estilo de distribución, o Diststyle, de la tabla puede ser KEY, AUTO, EVEN o ALL.

Backup indica si se realiza una copia de seguridad de la tabla cuando se toma una instantánea. Los valores válidos son YES o NO.

Create es la marca de tiempo de cuando se crea la tabla. La fecha de creación no está disponible para las tablas de Amazon Redshift creadas antes de noviembre de 2018. Las tablas creadas antes de esta fecha muestran n/a (No disponible).

Unique Constraints enumera las restricciones de clave única y principal de la tabla.

Foreign-key constraints enumera las restricciones de clave extranjera de la tabla.

\dC[+] [PATRÓN]

Enumera las conversiones. Incluye el tipo de origen, el tipo de destino y si la conversión está implícita.

A continuación, se muestra un subconjunto de resultados de \dC+.

```
List of casts
         source type         |         target type         |      function       |
 implicit?   | description
-----------------------------+-----------------------------+---------------------
+---------------+-------------
 "char"                      | character                   | bpchar              | in
 assignment |
 "char"                      | character varying           | text                | in
 assignment |
 "char"                      | integer                     | int4                | no
          |
 "char"                      | text                        | text                | yes
          |
 "path"                      | point                       | point               | no
          |
 "path"                      | polygon                     | polygon             | in
 assignment |
 abstime                     | date                        | date                | in
 assignment |
 abstime                     | integer                     | (binary coercible)  | no
          |
 abstime                     | time without time zone      | time                | in
 assignment |
 abstime                     | timestamp with time zone    | timestamptz         | yes
          |
 abstime                     | timestamp without time zone | timestamp           | yes
          |
 bigint                      | bit                         | bit                 | no
          |
 bigint                      | boolean                     | bool                | yes
          |
 bigint                      | character                   | bpchar              | in
 assignment |
 bigint                      | character varying           | text                | in
 assignment |
 bigint                      | double precision            | float8              | yes
          |
```

```
bigint                      | integer                     | int4               | in
assignment |
bigint                      | numeric                     | numeric            | yes
         |
bigint                      | oid                         | oid                | yes
         |
bigint                      | real                        | float4             | yes
         |
bigint                      | regclass                    | oid                | yes
         |
bigint                      | regoper                     | oid                | yes
         |
bigint                      | regoperator                 | oid                | yes
         |
bigint                      | regproc                     | oid                | yes
         |
bigint                      | regprocedure                | oid                | yes
         |
bigint                      | regtype                     | oid                | yes
         |
bigint                      | smallint                    | int2               | in
assignment |
bigint                      | super                       | int8_partiql       | in
assignment |
```

\dd[S] [PATRÓN]

Muestra las descripciones de objetos que no se muestran en ningún otro lugar.

\de

Muestra las tablas externas. Esto incluye las tablas del catálogo de datos AWS Glue, Hive Metastore y tablas federadas de Amazon RDS/Aurora MySQL, Amazon RDS/Aurora PostgreSQL y tablas de recurso compartido de datos de Amazon Redshift.

\de NOMBRE

Describe una tabla externa.

El siguiente ejemplo muestra una tabla externa de AWS Glue.

```
# \de spectrum.lineitem
```

```
                          Glue External table "spectrum.lineitem"
     Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----------------+---------------+---------------+----------+---------------+----------
 l_orderkey      | bigint        | bigint        | 1        | 0             |
 l_partkey       | bigint        | bigint        | 2        | 0             |
 l_suppkey       | int           | int           | 3        | 0             |
 l_linenumber    | int           | int           | 4        | 0             |
 l_quantity      | decimal(12,2) | decimal(12,2) | 5        | 0             |
 l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0             |
 l_discount      | decimal(12,2) | decimal(12,2) | 7        | 0             |
 l_tax           | decimal(12,2) | decimal(12,2) | 8        | 0             |
 l_returnflag    | char(1)       | char(1)       | 9        | 0             |
 l_linestatus    | char(1)       | char(1)       | 10       | 0             |
 l_shipdate      | date          | date          | 11       | 0             |
 l_commitdate    | date          | date          | 12       | 0             |
 l_receiptdate   | date          | date          | 13       | 0             |
 l_shipinstruct  | char(25)      | char(25)      | 14       | 0             |
 l_shipmode      | char(10)      | char(10)      | 15       | 0             |
 l_comment       | varchar(44)   | varchar(44)   | 16       | 0             |

Location: s3://redshiftbucket/kfhose2019/12/31
Input_format: org.apache.hadoop.mapred.TextInputFormat
Output_format: org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat
Serialization_lib: org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe
Serde_parameters: {"field.delim":"|","serialization.format":"|"}
Parameters:
 {"EXTERNAL":"TRUE","numRows":"178196721475","transient_lastDdlTime":"1577771873"}
```

Una tabla de Hive Metastore.

```
# \de emr.lineitem
                    Hive Metastore External Table "emr.lineitem"
     Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----------------+---------------+---------------+----------+---------------+----------
 l_orderkey      | bigint        | bigint        | 1        | 0             |
 l_partkey       | bigint        | bigint        | 2        | 0             |
 l_suppkey       | int           | int           | 3        | 0             |
 l_linenumber    | int           | int           | 4        | 0             |
 l_quantity      | decimal(12,2) | decimal(12,2) | 5        | 0             |
 l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0             |
 l_discount      | decimal(12,2) | decimal(12,2) | 7        | 0             |
 l_tax           | decimal(12,2) | decimal(12,2) | 8        | 0             |
```

```
 l_returnflag    | char(1)       | char(1)       | 9        | 0            |
 l_linestatus    | char(1)       | char(1)       | 10       | 0            |
 l_commitdate    | date          | date          | 11       | 0            |
 l_receiptdate   | date          | date          | 12       | 0            |
 l_shipinstruct  | char(25)      | char(25)      | 13       | 0            |
 l_shipmode      | char(10)      | char(10)      | 14       | 0            |
 l_comment       | varchar(44)   | varchar(44)   | 15       | 0            |
 l_shipdate      | date          | date          | 16       | 1            |

Location: s3://redshiftbucket/cetas
Input_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetInputFormat
Output_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetOutputFormat
Serialization_lib: org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe
Serde_parameters: {"serialization.format":"1"}
Parameters: {"EXTERNAL":"TRUE", "numRows":"4307207",
 "transient_lastDdlTime":"1626990007"}
```

Tabla externa de PostgreSQL.

```
# \de pgrsql.alltypes
                              Postgres Federated Table "pgrsql.alltypes"
 Column |        External Type        |        Redshift Type        | Position |
 Partition Key | Nullable
--------+-----------------------------+-----------------------------+----------
+---------------+----------
 col1   | bigint                      | bigint                      | 1        | 0
        |
 col2   | bigint                      | bigint                      | 2        | 0
        |
 col5   | boolean                     | boolean                     | 3        | 0
        |
 col6   | box                         | varchar(65535)              | 4        | 0
        |
 col7   | bytea                       | varchar(65535)              | 5        | 0
        |
 col8   | character(10)               | character(10)               | 6        | 0
        |
 col9   | character varying(10)       | character varying(10)       | 7        | 0
        |
 col10  | cidr                        | varchar(65535)              | 8        | 0
        |
```

```
 col11  | circle                   | varchar(65535)           | 9        | 0
        |
 col12  | date                     | date                     | 10       | 0
        |
 col13  | double precision         | double precision         | 11       | 0
        |
 col14  | inet                     | varchar(65535)           | 12       | 0
        |
 col15  | integer                  | integer                  | 13       | 0
        |
 col16  | interval                 | varchar(65535)           | 14       | 0
        |
 col17  | json                     | varchar(65535)           | 15       | 0
        |
 col18  | jsonb                    | varchar(65535)           | 16       | 0
        |
 col19  | line                     | varchar(65535)           | 17       | 0
        |
 col20  | lseg                     | varchar(65535)           | 18       | 0
        |
 col21  | macaddr                  | varchar(65535)           | 19       | 0
        |
 col22  | macaddr8                 | varchar(65535)           | 20       | 0
        |
 col23  | money                    | varchar(65535)           | 21       | 0
        |
 col24  | numeric                  | numeric(38,20)           | 22       | 0
        |
 col25  | path                     | varchar(65535)           | 23       | 0
        |
 col26  | pg_lsn                   | varchar(65535)           | 24       | 0
        |
 col28  | point                    | varchar(65535)           | 25       | 0
        |
 col29  | polygon                  | varchar(65535)           | 26       | 0
        |
 col30  | real                     | real                     | 27       | 0
        |
 col31  | smallint                 | smallint                 | 28       | 0
        |
 col32  | smallint                 | smallint                 | 29       | 0
        |
 col33  | integer                  | integer                  | 30       | 0
        |
```

```
 col34  | text                        | varchar(65535)              | 31       | 0
        |
 col35  | time without time zone      | varchar(65535)              | 32       | 0
        |
 col36  | time with time zone         | varchar(65535)              | 33       | 0
        |
 col37  | timestamp without time zone | timestamp without time zone | 34       | 0
        |
 col38  | timestamp with time zone    | timestamp with time zone    | 35       | 0
        |
 col39  | tsquery                     | varchar(65535)              | 36       | 0
        |
 col40  | tsvector                    | varchar(65535)              | 37       | 0
        |
 col41  | txid_snapshot               | varchar(65535)              | 38       | 0
        |
 col42  | uuid                        | varchar(65535)              | 39       | 0
        |
 col43  | xml                         | varchar(65535)              | 40       | 0
        |
```

\df[anptw][S+] [PATRÓN]

Enumera funciones de varios tipos. El comando `\df`, por ejemplo, devuelve una lista de funciones. Los resultados incluyen propiedades como nombre, tipo de datos devuelto, privilegios de acceso y metadatos adicionales. Los tipos de funciones pueden incluir desencadenadores, procedimientos almacenados, funciones de ventana y otros tipos. Cuando anexa `S+` al comando, por ejemplo, `\dfantS+`, se incluyen columnas de metadatos adicionales, como`owner`, `security` y `access privileges`.

\dL[S+] [PATRÓN]

Enumera datos sobre los lenguajes de procedimiento asociados a la base de datos. La información incluye el nombre, como plpgsql, y metadatos adicionales, que incluyen si es de confianza, privilegios de acceso y descripción. La llamada de muestra es, por ejemplo, `\dLS+`, que enumera los lenguajes y sus propiedades. Cuando anexa `S+` al comando, se incluyen columnas de metadatos adicionales, como `call handler` y `access privileges`.

Resultados de ejemplo:

```
List of languages
```

```
   name    | trusted | internal language |      call handler       |
      validator                         | access privileges |          description

-----------+---------+------------------+-------------------------
+-----------------------------------------------------------+-------------------
+--------------------------------
 c         | f       | t                | -                       |
 fmgr_c_validator(oid)                                        |                 |
 Dynamically-loaded C functions
 exfunc    | f       | f                | exfunc_call_handler()   | -
                                        | rdsdb=U/rdsdb     |
 internal  | f       | t                | -                       |
 fmgr_internal_validator(oid)                                 |                 |
 Built-in functions
 mlfunc    | f       | f                | mlfunc_call_handler()   | -
                                        | rdsdb=U/rdsdb     |
 plpgsql   | t       | f                | plpgsql_call_handler()  |
 plpgsql_validator(oid)                                       |                 |
 plpythonu | f       | f                | plpython_call_handler() |
 plpython_compiler(cstring,cstring,cstring,cstring,cstring) | rdsdb=U/rdsdb     |
 sql       | t       | t                | -                       |
 fmgr_sql_validator(oid)                                      | =U/rdsdb          | SQL-
language functions
```

\dm[S+] [PATRÓN]

Enumera las vistas materializadas. Por ejemplo, `\dmS+` enumera las vistas materializadas y sus propiedades. Cuando anexa `S+` al comando, se incluyen columnas de metadatos adicionales.

\dn[S+] [PATRÓN]

Enumera esquemas. Cuando anexa `S+` al comando, por ejemplo, `\dnS+`, se incluyen columnas de metadatos adicionales, como `description` y `access privileges`.

\dp [PATRÓN]

Enumera los privilegios de acceso a tablas, vistas y secuencias.

\dt[S+] [PATRÓN]

Enumera tablas. Cuando anexa `S+` al comando, por ejemplo, `\dtS+`, se incluyen columnas de metadatos adicionales, como `description` en este caso.

\du

Enumera los usuarios de la base de datos. Incluye su nombre y sus roles, como superusuario y atributos.

\dv[S+] [PATRÓN]

Enumera vistas. Incluye datos de propietario, esquema y tipo. Cuando anexa `S+` al comando, por ejemplo, `\dvS+`, se incluyen columnas de metadatos adicionales.

\H

Activa la salida HTML. Esto resulta útil para devolver rápidamente los resultados formateados. Por ejemplo, `select * from sales; \H` devuelve los resultados de la tabla de ventas, en HTML. Para volver a los resultados tablulares, utilice `\q`, o inactividad.

\i

Ejecuta comandos desde un archivo. Por ejemplo, si se asume que tiene rsql_steps.sql en el directorio de trabajo, lo siguiente ejecuta los comandos en el archivo: `\i rsql_steps.sql`.

\l[+] [PATRÓN]

Enumera bases de datos. Incluye propietario, codificación e información adicional.

\q

La inactividad, o comando `\q`, cierra la sesión de la base de datos y cierra de RSQL.

\sv[+] VIEWNAME

Muestra la definición de una vista.

\timing

Muestra el tiempo de ejecución, para una consulta, por ejemplo.

\z [PATRÓN]

El mismo resultado que \dp.

\?

Muestra información de ayuda. El parámetro opcional especifica el elemento que se va a explicar.

\EXIT

Cierra la sesión de todas las sesiones de base de datos y cierra Amazon Redshift RSQL. Además puede especificar un código de salida opcional. Por ejemplo, `\EXIT 15` saldrá de la terminal de Amazon Redshift RSQL y devolverá el código de salida 15.

En el siguiente ejemplo, se muestra el resultado de una conexión y la salida de RSQL.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.34.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=# \exit 15

% echo $?
15
```

\EXPORT

Especifica el nombre de un archivo de exportación que RSQL utiliza para almacenar la información de la base de datos que devuelve una instrucción SQL SELECT posterior.

export_01.sql

```
\export report file='E:\\accounts.out'
\rset rformat off
\rset width 1500
\rset heading "General Title"
\rset titledashes on
select * from td_dwh.accounts;
\export reset
```

Salida de la consola

```
Rformat is off.
Target width is 1500.
Heading is set to: General Title
Titledashes is on.
(exported 40 rows)
```

\LOGON

Se conecta a una base de datos. Puede especificar parámetros de conexión mediante sintaxis posicional o como cadena de conexión.

La sintaxis de comandos es la siguiente: `\logon {[DBNAME|- USERNAME|- HOST|- PORT|- [PASSWORD]] | conninfo}`

`DBNAME` es el nombre de la base de datos a la que se debe conectar. `USERNAME` es el nombre de usuario para contectarse. El `HOST` predeterminado es `localhost`. El `PORT` predeterminado es `5439`.

Cuando se especifica un nombre de host en un comando `\LOGON`, se convierte en el nombre de host predeterminado para agregar comandos `\LOGON` adicionales. Para cambiar el nombre de host predeterminado, especifique un nuevo `HOST` en un comando `\LOGON` adicional.

A continuación se muestra el resultado de ejemplo del comando `\LOGON` para `user1`.

```
(testcluster) user1@redshiftdb=# \logon dev
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user1".
(testcluster) user1@dev=#
```

Resultados de ejemplo de para user2.

```
(testcluster) user1@dev=# \logon dev user2 testcluster2.example.com
Password for user user2:
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user2" on host
 "testcluster2.example.com" at port "5439".
```

```
(testcluster2) user2@dev=#
```

\REMARK

Ampliación del comando \echo. \REMARK imprime la cadena especificada en el flujo de salida. \REMARK amplía \echo agregando la capacidad de dividir la salida en líneas separadas.

En el siguiente ejemplo, se muestra la salida desde el comando.

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

\RSET

El comando \rset establece parámetros de comando y variables. \rset tiene un modo interactivo y otro por lotes. No admite opciones como opciones bash, como -x, o argumentos; por ejemplo, --<arg>.

Establece variables, como las siguientes:

- ERRORLEVEL
- HEADING y RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- WIDTH

En el siguiente ejemplo, se especifica un encabezado.

```
\rset heading "Winter Sales Report"
```

Para obtener más ejemplos de cómo utilizar \rset, puede encontrar varios en los temas de Variables de Amazon Redshift RSQL.

\RUN

Ejecuta el script de Amazon Redshift RSQL contenido en el archivo especificado. \RUN amplía el comando \i agregando una opción para omitir líneas de encabezado en un archivo.

Si el nombre del archivo incluye una coma, un punto y coma o un espacio, colóquelo entre comillas simples. Además, si hay texto después del nombre del archivo, colóquelo entre comillas. En UNIX, los nombres de los archivos distinguen mayúsculas de minúsculas. En Windows, los nombres de los archivos distinguen entre mayúsculas y minúsculas.

En el siguiente ejemplo, se muestra la salida desde el comando.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as lineitem_cnt from lineitem;
select count(*) as customer_cnt from customer;
select count(*) as orders_cnt from orders;



(testcluster) user1@dev=# \run file=test.sql
 lineitem_cnt
--------------
      4307207
(1 row)

 customer_cnt
--------------
     37796166
(1 row)

 orders_cnt
------------
          0
(1 row)


(testcluster) user1@dev=# \run file=test.sql skip=2
2 records skipped in RUN file.
 orders_cnt
------------
          0
(1 row)
```

\OS

Un alias para el comando `\!`. `\OS` ejecuta el comando del sistema operativo que se pasa como parámetro. El control vuelve a Amazon Redshift RSQL después de ejecutar el comando. Por

ejemplo, puede ejecutar el siguiente comando para imprimir la hora de la fecha actual del sistema y volver al terminal RSQL: `\os date`.

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

\GOTO

Un nuevo comando para Amazon Redshift RSQL. `\GOTO` omite todos los comandos que intervienen y reanuda el procesamiento en el `\LABEL` especificado. El `\LABEL` debe ser una referencia anticipada. No puede saltar a un `\LABEL` que precede léxicamente al `\GOTO`.

A continuación se muestra una salida de ejemplo.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as cnt from lineitem \gset
select :cnt as cnt;
\if :cnt > 100
    \goto LABELB
\endif

\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'


(testcluster) user1@dev=# \i test.sql
   cnt
---------
 4307207
(1 row)

\label LABELA ignored
\label LABELB processed
this is label LABELB
```

\LABEL

Un nuevo comando para Amazon Redshift RSQL. `\LABEL` establece un punto de entrada para ejecutar el programa, como objetivo de un comando `\GOTO`.

En el siguiente ejemplo, se muestra un ejemplo de salida del comando.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) from lineitem limit 5;
\goto LABELB
\remark "this step was skipped by goto label";
\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'



(testcluster) user1@dev=# \i testgoto.sql
  count
 4307193
(1 row)

\label LABELA ignored
\label LABELB processed
this is label LABELB
```

\IF (\ELSEIF, \ELSE, \ENDIF)

`\IF` y los comandos relacionados ejecutan de forma condicional partes del script de entrada. Extensión de comando `\if` (`\elif`, `\else`, `\endif`) de PSQL. `\IF` y `\ELSEIF` admiten expresiones booleanas, incluidas las condiciones `AND`, `OR` y `NOT`.

En el siguiente ejemplo, se muestra un ejemplo de salida desde el comando.

```
(testcluster) user1@dev=# \! cat test.sql
SELECT query FROM stv_inflight LIMIT 1 \gset
select :query as query;
\if :query > 1000000
    \remark 'Query id is greater than 1000000'
\elseif :query = 1000000
    \remark 'Query id is equal than 1000000'
\else
    \remark 'Query id is less than 1000000'
\endif


(testcluster) user1@dev=# \i test.sql
```

```
 query
--------
 994803
(1 row)

Query id is less than 1000000
```

Use ERRORCODE en su lógica de ramificación.

```
\if :'ERRORCODE' = '00000'
    \remark 'The statement was executed without error'
\else
    \remark :LAST_ERROR_MESSAGE
\endif
```

Use \GOTO dentro de un bloque \IF para controlar cómo se ejecuta el código.

Variables de Amazon Redshift RSQL

Algunas palabras clave actúan como variables en RSQL. Puede establecer cada una en un valor específico o volver a establecer el valor. La mayoría se establecen con \rset, que tiene un modo interactivo y otro por lotes. Los comandos se pueden definir en minúsculas o mayúsculas.

ACTIVITYCOUNT

Indica el número de filas afectadas por la última solicitud enviada. En el caso de una solicitud de devolución de datos, es el número de filas devueltas a RSQL desde la base de datos. El valor es 0 o un número entero positivo. El valor máximo es 18 446 744 073 709 551 615.

La variable ACTIVITYCOUNT, que se trata de forma especial, es similar a la variable ROW_COUNT. No obstante, ROW_COUNT no notifica un recuento de filas afectadas a la aplicación cliente al finalizar el comando para SELECT, COPY o UNLOAD. En cambio, ACTIVITYCOUNT sí.

activitycount_01.sql:

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

Salida de la consola:

```
viewname | schemaname
----------+------------
(0 rows)

views do not exist
```

ERRORLEVEL

Asigna los niveles de gravedad a los errores. Utilice los niveles de gravedad para determinar un procedimiento a seguir. Si el comando ERRORLEVEL no se ha utilizado, su valor es ON de manera predeterminada.

errorlevel_01.sql:

```
\rset errorlevel 42P01 severity 0

select * from tbl;

select 1 as col;

\echo exit
\quit
```

Salida de la consola:

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1

exit
```

HEADING y RTITLE

Permite a los usuarios especificar un encabezado que aparece en la parte superior de un informe. El encabezado que especifica el comando RSET RTITLE incluye automáticamente la fecha actual del sistema de la computadora cliente.

Contenido de rset_heading_rtitle_02.rsql:

```
\remark Starting...
\rset rtitle "Marketing Department||Confidential//Third Quarter//Chicago"
\rset width 70
\rset rformat on
select * from rsql_test.tbl_currency order by id limit 2;
\exit
\remark Finishing...
```

Salida de la consola:

```
Starting...
Rtitle is set to: &DATE||Marketing Department||Confidential//Third Quarter//Chicago
 (Changes will take effect after RFORMAT is
switched ON)
Target width is 70.
Rformat is on.
09/11/20       Marketing       Department Confidential
                  Third Quarter
                     Chicago
id  | bankid  | name |      start_date
100 |       1 | USD | 2020-09-11 10:51:39.106905
110 |       1 | EUR | 2020-09-11 10:51:39.106905
(2 rows)

Press any key to continue . . .
```

MAXERROR

Designa un nivel máximo de gravedad de los errores a partir del que RSQL termina el procesamiento de trabajos. Los códigos de devolución son valores enteros que RSQL devuelve al sistema operativo cliente después de completar cada trabajo o tarea. El valor del código de devolución indica el estado de finalización del trabajo o tarea. Si un script contiene una instrucción que produce un nivel de gravedad de error superior al valor de `maxerror` designado, RSQL se cierra inmediatamente. Por lo tanto, para que RSQL se cierre con un nivel de gravedad de error de 8, utilice `RSET MAXERROR 7`.

Contenido de maxerror_01.sql:

```
\rset maxerror 0

select 1 as col;
```

```
\quit
```

Salida de la consola:

```
Maxerror is default.
(1 row)

col
1
```

RFORMAT

Permite a los usuarios especificar si se aplicará la configuración de los comandos de formato.

Contenido de rset_rformat.rsql:

```
\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsql_test.tbl_long where id = 500;
\rset rformat
select * from rsql_test.tbl_long where id = 500;
\rset rformat off
select * from rsql_test.tbl_long where id = 500;
\rset rformat on
select * from rsql_test.tbl_long where id = 500;
\exit
\remark Finishing...
```

Salida de la consola:

```
Starting...
Border style is 2. (Changes will take effect after RFORMAT is switched ON)
Output format is wrapped. (Changes will take effect after RFORMAT is switched ON)
Expanded display is on. (Changes will take effect after RFORMAT is switched ON)
Title is "Great Title". (Changes will take effect after RFORMAT is switched ON)
id  |                                                          long_string
500 | In general, the higher the number the more borders and lines the tables will
 have, but details depend on the particular
format.
```

```
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-----------------------------------------------------------------------------------------------
-----------+
| id           | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
 will have, but details depend on the
particular format. |
+-------------
+-----------------------------------------------------------------------------------------------
-----------+

Rformat is off.
id  |                                                                long_string
500 | In general, the higher the number the more borders and lines the tables will
 have, but details depend on the particular format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-----------------------------------------------------------------------------------------------
-----------+
| id           | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
 will have, but details depend on the
particular format. |
+-------------
+-----------------------------------------------------------------------------------------------
-----------+
Press any key to continue . . .
```

ROW_COUNT

Obtiene el número de registros a los que afecta la consulta anterior. Normalmente se utiliza para comprobar un resultado, como en el siguiente fragmento de código:

```
SET result = ROW_COUNT;
```

```
IF result = 0
...
```

TITLEDASHES

Este control permite a los usuarios especificar si se imprimirá una línea de caracteres de guion encima de los datos de columna devueltos para las instrucciones SQL.

Ejemplo:

```
\rset titledashes on
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
\rset titledashes off
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
```

Salida de la consola:

```
dept_no      emp_no          salary
------------ ----------- --------------------
100          1000346        1300.00
100          1000245        5000.00
100          1000262        2450.00

dept_no     emp_no          salary
100          1000346        1300.00
100          1000245        5000.00
100          1000262        2450.00
```

WIDTH

Establece el formato de salida como ajustado y especifica la anchura de destino de cada línea de un informe. Sin un parámetro, devuelve la configuración actual para el formato y para la anchura de destino.

Contenido de rset_width_01.rsql:

```
\echo Starting...
\rset width
```

```
\rset width 50
\rset width
\quit
\echo Finishing...
```

Salida de la consola:

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

Ejemplo con parámetro:

```
\echo Starting...
\rset rformat on
\pset format wrapped
select * from rsql_test.tbl_long where id = 500;
\rset width 50
select * from rsql_test.tbl_long where id = 500;
\quit
\echo Finishing...
```

Salida de la consola:

```
Starting...
Rformat is on.
Output format is wrapped.
id  |                                          long_string
500 | In general, the higher the number the more borders and lines the ta.
    |.bles will have, but details depend on the particular format.
(1 row)

Target width is 50.
id  |                                          long_string
500 | In general, the higher the number the more.
    |. borders and lines the tables will have, b.
    |.ut details depend on the particular format.
    |..
(1 row)
Press any key to continue . . .
```

Códigos de error de Amazon Redshift RSQL

Mensajes de éxito, advertencias y excepciones:

Código de error	Clase de error	Nombre de condición
00000	Clase 00: finalización correcta	successful_completion
01000	Clase 01: advertencia	warning
0100C	Clase 01: advertencia	dynamic_result_sets_returned
01008	Clase 01: advertencia	implicit_zero_bit_padding
01003	Clase 01: advertencia	null_value_eliminated_in_set_function
01007	Clase 01: advertencia	privilege_not_granted
01006	Clase 01: advertencia	privilege_not_revoked
01004	Clase 01: advertencia	string_data_right_truncation
01P01	Clase 01: advertencia	deprecated_feature
02000	Clase 02: sin datos	no_data
02001	Clase 02: sin datos	no_additional_dynamic_result_sets_returned
03000	Clase 03: instrucción SQL aún no completa	sql_statement_not_yet_complete
08000	Clase 08: excepción de conexión	connection_exception
08003	Clase 08: excepción de conexión	connection_does_not_exist
08006	Clase 08: excepción de conexión	connection_failure

Código de error	Clase de error	Nombre de condición
08001	Clase 08: excepción de conexión	sqlclient_unable_to_establish_sqlconnection
08004	Clase 08: excepción de conexión	sqlserver_rejected_establishment_of_sqlconnection
08007	Clase 08: excepción de conexión	transaction_resolution_unknown
08P01	Clase 08: excepción de conexión	protocol_violation
09000	Clase 09: excepción de acción activada	triggered_action_exception
0A000	Clase 0A: función no admitida	feature_not_supported
0A000	Clase 0A: función no admitida	feature_not_supported
0B000	Clase 0B: iniciación de transacción no válida	invalid_transaction_initiation
0F000	Clase 0F: excepción de localizador	locator_exception
0F001	Clase 0F: excepción de localizador	invalid_locator_specification
0L000	Clase 0L: concedente no válido	invalid_grantor
0LP01	Clase 0L: concedente no válido	invalid_grant_operation
0P000	Clase 0P: especificación de función no válida	invalid_role_specification

Código de error	Clase de error	Nombre de condición
0Z000	Clase 0Z: excepción de diagnóstico	diagnostics_exception
0Z002	Clase 0Z: excepción de diagnóstico	stacked_diagnostics_accessed_without_active_handler
20000	Clase 20: caso no encontrado	case_not_found
21000	Clase 21: violación de cardinalidad	cardinality_violation

Excepciones de datos:

Código de error	Clase de error	Nombre de condición
22000	Clase 22: excepción de datos	data_exception
2202E	Clase 22: excepción de datos	array_subscript_error
22021	Clase 22: excepción de datos	character_not_in_repertoire
22008	Clase 22: excepción de datos	datetime_field_overflow
22012	Clase 22: excepción de datos	division_by_zero
22005	Clase 01: advertencia	error_in_assignment
2200B	Clase 01: advertencia	escape_character_conflict
22022	Clase 01: advertencia	indicator_overflow
22015	Clase 01: advertencia	interval_field_overflow
2201E	Clase 01: advertencia	invalid_argument_for_logarithm
2201F	Clase 01: advertencia	invalid_argument_for_power_function

Código de error	Clase de error	Nombre de condición
2201G	Clase 01: advertencia	invalid_argument_for_width_bucket_function
22018	Clase 01: advertencia	invalid_character_value_for_cast
22007	Clase 01: advertencia	invalid_datetime_format
22019	Clase 01: advertencia	invalid_escape_character
2200D	Clase 01: advertencia	invalid_escape_octet
22025	Clase 01: advertencia	invalid_escape_sequence
22P06	Clase 01: advertencia	nonstandard_use_of_escape_character
22010	Clase 01: advertencia	invalid_indicator_parameter_value
22023	Clase 01: advertencia	invalid_parameter_value
2201B	Clase 01: advertencia	invalid_regular_expression
22009	Clase 01: advertencia	invalid_time_zone_displacement_value
2200C	Clase 01: advertencia	invalid_use_of_escape_character
2200G	Clase 01: advertencia	most_specific_type_mismatch
22004	Clase 01: advertencia	null_value_not_allowed
22002	Clase 01: advertencia	null_value_no_indicator_parameter
22003	Clase 01: advertencia	numeric_value_out_of_range
22026	Clase 01: advertencia	string_data_length_mismatch
22001	Clase 01: advertencia	string_data_right_truncation
22011	Clase 01: advertencia	substring_error
22027	Clase 01: advertencia	trim_error

Código de error	Clase de error	Nombre de condición
22024	Clase 01: advertencia	unterminated_c_string
2200F	Clase 01: advertencia	zero_length_character_string
22P01	Clase 01: advertencia	floating_point_exception
22P02	Clase 01: advertencia	invalid_text_representation
22P03	Clase 01: advertencia	invalid_binary_representation
22P04	Clase 01: advertencia	bad_copy_file_format
22P05	Clase 01: advertencia	untranslatable_character

Violaciones de restricciones de integridad:

Código de error	Clase de error	Nombre de condición
23000	Clase 23: violación de restricciones de integridad	integrity_constraint_violation
23001	Clase 23: violación de restricciones de integridad	restrict_violation
23502	Clase 23: violación de restricciones de integridad	not_null_violation
23503	Clase 23: violación de restricciones de integridad	foreign_key_violation
23505	Clase 23: violación de restricciones de integridad	unique_violation
23514	Clase 23: violación de restricciones de integridad	check_violation

Código de error	Clase de error	Nombre de condición
24000	Clase 24: estado de cursor no válido	invalid_cursor_state
01004	Clase 01: advertencia	string_data_right_truncation
25000	Clase 25: estado de transacción no válida	invalid_transaction_state
25001	Clase 25: estado de transacción no válida	active_sql_transaction
25002	Clase 25: estado de transacción no válida	invalid_transaction_state
25008	Clase 25: estado de transacción no válida	held_cursor_requires_same_isolation_level
25003	Clase 25: estado de transacción no válida	inappropriate_access_mode_for_branch_transaction
25004	Clase 25: estado de transacción no válida	inappropriate_isolation_level_for_branch_transaction
25005	Clase 25: estado de transacción no válida	no_active_sql_transaction_for_branch_transaction
25006	Clase 25: estado de transacción no válida	read_only_sql_transaction
25007	Clase 25: estado de transacción no válida	no_active_sql_transaction_for_branch_transaction
25P01	Clase 25: estado de transacción no válida	no_active_sql_transaction
25P02	Clase 25: estado de transacción no válida	in_failed_sql_transaction

Código de error	Clase de error	Nombre de condición
26000	Clase 26: nombre de instrucción SQL no válido	invalid_sql_statement_name
28000	Clase 28: especificación de autorización no válida	invalid_authorization_specification
2B000	Clase 2B: todavía existen descriptores de privilegios dependientes	dependent_privilege_descriptors_still_exist
2BP01	Clase 2B: todavía existen descriptores de privilegios dependientes	dependent_objects_still_exist
2D000	Clase 2D: terminación de transacción no válida	invalid_transaction_termination
2F000	Clase 2F: excepción de rutina SQL	sql_routine_exception
2F005	Clase 2F: excepción de rutina SQL	function_executed_no_return_statement
2F002	Clase 2F: excepción de rutina SQL	modifying_sql_data_not_permitted
2F003	Clase 2F: excepción de rutina SQL	prohibited_sql_statement_attempted
2F004	Clase 2F: excepción de rutina SQL	reading_sql_data_not_permitted
34000	Clase 34: nombre de cursor no válido	invalid_cursor_name

Código de error	Clase de error	Nombre de condición
38000	Clase 38: excepción de rutina externa	external_routine_exception
38001	Clase 38: excepción de rutina externa	containing_sql_not_permitted
38002	Clase 38: excepción de rutina externa	modifying_sql_data_not_permitted
38003	Clase 38: excepción de rutina externa	prohibited_sql_statement_attempted
38004	Clase 38: excepción de rutina externa	reading_sql_data_not_permitted
39000	Clase 39: excepción de invocación de rutina externa	external_routine_invocation_exception
39001	Clase 39: excepción de invocación de rutina externa	invalid_sqlstate_returned
39004	Clase 39: excepción de invocación de rutina externa	null_value_not_allowed
39P01	Clase 39: excepción de invocación de rutina externa	trigger_protocol_violated
39P02	Clase 39: excepción de invocación de rutina externa	srf_protocol_violated
3D000	Clase 3D: nombre de catálogo no válido	invalid_catalog_name
3F000	Clase 3F: nombre de esquema no válido	invalid_schema_name

Código de error	Clase de error	Nombre de condición
42000	Clase 42: error de sintaxis o infracción de la regla de acceso	syntax_error_or_access_rule_violation
42601	Clase 42: error de sintaxis o infracción de la regla de acceso	syntax_error
42501	Clase 42: error de sintaxis o infracción de la regla de acceso	insufficient_privilege
42846	Clase 42: error de sintaxis o infracción de la regla de acceso	cannot_coerce
42803	Clase 42: error de sintaxis o infracción de la regla de acceso	grouping_error
42830	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_foreign_key
42602	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_name
42622	Clase 42: error de sintaxis o infracción de la regla de acceso	name_too_long
42939	Clase 42: error de sintaxis o infracción de la regla de acceso	reserved_name

Código de error	Clase de error	Nombre de condición
42804	Clase 42: error de sintaxis o infracción de la regla de acceso	datatype_mismatch
42P18	Clase 42: error de sintaxis o infracción de la regla de acceso	indeterminate_datatype
42809	Clase 42: error de sintaxis o infracción de la regla de acceso	wrong_object_type
42703	Clase 42: error de sintaxis o infracción de la regla de acceso	undefined_column
42883	Clase 42: error de sintaxis o infracción de la regla de acceso	undefined_function
42P01	Clase 42: error de sintaxis o infracción de la regla de acceso	undefined_table
42P02	Clase 42: error de sintaxis o infracción de la regla de acceso	undefined_parameter
42704	Clase 42: error de sintaxis o infracción de la regla de acceso	undefined_object
42701	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_column

Código de error	Clase de error	Nombre de condición
42P03	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_cursor
42P04	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_database
42723	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_function
42P05	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_prepared_statement
42P06	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_schema
42P07	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_table
42712	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_alias
42710	Clase 42: error de sintaxis o infracción de la regla de acceso	duplicate_object
42702	Clase 42: error de sintaxis o infracción de la regla de acceso	ambiguous_column

Código de error	Clase de error	Nombre de condición
42725	Clase 42: error de sintaxis o infracción de la regla de acceso	ambiguous_function
42P08	Clase 42: error de sintaxis o infracción de la regla de acceso	ambiguous_parameter
42P09	Clase 42: error de sintaxis o infracción de la regla de acceso	ambiguous_alias
42P10	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_column_reference
42611	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_column_definition
42P11	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_cursor_definition
42P12	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_database_definition
42P13	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_function_definition
42P14	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_prepared_statement_definition

Código de error	Clase de error	Nombre de condición
42P15	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_schema_definition
42P16	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_table_definition
42P17	Clase 42: error de sintaxis o infracción de la regla de acceso	invalid_object_definition
44000	Clase 44: violación de WITH CHECK OPTION	with_check_option_violation
53000	Clase 53: recursos insuficientes	insufficient_resources
53100	Clase 53: recursos insuficientes	disk_full
53200	Clase 53: recursos insuficientes	out_of_memory
53300	Clase 53: recursos insuficientes	too_many_connections
54000	Clase 54: límite de programa excedido	program_limit_exceeded
54001	Clase 54: límite de programa excedido	statement_too_complex
54011	Clase 54: límite de programa excedido	too_many_columns

Código de error	Clase de error	Nombre de condición
54023	Clase 54: límite de programa excedido	too_many_arguments
55000	Clase 55: objeto que no se encuentra en estado de requisito previo	object_not_in_prerequisite_state
55006	Clase 55: objeto que no se encuentra en estado de requisito previo	object_in_use
55P02	Clase 55: objeto que no se encuentra en estado de requisito previo	cant_change_runtime_param
55P03	Clase 55: objeto que no se encuentra en estado de requisito previo	lock_not_available
57000	Clase 57: intervención del operador	operator_intervention
57014	Clase 57: intervención del operador	query_canceled
57P01	Clase 57: intervención del operador	admin_shutdown
57P02	Clase 57: intervención del operador	crash_shutdown
57P03	Clase 57: intervención del operador	cannot_connect_now

Código de error	Clase de error	Nombre de condición
58000	Clase 58: error del sistema (errores externos a PostgreSQL)	system_error
58030	Clase 58: error del sistema (errores externos a PostgreSQL)	io_error
58P01	Clase 58: error del sistema (errores externos a PostgreSQL)	undefined_file
58P02	Clase 58: error del sistema (errores externos a PostgreSQL)	duplicate_file
F0000	Clase F0: error de archivo de configuración	duplicate_file
F0001	Clase F0: error de archivo de configuración	lock_file_exists
P0000	Clase P0: error PL/pgSQL	plpgsql_error
P0001	Clase P0: error PL/pgSQL	raise_exception
P0002	Clase P0: error PL/pgSQL	no_data_found
P0003	Clase P0: error PL/pgSQL	too_many_rows
XX000	Clase XX: error interno	internal_error
XX001	Clase XX: error interno	data_corrupted
XX002	Clase XX: error interno	index_corrupted

Variables de entorno de Amazon Redshift RSQL

Amazon Redshift RSQL puede utilizar variables de entorno para seleccionar valores de parámetros predeterminados.

RSPASSWORD

> **Important**
>
> No recomendamos utilizar esta variable de entorno por motivos de seguridad, ya que algunos sistemas operativos permiten a los usuarios no administrativos ver las variables de entorno de los procesos.

Establece la contraseña de Amazon Redshift RSQL que se utilizará al conectarse a Amazon Redshift. Esta variable de entorno requiere Amazon Redshift RSQL 1.0.4 y superior.

RSQL da prioridad a RSPASSWORD si se establece uno. Si RSPASSWORD no está configurado y se está conectando mediante DSN, RSQL toma la contraseña de los parámetros del archivo DSN. Por último, si RSPASSWORD no está configurado y no está utilizando DSN, RSQL proporciona un mensaje de contraseña después de intentar conectarse.

A continuación se muestra un ejemplo de cómo configurar un RSPASSWORD:

```
export RSPASSWORD=TestPassw0rd
```

Conexión con SQL Workbench/J

Puede conectar con una base de datos mediante SQL Workbench/J, una herramienta de consulta de SQL gratuita, multiplataforma e independiente de DBMS.

Amazon Redshift no proporciona ni instala ninguna biblioteca ni herramienta de cliente SQL, por lo que debe instalar la que desee usar con su base de datos. Para instalar SQL Workbench/J, siga las instrucciones de la documentación de dicha herramienta (SQL Workbench/J). En general, para usar SQL Workbench/J, haga lo siguiente:

- Consulte la licencia de software de SQL Workbench/J.
- Descargue el paquete de SQL Workbench/J adecuado para su sistema operativo en su equipo cliente o instancia de Amazon EC2.
- Instale SQL Workbench/J en su sistema.

Tenga instalado en su sistema el entorno de ejecución de Java (JRE). Asegúrese de que está utilizando la versión correcta de JRE que requiere el cliente SQL Workbench/J.

- Conéctese a su base de datos mediante una conexión JDBC en SQL Workbench/J.

  Asegúrese de que el equipo cliente o la instancia de Amazon EC2 tenga el controlador JDBC de Amazon Redshift recomendado. Para obtener los enlaces para descargar la versión más reciente de los controladores, consulte Descargar el controlador JDBC versión 2.1 de Amazon Redshift. Asegúrese también de que ha configurado las opciones del firewall para permitir el acceso a la base de datos. Para obtener más información, consulte Paso 4: Autorizar el acceso al clúster en la Guía de introducción de Amazon Redshift.
- Cree un nuevo perfil de conexión en SQL Workbench/J que utilice el controlador de Amazon Redshift.

Conexión a un almacenamiento de datos mediante programación

Para obtener información sobre las herramientas para crear aplicaciones que se conecten a su almacenamiento de datos, consulte Herramientas para crear en AWS.

Puede conectarse a Amazon Redshift con un perfil de autenticación.

Si tiene muchas conexiones a Amazon Redshift, puede ser difícil administrar la configuración de todas ellas. A menudo, cada conexión JDBC u ODBC utiliza opciones de configuración específicas. Mediante un perfil de autenticación, puede almacenar las opciones de conexión juntas. De esta forma, los usuarios pueden elegir un perfil con el que se conectarán y evitar administrar la configuración de opciones individuales. Los perfiles se pueden aplicar a varios escenarios y tipos de usuario.

Después de crear un perfil de autenticación, los usuarios pueden agregar el perfil listo para usar a una cadena de conexión. De este modo, pueden conectarse a Amazon Redshift con la configuración correcta para cada rol y caso de uso.

Para obtener información de la API de Amazon Redshift, consulte CreateAuthenticationProfile.

Creación de un perfil de autenticación

Con el uso de la AWS CLI, crea un perfil de autenticación con el comando `create-authentication-profile`. De este modo, se presupone que dispone de un clúster de Amazon Redshift y una base de datos existentes. Sus credenciales deben tener permiso para conectarse a la

base de datos de Amazon Redshift y derechos para obtener el perfil de autenticación. Proporciona las opciones de configuración como cadena JSON o hace referencia a un archivo que contiene la cadena JSON.

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

En el siguiente ejemplo, se crea un perfil denominado `ExampleProfileName`. Aquí, puede agregar claves y valores que definan el nombre de su clúster y otras configuraciones de opciones, como una cadena JSON.

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
 --authentication-profile-content "{\"AllowDBUserOverride\":\"1\",\"Client_ID
\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",\"AutoCreate\":false,
\"enableFetchRingBuffer\":true,\"databaseMetadataCurrentDbOnly\":true}"
}
```

Este comando crea el perfil con la configuración JSON especificada. Se devuelve lo siguiente, lo que indica que se ha creado el perfil.

```
{"AuthenticationProfileName": "ExampleProfileName",
"AuthenticationProfileContent": "{\"AllowDBUserOverride\":\"1\",
\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID\",
\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" }
```

Limitaciones y cuotas para crear un perfil de autenticación

Cada cliente tiene una cuota de diez (10) perfiles de autenticación.

Pueden producirse ciertos errores con los perfiles de autenticación. Algunos ejemplos son si crea un nuevo perfil con un nombre existente o si supera su cuota de perfil. Para obtener más información, consulte CreateAuthenticationProfile.

No se pueden almacenar ciertos valores y claves de opción para cadenas de conexión JDBC, ODBC y Python en el almacén de perfiles de autenticación:

- `AccessKeyID`
- `access_key_id`
- `SecretAccessKey`

- secret_access_key_id
- PWD
- Password
- password

No puede almacenar la clave o el valor AuthProfile en el almacén de perfiles, para cadenas de conexión JDBC u ODBC. Para las conexiones de Python, no puede almacenar auth_profile.

Los perfiles de autenticación se almacenan en Amazon DynamoDB y se administran mediante AWS.

Trabajo con perfiles de autenticación

Después de crear un perfil de autenticación, puede incluir el nombre del perfil como opción de conexión para la versión 2.0 de JDBC AuthProfile. Con esta opción de conexión se recuperan las configuraciones almacenadas.

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-
Name>&AccessKeyID=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

A continuación, se muestra un ejemplo de la cadena URL de un JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AuthProfile="ExampleProfile"&AccessKeyID="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

Especifique tanto AccessKeyID como SecretAccessKey en la URL de JDBC, junto con el nombre del perfil de autenticación.

También puede separar las opciones de configuración con delimitadores de punto y coma, como en el siguiente ejemplo, que incluye opciones para registrar.

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/
tmp;AuthProfile=my_profile;AccessKeyID="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

> **Note**
>
> No agregue información confidencial al perfil de autenticación. Por ejemplo, no almacene un valor AccessKeyID o SecretAccessKey en un perfil de autenticación. El almacén de

perfiles de autenticación tiene reglas para prohibir el almacenamiento de claves secretas. Se produce un error si intenta almacenar una clave y un valor asociados a información confidencial.

Obtención de perfiles de autenticación

Para enumerar los perfiles de autenticación existentes, llame al siguiente comando.

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

En el siguiente ejemplo, se muestran dos perfiles recuperados. Se devuelven todos los perfiles si no especifica un nombre de perfil.

```
{ "AuthenticationProfiles": [ { "AuthenticationProfileName":
"testProfile1", "AuthenticationProfileContent": "{\"AllowDBUserOverride
\":\"1\",\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID
\",\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" }, { "AuthenticationProfileName":
"testProfile2", "AuthenticationProfileContent": "{\"AllowDBUserOverride
\":\"1\",\"Client_ID\":\"ExampleClientID\",\"App_ID\":\"ExampleAppID
\",\"AutoCreate\":false,\"enableFetchRingBuffer\":true,
\"databaseMetadataCurrentDbOnly\":true}" } ] }
```

Solución de problemas de conexión en Amazon Redshift

Si tiene problemas para conectarse a su clúster desde una herramienta de cliente SQL, hay distintos puntos que puede controlar para acotar la solución del problema. Si está usando certificados SSL o de servidor, primero elimine esta complejidad mientras solucione el problema de conexión. Una vez que haya encontrado una solución, vuelva a agregarla. Para obtener más información, consulte Configuración de las opciones de seguridad para las conexiones.

Important

Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Si tiene problemas para conectarse mediante SSL, es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales. Para obtener más información, consulte Migración a certificados de ACM para las conexiones SSL.

En la siguiente sección, se muestran algunos ejemplos de mensajes de error y posibles soluciones para los problemas de conexión. Como las diferentes herramientas de cliente SQL proporcionan diferentes mensajes de error, esta no es un lista completa, pero debe ser un buen punto de partida para la solución de problemas.

Temas

- Conexión desde fuera de Amazon EC2: problema con el tiempo de espera del firewall
- La conexión devuelve un error o se rechaza
- El cliente y el controlador son incompatibles
- Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster
- Configuración del parámetro de tamaño de búsqueda de la JDBC

Conexión desde fuera de Amazon EC2: problema con el tiempo de espera del firewall

Problema de ejemplo

Su conexión cliente a la base de datos parece que dejó de funcionar o que superó el tiempo de espera mientras ejecutaba consultas largas, como un comando COPY. En este caso, es posible que observe que la consola de Amazon Redshift muestra que se ha completado la consulta, pero, aparentemente, la propia herramienta cliente sigue ejecutando la consulta. Los resultados de la consulta podrían ser que falta procesar o que está incompleta según cuándo se haya detenido la conexión.

Posibles soluciones:

Este problema ocurre cuando se conecta a Amazon Redshift desde una máquina que no sea una instancia de Amazon EC2. En este caso, las conexiones inactivas se terminan con un componente de red intermedio, como un firewall, tras un periodo de inactividad. Este comportamiento es normal cuando se accede desde una red privada virtual (VPN) o desde la red local.

Para evitar estos tiempos de espera, le recomendamos realizar los siguientes cambios:

- Aumentar los valores del sistema cliente que administran los tiempos de espera de TCP/IP. Realice estos cambios en el equipo que está usando para conectarse a su clúster. El periodo de tiempo de espera debe adaptarse a su cliente y su red. Para obtener más información, consulte Modificación de la configuración del tiempo de espera de TCP/IP.
- Si lo prefiere, configure el comportamiento de keepalive en el nivel de DSN. Para obtener más información, consulte Modificación de la configuración del tiempo de espera del DSN.

Modificación de la configuración del tiempo de espera de TCP/IP

Para cambiar la configuración del tiempo de espera de TCP/IP, establezca las configuraciones de tiempo de espera conforme al sistema operativo que usa para conectarse a su clúster.

- Linux: si su cliente se está ejecutando en Linux, ejecute el siguiente comando como usuario raíz para cambiar la configuración del tiempo de espera para la sesión actual:

  ```
  /sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200
   net.ipv4.tcp_keepalive_probes=5
  ```

  Para continuar con la configuración, cree o modifique el archivo `/etc/sysctl.conf` con los siguientes valores y, luego, reinicie su sistema.

  ```
  net.ipv4.tcp_keepalive_time=200
  net.ipv4.tcp_keepalive_intvl=200
  net.ipv4.tcp_keepalive_probes=5
  ```

- Windows: si su cliente se ejecuta en Windows, edite los valores para las siguientes configuraciones de registro en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \Tcpip\Parameters\:
  - KeepAliveTime: 30000
  - KeepAliveInterval: 1000
  - TcpMaxDataRetransmissions: 10

  Estas configuraciones usan tipos de datos DWORD. Si no existen en la ruta de registro, puede crear las configuraciones y especificar estos valores recomendados. Para obtener más información acerca de cómo editar el registro de Windows, consulte la documentación de Windows.

  Después de configurar estos valores, reinicie su equipo para que se apliquen los cambios.

- Mac: si su cliente se está ejecutando en una Mac, ejecute los siguientes comandos para cambiar la configuración de tiempo de espera para la sesión actual:

  ```
  sudo sysctl net.inet.tcp.keepintvl=200000
  sudo sysctl net.inet.tcp.keepidle=200000
  sudo sysctl net.inet.tcp.keepinit=200000
  ```

```
sudo sysctl net.inet.tcp.always_keepalive=1
```

Para continuar con la configuración, cree o modifique el archivo `/etc/sysctl.conf` con los siguientes valores:

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

Reinicie su equipo y, luego, ejecute los siguientes comandos para controlar que los valores están configurados.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

Modificación de la configuración del tiempo de espera del DSN

Puede configurar el comportamiento de keepalive en el nivel de DSN que elija. Puede hacerlo agregando o modificando los siguientes parámetros en el archivo odbc.ini:

KeepAlivesCount

La cantidad de paquetes keepalive de TCP que se pueden perder antes de que se considere que se interrumpió la conexión.

KeepAlivesIdle

La cantidad de segundos de inactividad antes de que el controlador envíe un paquete keepalive de TCP.

KeepAlivesInterval

La cantidad de segundos entre cada retransmisión de keepalive de TCP.

En Windows, modifique estos parámetros en el Registro agregando o modificando las claves de HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI*su_DSN*. En Linux y Mac OS, agregue o modifique estos parámetros en la entrada del DSN destino directamente en el archivo odbc.ini.

Para obtener más información acerca de cómo modificar el archivo odbc.ini en equipos Linux y Mac OS, consulte Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X.

Si estos parámetros no existen o si tienen un valor 0, el sistema usará los parámetros keepalive especificados para TCP/IP con objeto de determinar el comportamiento keepalive del DSN. En Windows, puede encontrar los parámetros TCP/IP en el registro en `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`. En Linux y Mac OS, puede encontrar los parámetros de TCP/IP en el archivo sysctl.conf.

La conexión devuelve un error o se rechaza

Ejemplos de errores

- "No se pudo establecer conexión con *`<endpoint>`*".
- "No se pudo conectar al servidor: se ha agotado el tiempo de espera. ¿El servidor se está ejecutando en el host *`'<endpoint>'`* y acepta conexiones TCP/IP en el puerto *`'<port>'`*?"
- "Conexión rechazada. Compruebe que el nombre de host y el puerto sean los correctos y que el administrador de correo acepte conexiones TCP/IP".

Posibles soluciones:

Generalmente, cuando recibe un mensaje de error indicando que hay un error al establecer una conexión, se trata de un problema con el permiso para acceder al clúster o con el tráfico de red que llega al clúster.

Para conectarse al clúster desde una herramienta cliente fuera de la red en la que se encuentra el clúster, debe agregar una regla de entrada al grupo de seguridad del clúster. La configuración de las reglas depende de si el clúster de Amazon Redshift se ha creado en una nube privada virtual (VPC):

- Si ha creado el clúster de Amazon Redshift en una nube privada virtual (VPC) basada en Amazon VPC, agregue una regla de entrada al grupo de seguridad de VPC que especifique la dirección CIDR/IP del cliente, en Amazon VPC. Para obtener más información sobre la configuración de los grupos de seguridad de la VPC para su clúster y las opciones de acceso público, consulte Administración de clústeres en una VPC.
- Si creó su clúster de Amazon Redshift fuera de una VPC, agregue su dirección CIDR/IP de cliente al grupo de seguridad del clúster en Amazon Redshift. Para obtener más información acerca de

cómo configurar los grupos de seguridad del clúster, consulte Grupos de seguridad del clúster de Amazon Redshift.

Si intenta conectarse al clúster desde una herramienta cliente que se ejecuta en una instancia de Amazon EC2, agregue también una regla de entrada. En este caso, agregue una regla al grupo de seguridad del clúster. La regla debe especificar el grupo de seguridad de Amazon EC2 asociado a la instancia de Amazon EC2 de la herramienta cliente.

En algunos casos, es posible que tenga una capa entre el cliente y el servidor, como un firewall. En estos casos, asegúrese de que el firewall acepte conexiones entrantes a través del puerto que configuró para el clúster.

El cliente y el controlador son incompatibles

Ejemplo de error

"El DSN especificado presenta una incompatibilidad de arquitectura entre el controlador y la aplicación".

Posible solución

Cuando intenta conectarse y obtiene un error sobre una discordancia de arquitectura, esto significa que la herramienta cliente y el controlador no son compatibles. Esto ocurre porque su arquitectura del sistema no coincide. Por ejemplo, esto puede ocurrir si tiene una herramienta de cliente de 32 bits, pero tiene instalada la versión de 64 bits del controlador. Algunas veces, las herramientas de cliente de 64 bits pueden usar controladores de 32 bits, pero no puede usar aplicaciones de 32 bits con controladores de 64 bits. Asegúrese de que el controlador y la herramienta de cliente estén usando la misma versión de arquitectura de sistema.

Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster

Problema de ejemplo

Tiene un problema con la finalización de las consultas. Aparentemente, las consultas se están ejecutan pero dejan de responder en la herramienta de cliente SQL. Algunas veces, las consultas no aparecen en el clúster, como en las tablas de sistema o en la consola de Amazon Redshift.

Posible solución

Este problema puede ocurrir debido a la pérdida de paquetes. En este caso, hay una diferencia en el tamaño máximo de la unidad de transmisión (MTU) en la ruta de red entre dos hosts de Internet

Protocol (IP). El tamaño de la MTU determina el tamaño máximo, en bytes, de un paquete que puede ser transferido en una trama Ethernet desde una conexión de red. En AWS, algunos tipos de instancia de Amazon EC2 admiten una MTU de 1500 (tramas Ethernet v2) y otros tipos de instancia admiten una MTU de 9001 (tramas gigantes TCP/IP).

Para evitar problemas relacionados con las diferencias en tamaños de la MTU, recomendamos realizar alguna de las siguientes operaciones:

- Si el clúster utiliza la plataforma EC2-VPC, configure el grupo de seguridad de Amazon VPC con una regla de entrada personalizada del protocolo de mensajes de control de Internet (ICMP, Internet Control Message Protocol) que devuelva `Destination Unreachable`. Por lo tanto, la regla indica al host de origen que utilice el tamaño mínimo de MTU a lo largo de la ruta de red. Para obtener más información acerca de este método, consulte Configuración de los grupos de seguridad para permitir el ICMP "Destination Unreachable".
- Si el clúster usa la plataforma EC2-Classic o si no puede permitir la regla entrante de ICMP, deshabilite las tramas gigantes TCP/IP para que se usen las tramas Ethernet v2. Para obtener más información acerca de este método, consulte Configuración de la MTU de una instancia.

Configuración de los grupos de seguridad para permitir el ICMP "Destination Unreachable"

Cuando haya una diferencia en el tamaño de la MTU en la red entre los dos hosts, primero asegúrese de que su configuración de red no bloque la detección de la MTU de la ruta (PMTUD). La PMTUD permite que el host receptor responda al host origen con el siguiente mensaje de ICMP: `Destination Unreachable: fragmentation needed and DF set (ICMP Type 3, Code 4)`. Este mensaje le indica al host origen que use el mínimo tamaño de la MTU en la ruta de la red para volver a enviar la solicitud. Sin esta negociación, puede perderse el paquete porque la solicitud es muy grande para que la acepte el host receptor. Para obtener más información acerca de este mensaje de ICMP, consulte RFC792 en el sitio web Internet Engineering Task Force (IETF).

Si no configura de forma explícita esta regla de entrada de ICMP para su grupo de seguridad de Amazon VPC, se bloquea la PMTUD. En AWS, los grupos de seguridad son como un firewall virtual que especifican reglas para controlar el tráfico entrante y saliente de una instancia. Para obtener información acerca del grupo de seguridad del clúster de Amazon Redshift, consulte Grupos de seguridad del clúster de Amazon Redshift. Para los clústeres que usan la plataforma EC2-VPC, Amazon Redshift utiliza grupos de seguridad de VPC para permitir o rechazar el tráfico al clúster. De manera predeterminada, los grupos de seguridad están bloqueados y rechazan el tráfico entrante. Para obtener información acerca de cómo configurar reglas de entrada y salida para instancias EC2-

Classic o EC2-VPC, consulte Diferencias entre instancias en EC2-Classic y una VPC en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para obtener más información acerca de cómo agregar reglas a los grupos de seguridad de VPC, consulte Administración de grupos de seguridad de VPC para un clúster. Para obtener más información acerca de la configuración específica de PMTUD que se requiere en esta regla, consulte Detección de la MTU de la ruta en la Guía del usuario de Amazon EC2 para instancias de Linux.

Configuración de la MTU de una instancia

En algunos casos, el clúster puede usar la plataforma EC2-Classic o no puede permitir la regla ICMP personalizada para el tráfico entrante. En estos casos, se recomienda ajustar la MTU a 1500 en la interfaz de red (NIC) de las instancias EC2 desde las que se conecta al clúster de Amazon Redshift. Este ajuste deshabilita las tramas gigantes TCP/IP para garantizar que las conexiones usen siempre el mismo tamaño de paquete. No obstante, esta opción reduce el rendimiento máximo de su red para toda la instancia, no solo para las conexiones a Amazon Redshift. Para obtener más información, consulte los siguientes procedimientos.

Pasos para configurar la MTU en un sistema operativo Microsoft Windows

Si su cliente se ejecuta en un sistema operativo Microsoft Windows, puede revisar y configurar el valor de la MTU para el adaptador Ethernet usando el comando `netsh`.

1. Ejecute el siguiente comando para determinar el valor actual de la MTU:

   ```
   netsh interface ipv4 show subinterfaces
   ```

2. Revise el valor de `MTU` para el adaptador `Ethernet` en la salida.
3. Si el valor no es `1500`, ejecute el siguiente comando para verlo:

   ```
   netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
   ```

   Después de configurar este valor, reinicie su equipo para que se apliquen los cambios.

Pasos para configurar la MTU en un sistema operativo Linux

Si su cliente se ejecuta en un sistema operativo Linux, puede revisar y configurar el valor de la MTU usando el comando `ip`.

1. Ejecute el siguiente comando para determinar el valor actual de la MTU:

```
$ ip link show eth0
```

2. Revise el valor posterior a `mtu` en la salida.
3. Si el valor no es `1500`, ejecute el siguiente comando para verlo:

```
$ sudo ip link set dev eth0 mtu 1500
```

Pasos para configurar la MTU en un sistema operativo Mac

- Siga las instrucciones del sitio de soporte de macOS sobre `How to change the MTU for troubleshooting purposes`. Para obtener más información, consulte el sitio web de soporte.

Configuración del parámetro de tamaño de búsqueda de la JDBC

De manera predeterminada, el controlador Java Database Connectivity (JDBC, Conectividad de base de datos java) recopila todos los resultados de una consulta a la vez. Por este motivo, cuando intenta recuperar un conjunto grande de resultados con una conexión JDBC, es posible que se produzca un error de memoria insuficiente del cliente. Para habilitar su cliente y recuperar conjuntos de resultados en lotes, en lugar de hacerlo en una única búsqueda del tipo "todo o nada", configure el parámetro de tamaño de búsqueda de la JDBC en su aplicación cliente.

> **Note**
>
> El tamaño de búsqueda no es compatible con la Open Database Connectivity (ODBC, Conectividad de base de datos abierta).

Para conseguir el mejor rendimiento, configure el tamaño de búsqueda con el valor máximo que no genere errores de memoria insuficiente. Un valor de tamaño de búsqueda inferior genera más vueltas en el servidor, lo que prolonga los tiempos de ejecución. El servidor reserva recursos, incluido el slot de consultas de Workload Management (WLM, Administración de cargas de trabajo) y la memoria asociada hasta que el cliente recupera todo el conjunto de resultados o hasta que se cancela la consulta. Cuando ajusta el tamaño de búsqueda como corresponde, esos recursos se liberan con mayor rapidez, lo que hace que queden disponibles para otras consultas.

> **Note**
>
> Si necesita extraer grandes conjuntos de datos, le recomendamos que utilice una instrucción UNLOAD para transferir los datos a Amazon S3. Cuando usa UNLOAD, los nodos de computación trabajan en paralelo para acelerar la transferencia de datos.

Para obtener más información acerca de la configuración de los parámetros de tamaño de búsqueda de JDBC, visite Getting results based on a cursor en la documentación de PostgreSQL.

Uso de la API de datos de Amazon Redshift

Puede obtener acceso a su base de datos de Amazon Redshift a través de la API de datos integrada de dicho servicio. Gracias a esta API, puede obtener acceso a los datos de Amazon Redshift con aplicaciones basadas en servicios web, entre ellas, AWS Lambda, blocs de notas de Amazon SageMaker y AWS Cloud9. Para obtener más información sobre estas aplicaciones, consulte AWS Lambda, Amazon SageMaker y AWS Cloud9.

La API de datos no requiere una conexión persistente a la base de datos. En su lugar, proporciona un punto de enlace HTTP seguro e integración con los AWS SDK. Puede usar el punto de enlace para ejecutar instrucciones SQL sin administrar conexiones. Las llamadas a la API de datos son asíncronas.

La API de datos utiliza las credenciales almacenadas en AWS Secrets Manager o las credenciales temporales de la base de datos. No es necesario transmitir contraseñas en las llamadas a la API con ninguno de los dos métodos de autorización. Para obtener más información sobre AWS Secrets Manager, consulte ¿Qué es AWS Secrets Manager? en la Guía del usuario de AWS Secrets Manager.

Para obtener más información sobre las operaciones de la API de datos, consulte Referencia de la API de datos de Amazon Redshift.

Uso de la API de datos de Amazon Redshift

Antes de utilizar la API de datos de Amazon Redshift, consulte los siguientes pasos:

1. Determine si usted, como persona que llama a la API de datos, cuenta con la autorización necesaria. Para obtener más información acerca de la autorización, consulte Autorización del acceso a la API de datos de Amazon Redshift.

2. Determine si tiene previsto llamar a la API de datos con credenciales de autenticación de Secrets Manager, o bien, con credenciales temporales. Para obtener más información, consulte Elección de las credenciales de autenticación de base de datos al llamar a la API de datos de Amazon Redshift.
3. Configure un secreto si utiliza Secrets Manager para las credenciales de autenticación. Para obtener más información, consulte Almacenamiento de credenciales de base de datos en AWS Secrets Manager.
4. Revise las consideraciones y las limitaciones que intervienen al llamar a la API de datos. Para obtener más información, consulte Consideraciones que deben tenerse en cuenta al llamar a la API de datos de Amazon Redshift.
5. Llame a la API de datos desde la AWS Command Line Interface (AWS CLI), desde su propio código o mediante el editor de consultas de la consola de Amazon Redshift. Si desea ver algunos ejemplos de llamadas desde la AWS CLI, consulte Llamadas a la API de datos.

Consideraciones que deben tenerse en cuenta al llamar a la API de datos de Amazon Redshift

Cuando llame a la API de datos, tenga en cuenta los siguientes aspectos:

- La API de datos de Amazon Redshift puede acceder a las bases de datos de los clústeres aprovisionados de Amazon Redshift y de los grupos de trabajo de Redshift sin servidor. Para obtener una lista de Regiones de AWS en las que está disponible la API de datos de Redshift, consulte los puntos de conexión enumerados para la API de datos de Redshift en la Referencia general de Amazon Web Services.
- La duración máxima de una consulta es de 24 horas.
- La cantidad máxima de consultas activas (consultas `STARTED` y `SUBMITTED`) por clúster de Amazon Redshift es de 200.
- El tamaño máximo del resultado de la consulta es 100 MB (después de la compresión gzip). Si una llamada devuelve más de 100 MB de datos como respuesta, se terminará la llamada.
- El tiempo máximo de retención de los resultados de la consulta es de 24 horas.
- El tamaño máximo de las instrucciones de la consulta es de 100 KB.
- La API de datos está disponible para consultar clústeres de uno o más nodos con los siguientes tipos de nodos:
  - dc2.large

- dc2.8xlarge
- ds2.xlarge
- ds2.8xlarge
- ra3.xlplus
- ra3.4xlarge
- ra3.16xlarge

- El clúster debe estar en una nube virtual privada (VPC) basada en el servicio Amazon VPC.
- De manera predeterminada, los usuarios que tengan el mismo rol de IAM o permisos de IAM que el ejecutor de una operación `ExecuteStatement` o `BatchExecuteStatement` de la API pueden actuar en la misma instrucción con las operaciones `CancelStatement`, `DescribeStatement`, `GetStatementResult` y `ListStatements` de la API. Para actuar sobre la misma instrucción SQL de otro usuario, el usuario debe poder asumir el rol de IAM del usuario que ejecutó la instrucción SQL. Para obtener más información sobre cómo asumir un rol, consulte Autorización del acceso a la API de datos de Amazon Redshift.
- Las instrucciones SQL del parámetro `Sqls` de la operación de la API `BatchExecuteStatement` se ejecutan como una sola transacción. Se ejecutan en serie en el orden de la matriz. Las instrucciones SQL posteriores no se inician hasta que se completa la instrucción anterior de la matriz. Si alguna instrucción SQL falla, dado que se ejecuta como una sola transacción, se deshace todo el trabajo.
- El tiempo máximo de retención de un token de cliente utilizado en una operación de API `ExecuteStatement` o `BatchExecuteStatement` es de 8 horas.
- Cada API de la API de datos de Redshift tiene una cuota de transacciones por segundo antes de limitar las solicitudes. Para conocer la cuota, consulte Cuotas para la API de datos de Amazon Redshift. Si la tasa de solicitudes supera la cuota, se devuelve una `ThrottlingException` con el código de estado HTTP 400. Para responder a la limitación, utilice una estrategia de reintentos tal como se describe en el apartado Comportamiento de los reintentos de la Guía de referencia de los SDK y las herramientas de AWS. Esta estrategia se implementa automáticamente para los errores de limitación en algunos SDK de AWS.

> **Note**
>
> De forma predeterminada, los reintentos no están habilitados en AWS Step Functions. Si necesita llamar a una API de datos de Redshift en una máquina de estados de Step Functions, incluya el parámetro de idempotencia `ClientToken` en la llamada a la API de datos de Redshift. El valor de `ClientToken` debe persistir entre los reintentos. En

el siguiente fragmento de ejemplo de una solicitud a la API `ExecuteStatement`, la expresión `States.ArrayGetItem(States.StringSplit($$.Execution.Id, ':'), 7)` utiliza una función intrínseca para extraer la parte del UUID de `$$.Execution.Id`, que es única para cada ejecución de la máquina de estado. Para obtener más información, consulte Funciones intrínsecas en la Guía para desarrolladores de AWS Step Functions.

```
{
  "Database": "dev",
  "Sql": "select 1;",
  "ClusterIdentifier": "MyCluster",
  "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
 ':'), 7)"
}
```

Elección de las credenciales de autenticación de base de datos al llamar a la API de datos de Amazon Redshift

Cuando se llama a la API de datos, se utiliza uno de los siguientes métodos de autenticación en determinadas operaciones de la API. Para cada método, se requiere una combinación diferente de parámetros.

AWS Secrets Manager

Con este método, proporcione el `secret-arn` de un secreto almacenado en AWS Secrets Manager que tenga `username` y `password`. El secreto especificado contiene las credenciales para conectarse a la `database` que se indique. Cuando se conecta a un clúster, también proporciona el nombre de la base de datos. Si proporciona un identificador de clúster (`dbClusterIdentifier`), debe coincidir con el identificador de clúster almacenado en el secreto. Cuando se conecta a un grupo de trabajo sin servidor, también proporciona el nombre de la base de datos. Para obtener más información, consulte Almacenamiento de credenciales de base de datos en AWS Secrets Manager.

Credenciales temporales

Con este método, elija una de las siguientes opciones:

- Al conectarse a un grupo de trabajo sin servidor, se especifica el nombre del grupo de trabajo y de la base de datos. El nombre de usuario de base de datos se deriva de la identidad de

IAM. Por ejemplo, `arn:iam::123456789012:user:foo` tiene el nombre de usuario de base de datos `IAM:foo`. Además, se requiere permiso para llamar a la operación `redshift-serverless:GetCredentials`.

- Al conectarse a un clúster como una identidad de IAM, especifique el identificador de clúster y el nombre de la base de datos. El nombre de usuario de base de datos se deriva de la identidad de IAM. Por ejemplo, `arn:iam::123456789012:user:foo` tiene el nombre de usuario de base de datos `IAM:foo`. Además, se requiere permiso para llamar a la operación `redshift:GetClusterCredentialsWithIAM`.
- Al conectarse a un clúster como un usuario de base de datos, especifique el identificador de clúster, el nombre de la base de datos y el nombre de usuario de base de datos. Además, se requiere permiso para llamar a la operación `redshift:GetClusterCredentials`. Para obtener información sobre cómo unir grupos de bases de datos al conectarse con este método, consulte Unión a grupos de bases de datos al conectarse a un clúster.

Con estos métodos, también puede proporcionar un valor de `region` que especifica la Región de AWS en la que se encuentran los datos.

Asignación de tipos de datos JDBC al llamar a la API de datos de Amazon Redshift

En la tabla siguiente se mapean los tipos de datos de Java Database Connectivity (JDBC) con los tipos de datos que especifica en las llamadas a la API de datos.

Tipo de datos JDBC	Tipo de datos de la API de datos
`INTEGER, SMALLINT, BIGINT`	`LONG`
`FLOAT, REAL, DOUBLE`	`DOUBLE`
`DECIMAL`	`STRING`
`BOOLEAN, BIT`	`BOOLEAN`
`BLOB, BINARY, LONGVARBINARY, VARBINARY`	`BLOB`
`VARBINARY`	`STRING`
`CLOB`	`STRING`

Tipo de datos JDBC	Tipo de datos de la API de datos
Otros tipos (incluidos los tipos relacionados con la fecha y hora)	`STRING`

Los valores de las cadenas se transmiten a la base de datos de Amazon Redshift y se convierten implícitamente en un tipo de datos de la base de datos.

> **Note**
>
> Actualmente, la API de datos no admite matrices de identificadores únicos universales (UUID).

Ejecución de instrucciones SQL con parámetros cuando se llama a la API de datos de Amazon Redshift

Puede controlar el texto SQL enviado al motor de base de datos llamando a la operación de la API de datos con los parámetros relativos a partes de la instrucción SQL. Los parámetros con nombre proporcionan una manera flexible de transmitir parámetros sin codificarlos de forma rígida en el texto SQL. Sirven para que vuelva a utilizar el texto SQL y evite los problemas de inyección SQL.

En el siguiente ejemplo, se muestran los parámetros con nombre de un campo `parameters` de un comando `execute-statement` de la AWS CLI.

```
--parameters "[{\"name\": \"id\", \"value\": \"1\"},{\"name\": \"address\", \"value\":
 \"Seattle\"}]"
```

A la hora de utilizar parámetros con nombre, tenga en cuenta lo siguiente:

- Los parámetros con nombre solo se pueden usar para reemplazar valores en las instrucciones SQL.
  - Puede reemplazar los valores en una instrucción INSERT, por ejemplo, `INSERT INTO mytable VALUES(:val1)`.

    Los parámetros con nombre pueden estar dispuestos en cualquier orden y se pueden utilizar parámetros más de una vez en el texto SQL. En la opción de parámetros que se muestra en un

ejemplo anterior, los valores 1 y `Seattle` se insertan en las columnas de tabla `id` y `address`. En el texto SQL, se especifican los parámetros con nombre de la siguiente manera:

```
--sql "insert into mytable values (:id, :address)"
```

- Puede reemplazar los valores en una cláusula de condiciones, como `WHERE attr >= :val1`, `WHERE attr BETWEEN :val1 AND :val2` y `HAVING COUNT(attr) > :val`.
- No puede reemplazar los nombres de columna en una instrucción SQL, como `SELECT column-name`, `ORDER BY column-name` o `GROUP BY column-name`.

  Por ejemplo, la siguiente instrucción SELECT tiene un error de sintaxis no válida.

  ```
  --sql "SELECT :colname, FROM event" --parameters "[{\"name\": \"colname\", \"value
  \": \"eventname\"}]"
  ```

  Si describe (operación `describe-statement`) la instrucción con el error de sintaxis, la `QueryString` que se devuelve no sustituye el nombre de columna por el parámetro (`"QueryString": "SELECT :colname, FROM event"`) y se notifica un error (ERROR: error de sintaxis en o cerca de \"FROM\"\n Posición: 12).
- No puede reemplazar los nombres de columna en una función de agregación, como `COUNT(column-name)`, `AVG(column-name)` o `SUM(column-name)`.
- No puede reemplazar los nombres de columna en una cláusula JOIN.

- Cuando se ejecuta SQL, los datos se convierten de forma implícita en un tipo de datos. Para obtener más información acerca de la conversión de tipos de datos, consulte Tipos de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- No se puede establecer un valor en NULL. La API de datos lo interpreta como la cadena literal `NULL`. En el siguiente ejemplo, se reemplaza `id` con la cadena literal `null`. No con el valor NULL de SQL.

  ```
  --parameters "[{\"name\": \"id\", \"value\": \"null\"}]"
  ```
- No se puede establecer un valor de longitud cero. Se produce un error en la instrucción SQL de la API de datos. En el siguiente ejemplo, se intenta establecer `id` con un valor de longitud cero y se produce un error en la instrucción SQL.

  ```
  --parameters "[{\"name\": \"id\", \"value\": \"\"}]"
  ```

- No se puede establecer un nombre de tabla en la instrucción SQL con un parámetro. La API de datos cumple la regla de JDBC `PreparedStatement`.
- La salida de la operación `describe-statement` devuelve los parámetros de consulta de una instrucción SQL.
- Solo la operación `execute-statement` admite instrucciones SQL con parámetros.

Ejecución de instrucciones SQL con un token de idempotencia cuando se llama a la API de datos de Amazon Redshift

Cuando realiza una solicitud de API de mutación, la solicitud suele devolver un resultado antes de que se hayan completado los flujos de trabajo asíncronos de la operación. También es posible que se agote el tiempo de espera de las operaciones o que surjan otros problemas con el servidor antes de que finalicen, aunque la solicitud ya haya devuelto un resultado. Esto podría dificultar la determinación de si la solicitud se ha realizado correctamente o no, y podría dar lugar a múltiples reintentos para garantizar que la operación se completa correctamente. No obstante, si la solicitud original y los reintentos posteriores se realizan correctamente, la operación se completa varias veces. Esto significa que podría actualizar más recursos de los previstos.

La idempotencia garantiza que una solicitud a la API no se complete más de una vez. Con una solicitud idempotente, si la solicitud original se completa correctamente, cualquier reintento posterior también se completa correctamente sin realizar ninguna otra acción. Las operaciones `ExecuteStatement` y `BatchExecuteStatement` de la API de datos tienen un parámetro idempotente `ClientToken` opcional. `ClientToken` caduca a las 8 horas.

> **Important**
>
> Si llama a las operaciones `ExecuteStatement` y `BatchExecuteStatement` desde un SDK de AWS, este genera automáticamente un token de cliente para utilizarlo en el reintento. En este caso, no recomendamos utilizar el parámetro `client-token` con las operaciones `ExecuteStatement` y `BatchExecuteStatement`. Consulte el registro de CloudTrail para ver `ClientToken`. Para ver un ejemplo de registro de CloudTrail, consulte Ejemplo de la API de datos de Amazon Redshift.

El siguiente comando `execute-statement` de la AWS CLI ilustra el parámetro `client-token` opcional para idempotencia.

```
aws redshift-data execute-statement
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --sql "select * from stl_query limit 1"
    --database dev
    --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

En la siguiente tabla se muestran algunas respuestas comunes que puede obtener para solicitudes de API idempotentes y se ofrecen recomendaciones de reintento.

Respuesta	Recomendación	Comentarios
200 (OK)	No reintentar	La solicitud original se ha completado correctamente. Cualquier reintento posterior se devuelve correctamente.
Códigos de respuesta de la serie 400	No reintentar	Hay un problema con la solicitud, uno de los siguientes: • Incluye un parámetro o una combinación de parámetros que no es válida. • Utiliza una acción o un recurso para el que no tiene permisos. • Utiliza un recurso que está en proceso de cambiar de estado. Si la solicitud implica un recurso que está en proceso de cambiar de estado, el reintento de la solicitud podría realizarse correctamente.
Códigos de respuesta de la serie 500	Reintentar	El error se debe a un problema en el servidor de AWS y suele ser transitorio. Repita la solicitud con una estrategia de retardo adecuada.

Para obtener información sobre los códigos de respuesta de Amazon Redshift, consulte Common Errors (Errores comunes) en Amazon Redshift API Reference (Referencia de la API de Amazon Redshift).

Autorización del acceso a la API de datos de Amazon Redshift

Para poder obtener acceso a la API de datos, el usuario debe contar con la autorización respectiva. Puede autorizar a un usuario a obtener acceso a la API de datos si agrega la política administrada, que es una política de AWS Identity and Access Management (IAM) predefinida, a ese usuario. Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift. Para ver los permisos permitidos y denegados por las políticas administradas, consulte la consola de IAM (https://console.aws.amazon.com/iam/).

Amazon Redshift proporciona la política administrada `AmazonRedshiftDataFullAccess`. Esta política proporciona acceso pleno a las operaciones de la API de datos de Amazon Redshift. Esta política también permite el acceso limitado a operaciones específicas de la API de Amazon Redshift, AWS Secrets Manager e IAM que se necesitan para autenticar y obtener acceso a un clúster de Amazon Redshift o a un grupo de trabajo de Redshift sin servidor.

También puede crear una política de IAM propia que permita obtener acceso a recursos específicos. Para crear su política, utilice la política `AmazonRedshiftDataFullAccess` como la plantilla de partida. Una vez creada la política, agréguela a todos los usuarios que deban acceder a la API de datos.

Tenga en cuenta los siguientes requisitos de la política de IAM asociada al usuario:

- Si se utiliza AWS Secrets Manager para la autenticación, confirmar la política permite que se use la acción `secretsmanager:GetSecretValue` para recuperar el secreto etiquetado con la clave `RedshiftDataFullAccess`.
- Si se utilizan credenciales temporales para autenticar un clúster, confirmar la política permite el uso de la acción `redshift:GetClusterCredentials` en el nombre de usuario de base de datos `redshift_data_api_user` correspondiente a cualquiera de las bases de datos del clúster. Es necesario que este nombre de usuario ya se haya creado en su base de datos.
- Si utiliza credenciales temporales para autenticarse en un grupo de trabajo sin servidor, confirme que la política permite el uso de la acción `redshift-serverless:GetCredentials` para recuperar el grupo de trabajo etiquetado con la clave `RedshiftDataFullAccess`. El usuario

de la base de datos se asigna 1:1 a la identidad de AWS Identity and Access Management (IAM) de origen. Por ejemplo, el usuario sample_user se asigna al usuario `IAM:sample_user` de la base de datos y el rol de IAM sample_role se asigna a `IAMR:sample_role`. Para obtener más información acerca de las identidades de IAM, consulte Identidades (usuarios, grupos de usuarios y roles) en la Guía del usuario de IAM.

Para ejecutar una consulta en un clúster que es propiedad de otra cuenta, la cuenta propietaria debe proporcionar un rol de IAM que la API de datos pueda asumir en la cuenta que llama. Por ejemplo, supongamos que la cuenta B posee un clúster al que la cuenta A necesita acceder. La cuenta B puede adjuntar la política administrada por AWS `AmazonRedshiftDataFullAccess` al rol de IAM de la cuenta B. A continuación, la cuenta B se fía de la cuenta A gracias a una política de confianza como la siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Por último, el rol de IAM de la cuenta A debe ser capaz de asumir el rol de IAM de la cuenta B.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

En los siguientes enlaces, encontrará más información sobre AWS Identity and Access Management en la Guía del usuario de IAM.

- Para obtener más información sobre cómo crear roles de IAM, consulte Creación de roles de IAM.
- Para obtener más información sobre cómo crear una política de IAM, consulte Creación de políticas de IAM.
- Para obtener información sobre cómo agregar una política de IAM a un usuario, consulte Adición y eliminación de permisos de identidad de IAM.

Almacenamiento de credenciales de base de datos en AWS Secrets Manager

Al llamar a la API de datos, puede transmitir las credenciales del clúster o grupo de trabajo sin servidor con un secreto en AWS Secrets Manager. Para pasar credenciales mediante este método, especifique el nombre del secreto o el Nombre de recurso de Amazon (ARN) del secreto.

Para almacenar credenciales con Secrets Manager, se necesita contar con el permiso de la política administrada `SecretManagerReadWrite`. Para obtener más información sobre los permisos mínimos, consulte Creación y administración de secretos con AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Si desea almacenar las credenciales en un secreto para un clúster de Amazon Redshift

1. Utilice la consola de AWS Secrets Manager para crear un secreto que contenga credenciales para el clúster:

   - Cuando elija Store a new secret (Almacenar un secreto nuevo), elija Credentials for Redshift cluster (Credenciales para clúster de Redshift).
   - Almacene sus valores para User name (Nombre de usuario) que es el usuario de la base de datos, Password (Contraseña) y DB cluster (Clúster de base de datos) que es el identificador del clúster, en su secreto.
   - Etiquete el secreto con la clave `RedshiftDataFullAccess`. La política administrada por AWS `AmazonRedshiftDataFullAccess` solo permite la acción `secretsmanager:GetSecretValue` para los secretos etiquetados con la clave `RedshiftDataFullAccess`.

   Para obtener instrucciones, consulte Creación de un secreto básico en la Guía del usuario de AWS Secrets Manager.

2. Utilice la consola de AWS Secrets Manager para ver los detalles del secreto que ha creado, o ejecute el comando de la AWS CLI `aws secretsmanager describe-secret`.

   Anote el nombre y el ARN del secreto. Puede utilizarlos en las llamadas a la API de datos.

Para almacenar las credenciales en un secreto para un grupo de trabajo sin servidor

1. Utilice los comandos de la AWS CLI de AWS Secrets Manager para almacenar un secreto que contenga credenciales para el grupo de trabajo sin servidor:

   - Cree su secreto en un archivo, por ejemplo, un archivo JSON llamado `mycreds.json`. Proporcione los valores de User name (Nombre de usuario) (usuario de base de datos) y Password (Contraseña) en el archivo.

     ```
     {
           "username": "myusername",
           "password": "mypassword"
     }
     ```

   - Almacene los valores en el secreto y etiquete el secreto con la clave `RedshiftDataFullAccess`.

     ```
     aws secretsmanager create-secret --name MyRedshiftSecret  --tags
      Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
     mycreds.json
     ```

     El ejemplo siguiente muestra la salida.

     ```
     {
         "ARN":
      "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
         "Name": "MyRedshiftSecret",
         "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
     }
     ```

   Para obtener más información, consulte Creación de un secreto básico con AWS CLI en la Guía del usuario de AWS Secrets Manager.

2. Utilice la consola de AWS Secrets Manager para ver los detalles del secreto que ha creado, o ejecute el comando de la AWS CLI `aws secretsmanager describe-secret`.

   Anote el nombre y el ARN del secreto. Puede utilizarlos en las llamadas a la API de datos.

Creación de un punto de enlace de la VPC de Amazon VPC (AWS PrivateLink) para la API de datos

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS, como clústeres y aplicaciones de Amazon Redshift, en una nube virtual privada (VPC). AWS PrivateLink proporciona conectividad segura y privada entre las nubes virtuales privadas (VPC) y los servicios de AWS a través de la red de Amazon. Con AWS PrivateLink, puede crear puntos de enlace de la VPC que puede utilizar para conectarse a servicios a través de diferentes cuentas y VPC basadas en Amazon VPC. Para obtener más información acerca de AWS PrivateLink, consulte Servicios de punto de enlace de la VPC (AWS PrivateLink) en la guía del usuario de Amazon Virtual Private Cloud.

Puede llamar a la API de datos con los puntos de enlace de la Amazon VPC. El uso de un punto de enlace de la Amazon VPC mantiene el tráfico entre las aplicaciones de su Amazon VPC y la API de datos en la red de AWS, sin usar direcciones IP públicas. Los puntos de enlace de la Amazon VPC pueden ayudarle a cumplir los requisitos reglamentarios y de conformidad relacionados con la limitación de la conectividad a internet público. Por ejemplo, si utiliza un punto de enlace de la Amazon VPC, puede mantener el tráfico entre una aplicación que se ejecuta en una instancia Amazon EC2 y la API de datos en las VPC donde se contienen.

Después de crear el punto de enlace de la Amazon VPC, puede comenzar a usarlo sin realizar ningún cambio de código o configuración en la aplicación.

Para crear un punto de enlace de la Amazon VPC para la API de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija Endpoints (Puntos de enlace) y, a continuación, elija Create Endpoint (Crear punto de enlace).
3. En la página Create Endpoint (Crear punto de enlace), en Service category (Categoría de servicio), elija AWS services(Servicios de AWS). En Service Name (Nombre del servicio), elija redshift-data (`com.amazonaws.region.redshift-data`).
4. Para VPC, elija la VPC en la que crear el punto de enlace.

Elija la VPC que contiene la aplicación que realiza llamadas a la API de datos.

5. En Subnets (Subredes), elija la subred para cada zona de disponibilidad (AZ) utilizada por el servicio de AWS que ejecuta la aplicación.

   Para crear un punto de enlace de la VPC de Amazon VPC, especifique el rango de direcciones IP privadas con las que se puede acceder al punto de enlace. Para ello, elija la subred para cada zona de disponibilidad. Al hacerlo, se restringe el punto de enlace de la VPC al rango de direcciones IP privadas específico de cada zona de disponibilidad y también se crea un punto de enlace de la Amazon VPC en cada zona de disponibilidad.

6. En Enable Private DNS Name (Habilitar nombre de DNS privado), seleccione Enable for this endpoint (Habilitar para este punto de enlace).

   El DNS privado resuelve el nombre de host de DNS de la API de datos estándar (`https://redshift-data.region.amazonaws.com`) en las direcciones IP privadas asociadas con el nombre de host de DNS específico del punto de enlace de la Amazon VPC. Como resultado, puede acceder al punto de enlace de la VPC de la API de datos utilizando los SDK de AWS CLI o la AWS sin realizar ningún cambio de código o configuración para actualizar la URL del punto de enlace de la API de datos.

7. En Security group (Grupo de seguridad), elija los grupos de seguridad que deban asociarse al punto de enlace de la Amazon VPC.

   Elija el grupo de seguridad que permita el acceso al servicio de AWS que ejecuta la aplicación. Por ejemplo, si una instancia Amazon EC2 está ejecutando la aplicación, elija el grupo de seguridad que permita el acceso a la instancia Amazon EC2. El grupo de seguridad le permite controlar el tráfico al punto de enlace de la Amazon VPC desde los recursos de la VPC.

8. Elija Create endpoint (Crear punto de enlace).

Una vez creado el punto de enlace, elija el vínculo en la AWS Management Console para ver los detalles del punto de enlace.

La ficha Details (Detalles) del punto de enlace muestra los nombres de host de DNS que se generaron al crear el punto de enlace de la Amazon VPC.

Puede utilizar el punto de enlace estándar (`redshift-data.region.amazonaws.com`) o uno de los puntos de enlace específicos de la VPC para llamar a la API de datos dentro de la Amazon VPC. El punto de enlace de la API de datos estándar se dirige automáticamente al punto de enlace

de la Amazon VPC. Este enrutamiento se produce porque cuando se creó el punto de enlace de la Amazon VPC se habilitó el nombre de host de DNS privado.

Cuando utiliza un punto de enlace de la Amazon VPC en una llamada a la API de datos, todo el tráfico entre la aplicación y la API de datos permanece en las Amazon VPC donde se contienen. Puede usar un punto de enlace de la Amazon VPC para cualquier tipo de llamada a la API de datos. Para obtener más información sobre la llamada a la API de datos, consulte Consideraciones que deben tenerse en cuenta al llamar a la API de datos de Amazon Redshift.

Unión a grupos de bases de datos al conectarse a un clúster

Los grupos de bases de datos son colecciones de usuarios de bases de datos. Se pueden conceder privilegios de base de datos a los grupos. Un administrador puede configurar un rol de IAM para que estos grupos de bases de datos se tengan en cuenta cuando su código SQL se ejecute con la API de datos. Para obtener más información sobre los grupos de bases de datos, consulte Grupos en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Puede configurar el rol de IAM del intermediario de la API de datos para que el usuario de base de datos especificado en la llamada se una a los grupos de bases de datos cuando la API de datos se conecte a un clúster. Esta capacidad solo se admite cuando se conecta a clústeres aprovisionados. No es compatible cuando se conecta a grupos de trabajo de Redshift sin servidor. El rol de IAM del intermediario de la API de datos también debe permitir la acción `redshift:JoinGroup`.

Agregue etiquetas a los roles de IAM para configurarlo. El administrador del rol de IAM del intermediario agrega etiquetas con la clave `RedshiftDbGroups` y un valor de clave de una lista de grupos de bases de datos. El valor es una lista de nombres de grupos de bases de datos separados por dos puntos (:) hasta una longitud total de 256 caracteres. Los grupos de bases de datos deben estar previamente definidos en la base de datos conectada. Si algún grupo especificado no se encuentra en la base de datos, se omite. Por ejemplo, para los grupos de bases de datos `accounting` y `retail`, la clave-valor es `accounting:retail`. El par clave-valor de etiqueta `{"Key":"RedshiftDbGroups","Value":"accounting:retail"}` lo utiliza la API de datos para determinar qué grupos de base de datos están asociados al usuario de base de datos proporcionado en la llamada a la API de datos.

Para agregar grupos de bases de datos como etiquetas a un rol de IAM

1. Inicie sesión en AWS Management Console y abra la consola IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de la consola, elija Roles (Roles) y, a continuación, elija el nombre de la entidad que desea editar.
3. Elija la pestaña Etiquetas y, a continuación, Administrar etiquetas.
4. Elija Agregar etiqueta y, a continuación, agregue la clave RedshiftDbGroups y un valor que sea una *lista de grupos de bases de datos separados por dos puntos*.
5. Elija Guardar cambios.

   Ahora, cuando una entidad principal de IAM (con este rol de IAM asociado) llama a la API de datos, el usuario de base de datos especificado se une a los grupos de base de datos indicados en el rol de IAM.

Para obtener más información sobre cómo adjuntar una etiqueta a una entidad principal, incluidos los roles de IAM y los usuarios de IAM, consulte Etiquetado de recursos de IAM en la Guía del usuario de IAM.

Llamadas a la API de datos

Se puede llamar a la API de datos o a la AWS CLI a fin de ejecutar instrucciones SQL en el clúster o grupo de trabajo sin servidor. Las operaciones principales para ejecutar instrucciones SQL son `ExecuteStatement` y `BatchExecuteStatement` en la Referencia de API de datos de Amazon Redshift. La API de datos admite los lenguajes de programación compatibles con el AWS SDK. Para obtener más información sobre estos, consulte Herramientas para crear en AWS.

Para ver ejemplos de código de llamadas a la API de datos, consulte la Introducción a la API de datos de Redshift en GitHub. Este repositorio contiene ejemplos de uso de AWS Lambda para acceder a los datos de Amazon Redshift desde Amazon EC2, AWS Glue Data Catalog y Amazon SageMaker Runtime. Los lenguajes de programación de ejemplo incluyen Python, Go, Java y Javascript.

Puede llamar a la API de datos utilizando la AWS CLI.

En los siguientes ejemplos, se utiliza la AWS CLI para llamar a la API de datos. Para ejecutar los ejemplos, edite los valores de los parámetros para que se ajusten a su entorno. En muchos de los ejemplos se proporciona un `cluster-identifier` que se ejecuta en un clúster. Cuando se ejecuta en un grupo de trabajo sin servidor, se debe proporcionar un `workgroup-name` en su lugar. En estos ejemplos, se demuestran algunas de las operaciones de la API de datos. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

Los comandos que figuran en los siguientes ejemplos se han dividido y se han formateado para facilitar su lectura.

Para ejecutar una instrucción SQL

Para ejecutar una instrucción SQL, utilice el comando AWS CLI de la `aws redshift-data execute-statement`.

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster y devuelve un identificador que permite obtener los resultados. En este ejemplo, se utiliza el método de autenticación de AWS Secrets Manager.

```
aws redshift-data execute-statement
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --sql "select * from stl_query limit 1"
    --database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598323175.823,
    "Database": "dev",
    "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
    "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-
hKgPWn"
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster y devuelve un identificador que permite obtener los resultados. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data execute-statement
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
```

```
    --sql "select * from stl_query limit 1"
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un grupo de trabajo sin servidor y devuelve un identificador que permite obtener los resultados. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data execute-statement
    --database dev
    --workgroup-name myworkgroup
    --sql "select 1;"
```

A continuación se muestra un ejemplo de respuesta.

```
{
 "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
 "Database": "dev",
 "DbUser": "IAMR:RoleName",
 "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
 "WorkgroupName": "myworkgroup"
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster y devuelve un identificador que permite obtener los resultados. En este ejemplo se utiliza el método de autenticación de AWS Secrets Manager y un token de idempotencia.

```
aws redshift-data execute-statement
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
```

```
    --sql "select * from stl_query limit 1"
    --database dev
    --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598323175.823,
    "Database": "dev",
    "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
    "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-
hKgPWn"
}
```

Para ejecutar una instrucción SQL con parámetros

Para ejecutar una instrucción SQL, utilice el comando AWS CLI de la `aws redshift-data execute-statement`.

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster y devuelve un identificador que permite obtener los resultados. En este ejemplo, se utiliza el método de autenticación de AWS Secrets Manager. El texto SQL tiene el parámetro con nombre `distance`. En este caso, la distancia utilizada en el predicado es `5`. En una instrucción SELECT, los parámetros con nombre de los nombres de columna solo se pueden usar en el predicado. Los valores de los parámetros con nombre para la instrucción SQL se especifican en la opción `parameters`.

```
aws redshift-data execute-statement
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --sql "SELECT ratecode FROM demo_table WHERE trip_distance > :distance"
    --parameters "[{\"name\": \"distance\", \"value\": \"5\"}]"
    --database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598323175.823,
```

```
    "Database": "dev",
    "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
    "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-
hKgPWn"
}
```

En el siguiente ejemplo, se utiliza la tabla EVENT de la base de datos de muestra. Para obtener más información, consulte Tabla EVENT en la Guía para desarrolladores de bases de datos de Amazon Redshift..

Si aún no dispone de una tabla EVENT en la base de datos, puede crear una con la API de datos de la siguiente manera:

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "create table event( eventid integer not null distkey,
                           venueid smallint not null,
                           catid smallint not null,
                           dateid smallint not null sortkey,
                           eventname varchar(200),
                           starttime timestamp)"
```

El siguiente comando inserta una fila en la tabla EVENT.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event
 values(:eventid, :venueid::smallint, :catid, :dateid, :eventname, :starttime)"
--parameters "[{\"name\": \"eventid\", \"value\": \"1\"}, {\"name\": \"venueid\",
 \"value\": \"1\"},
              {\"name\": \"catid\", \"value\": \"1\"},
              {\"name\": \"dateid\", \"value\": \"1\"},
              {\"name\": \"eventname\", \"value\": \"event 1\"},
              {\"name\": \"starttime\", \"value\": \"2022-02-22\"}]"
```

El siguiente comando inserta una segunda fila en la tabla EVENT. Este ejemplo hace lo siguiente:

- El parámetro con nombre `id` se utiliza cuatro veces en el texto SQL.
- La conversión del tipo implícita se aplica automáticamente cuando se inserta un parámetro `starttime`.
- La columna `venueid` se convierte en un tipo de datos SMALLINT.
- Las cadenas de caracteres que representan el tipo de datos DATE se convierten de forma implícita en el tipo de datos TIMESTAMP.
- Los comentarios se pueden emplear en el texto SQL.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event values(:id, :id::smallint, :id, :id, :eventname, :starttime) /
*this is comment, and it won't apply parameterization for :id, :eventname or :starttime
 here*/"
--parameters "[{\"name\": \"eventname\", \"value\": \"event 2\"},
              {\"name\": \"starttime\", \"value\": \"2022-02-22\"},
              {\"name\": \"id\", \"value\": \"2\"}]"
```

A continuación, se muestran las dos filas que se han insertado:

```
 eventid | venueid | catid | dateid | eventname |      starttime
---------+---------+-------+--------+-----------+---------------------
       1 |       1 |     1 |      1 | event 1   | 2022-02-22 00:00:00
       2 |       2 |     2 |      2 | event 2   | 2022-02-22 00:00:00
```

El siguiente comando utiliza un parámetro con nombre en una cláusula WHERE que permite recuperar la fila donde `eventid` es 1.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
```

```
--sql "select * from event where eventid=:id"
--parameters "[{\"name\": \"id\", \"value\": \"1\"}]"
```

Ejecute el siguiente comando para obtener los resultados SQL de la instrucción SQL precedente:

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Proporciona los siguientes resultados:

```
{
    "Records": [
        [
            {
                "longValue": 1
            },
            {
                "longValue": 1
            },
            {
                "longValue": 1
            },
            {
                "longValue": 1
            },
            {
                "stringValue": "event 1"
            },
            {
                "stringValue": "2022-02-22 00:00:00.0"
            }
        ]
    ],
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "eventid",
            "length": 0,
            "name": "eventid",
```

```
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "venueid",
            "length": 0,
            "name": "venueid",
            "nullable": 0,
            "precision": 5,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int2"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "catid",
            "length": 0,
            "name": "catid",
            "nullable": 0,
            "precision": 5,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int2"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "dateid",
            "length": 0,
            "name": "dateid",
            "nullable": 0,
            "precision": 5,
```

```
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "int2"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "eventname",
            "length": 0,
            "name": "eventname",
            "nullable": 1,
            "precision": 200,
            "scale": 0,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "varchar"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "label": "starttime",
            "length": 0,
            "name": "starttime",
            "nullable": 1,
            "precision": 29,
            "scale": 6,
            "schemaName": "public",
            "tableName": "event",
            "typeName": "timestamp"
        }
    ],
    "TotalNumRows": 1
}
```

Para ejecutar varias instrucciones SQL

Para ejecutar varias instrucciones SQL con un solo comando, utilice el comando `aws redshift-data batch-execute-statement` de la AWS CLI.

El siguiente comando de la AWS CLI ejecuta tres instrucciones SQL en un clúster y devuelve un identificador que permite obtener los resultados. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data batch-execute-statement
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --sqls "set timezone to BST" "select * from mytable" "select * from another_table"
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Database": "dev",
    "DbUser": "myuser",
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Para enumerar metadatos relativos a las instrucciones SQL

Para enumerar los metadatos relativos a las instrucciones SQL, utilice el comando `aws redshift-data list-statements` de la AWS CLI. La autorización para ejecutar este comando se basa en los permisos de IAM de la persona que llama.

El siguiente comando de la AWS CLI enumera las instrucciones SQL que se ejecutaron.

```
aws redshift-data list-statements
    --region us-west-2
    --status ALL
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Statements": [
        {
            "CreatedAt": 1598306924.632,
```

```
            "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
            "QueryString": "select * from stl_query limit 1",
            "Status": "FINISHED",
            "UpdatedAt": 1598306926.667
        },
        {
            "CreatedAt": 1598311717.437,
            "Id": "e0ebd578-58b3-46cc-8e52-8163fd7e01aa",
            "QueryString": "select * from stl_query limit 1",
            "Status": "FAILED",
            "UpdatedAt": 1598311719.008
        },
        {
            "CreatedAt": 1598313683.65,
            "Id": "c361d4f7-8c53-4343-8c45-6b2b1166330c",
            "QueryString": "select * from stl_query limit 1",
            "Status": "ABORTED",
            "UpdatedAt": 1598313685.495
        },
        {
            "CreatedAt": 1598306653.333,
            "Id": "a512b7bd-98c7-45d5-985b-a715f3cfde7f",
            "QueryString": "select 1",
            "Status": "FINISHED",
            "UpdatedAt": 1598306653.992
        }
    ]
}
```

Para describir metadatos relativos a una instrucción SQL

Para obtener descripciones de los metadatos de una instrucción SQL, utilice el comando `aws redshift-data describe-statement` de la AWS CLI. La autorización para ejecutar este comando se basa en los permisos de IAM de la persona que llama.

El siguiente comando de la AWS CLI describe una instrucción SQL.

```
aws redshift-data describe-statement
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ClusterIdentifier": "mycluster-test",
    "CreatedAt": 1598306924.632,
    "Duration": 1095981511,
    "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
    "QueryString": "select * from stl_query limit 1",
    "RedshiftPid": 20859,
    "RedshiftQueryId": 48879,
    "ResultRows": 1,
    "ResultSize": 4489,
    "Status": "FINISHED",
    "UpdatedAt": 1598306926.667
}
```


A continuación, se muestra un ejemplo de una respuesta `describe-statement` que surge después de ejecutar un comando `batch-execute-statement` con varias instrucciones SQL.


```
{
    "ClusterIdentifier": "mayo",
    "CreatedAt": 1623979777.126,
    "Duration": 6591877,
    "HasResultSet": true,
    "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
    "RedshiftPid": 31459,
    "RedshiftQueryId": 0,
    "ResultRows": 2,
    "ResultSize": 22,
    "Status": "FINISHED",
    "SubStatements": [
        {
            "CreatedAt": 1623979777.274,
            "Duration": 3396637,
            "HasResultSet": true,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:1",
            "QueryString": "select 1;",
            "RedshiftQueryId": -1,
            "ResultRows": 1,
            "ResultSize": 11,
            "Status": "FINISHED",
            "UpdatedAt": 1623979777.903
        },
        {
            "CreatedAt": 1623979777.274,
```

```
            "Duration": 3195240,
            "HasResultSet": true,
            "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
            "QueryString": "select 2;",
            "RedshiftQueryId": -1,
            "ResultRows": 1,
            "ResultSize": 11,
            "Status": "FINISHED",
            "UpdatedAt": 1623979778.076
        }
    ],
    "UpdatedAt": 1623979778.183
}
```

Para obtener los resultados de una instrucción SQL

Para obtener el resultado de una instrucción SQL que ya se ejecutó, utilice el comando `redshift-data get-statement-result` de la AWS CLI. Puede proporcionar un `Id` que reciba en respuesta a `execute-statement` o `batch-execute-statement`. El valor `Id` para una instrucción SQL ejecutada por `batch-execute-statement` se puede recuperar en el resultado de `describe-statement` y lleva como sufijo dos puntos y un número de secuencia, como `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2`. Si ejecuta varias instrucciones SQL con `batch-execute-statement`, cada una de ellas tiene un valor `Id` como se muestra en `describe-statement`. La autorización para ejecutar este comando se basa en los permisos de IAM de la persona que llama.

La siguiente instrucción devuelve el resultado de una instrucción SQL que se ejecuta mediante `execute-statement`.

```
aws redshift-data get-statement-result
    --id d9b6c0c9-0747-4bf4-b142-e8883122f766
    --region us-west-2
```

La siguiente instrucción devuelve el resultado de la segunda instrucción SQL que se ejecuta mediante `batch-execute-statement`.

```
aws redshift-data get-statement-result
    --id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
```

```
    --region us-west-2
```

A continuación, se muestra un ejemplo de una respuesta a una llamada a `get-statement-result`.

```
{
    "ColumnMetadata": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "userid",
            "length": 0,
            "name": "userid",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "query",
            "length": 0,
            "name": "query",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "label",
            "length": 0,
            "name": "label",
            "nullable": 0,
```

```
            "precision": 320,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "bpchar"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "xid",
            "length": 0,
            "name": "xid",
            "nullable": 0,
            "precision": 19,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int8"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "pid",
            "length": 0,
            "name": "pid",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "database",
            "length": 0,
            "name": "database",
            "nullable": 0,
            "precision": 32,
            "scale": 0,
```

```
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "bpchar"
        },
        {
            "isCaseSensitive": true,
            "isCurrency": false,
            "isSigned": false,
            "label": "querytxt",
            "length": 0,
            "name": "querytxt",
            "nullable": 0,
            "precision": 4000,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "bpchar"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "label": "starttime",
            "length": 0,
            "name": "starttime",
            "nullable": 0,
            "precision": 29,
            "scale": 6,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "timestamp"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "label": "endtime",
            "length": 0,
            "name": "endtime",
            "nullable": 0,
            "precision": 29,
            "scale": 6,
            "schemaName": "",
            "tableName": "stll_query",
```

```
            "type": 93,
            "typeName": "timestamp"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "aborted",
            "length": 0,
            "name": "aborted",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "insert_pristine",
            "length": 0,
            "name": "insert_pristine",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": true,
            "label": "concurrency_scaling_status",
            "length": 0,
            "name": "concurrency_scaling_status",
            "nullable": 0,
            "precision": 10,
            "scale": 0,
            "schemaName": "",
            "tableName": "stll_query",
            "typeName": "int4"
```

```
        }
    ],
    "Records": [
        [
            {
                "longValue": 1
            },
            {
                "longValue": 3
            },
            {
                "stringValue": "health"
            },
            {
                "longValue": 1023
            },
            {
                "longValue": 15279
            },
            {
                "stringValue": "dev"
            },
            {
                "stringValue": "select system_status from stv_gui_status;"
            },
            {
                "stringValue": "2020-08-21 17:33:51.88712"
            },
            {
                "stringValue": "2020-08-21 17:33:52.974306"
            },
            {
                "longValue": 0
            },
            {
                "longValue": 0
            },
            {
                "longValue": 6
            }
        ]
    ],
    "TotalNumRows": 1
```

```
}
```

Para describir una tabla

Para obtener los metadatos que describen una tabla, utilice el comando `aws redshift-data describe-table` de la AWS CLI.

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster y devuelve los metadatos que describen una tabla. En este ejemplo, se utiliza el método de autenticación de AWS Secrets Manager.

```
aws redshift-data describe-table
    --region us-west-2
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ColumnList": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_id",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
```

```
            "length": 2147483647,
            "name": "feature_name",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        }
    ]
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster que describe una tabla. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data describe-table
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
    --table sql_features
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "ColumnList": [
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_id",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
```

```
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "feature_name",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "sub_feature_id",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "sub_feature_name",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "is_supported",
            "nullable": 1,
```

```
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "is_verified_by",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        },
        {
            "isCaseSensitive": false,
            "isCurrency": false,
            "isSigned": false,
            "length": 2147483647,
            "name": "comments",
            "nullable": 1,
            "precision": 2147483647,
            "scale": 0,
            "schemaName": "information_schema",
            "tableName": "sql_features",
            "typeName": "character_data"
        }
    ]
}
```

Para enumerar las bases de datos de un clúster

Para enumerar las bases de datos de un clúster, utilice el comando `aws redshift-data list-databases` de la AWS CLI.

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster para mostrar bases de datos. En este ejemplo, se utiliza el método de autenticación de AWS Secrets Manager.

```
aws redshift-data list-databases
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Databases": [
        "dev"
    ]
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster para mostrar bases de datos. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data list-databases
    --region us-west-2
    --db-user myuser
    --cluster-identifier mycluster-test
    --database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Databases": [
        "dev"
    ]
}
```

Para enumerar los esquemas de una base de datos

Para enumerar los esquemas de una base de datos, utilice el comando `aws redshift-data list-schemas` de la AWS CLI.

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster para mostrar esquemas en una base de datos. En este ejemplo, se utiliza el método de autenticación de AWS Secrets Manager.

```
aws redshift-data list-schemas
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster para mostrar esquemas en una base de datos. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data list-schemas
    --region us-west-2
    --db-user mysuser
    --cluster-identifier mycluster-test
    --database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Schemas": [
        "information_schema",
        "pg_catalog",
        "pg_internal",
        "public"
    ]
}
```

Para enumerar las tablas de una base de datos

Para enumerar las tablas de una base de datos, utilice el comando `aws redshift-data list-tables` de la AWS CLI.

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster para mostrar tablas en una base de datos. En este ejemplo, se utiliza el método de autenticación de AWS Secrets Manager.

```
aws redshift-data list-tables
    --region us-west-2
    --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
    --cluster-identifier mycluster-test
    --database dev
    --schema information_schema
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
}
```

El siguiente comando de la AWS CLI ejecuta una instrucción SQL en un clúster para mostrar tablas en una base de datos. En este ejemplo, se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data list-tables
     --region us-west-2
     --db-user myuser
```

```
     --cluster-identifier mycluster-test
     --database dev
     --schema information_schema
```

A continuación se muestra un ejemplo de respuesta.

```
{
    "Tables": [
        {
            "name": "sql_features",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        },
        {
            "name": "sql_implementation_info",
            "schema": "information_schema",
            "type": "SYSTEM TABLE"
        }
    ]
}
```

Solución de problemas de la API de datos de Amazon Redshift

Use las siguientes secciones, tituladas con mensajes de error comunes, para ayudar a solucionar problemas que tenga con la API de datos.

Temas

- El paquete de la consulta es demasiado grande
- Límite de tamaño superado de respuesta de base de datos

El paquete de la consulta es demasiado grande

Si aparece un error que indica que el paquete de una consulta es demasiado grande, por lo general, el conjunto de resultados que se obtiene para una fila también es demasiado grande. El límite de tamaño de la API de datos es 64 KB por fila en el conjunto de resultados devuelto por la base de datos.

Para solventar este problema, asegúrese de que cada fila de un conjunto de resultados sea de 64 KB o menos.

Límite de tamaño superado de respuesta de base de datos

Si aparece un error que indica que la respuesta de la base de datos ha superado el límite de tamaño, por lo general, esto significa que el tamaño del conjunto de resultados devuelto por la base de datos era demasiado grande. El límite de la API de datos es 100 MB en el conjunto de resultados devuelto por la base de datos.

Para resolver este problema, asegúrese de que las llamadas a la API de datos devuelvan 100 MB o menos. Si necesita devolver más de 100 MB, puede ejecutar varias llamadas de instrucción con la cláusula `LIMIT` en la consulta.

Programación de operaciones de la API de datos de Amazon Redshift con Amazon EventBridge

Puede crear reglas que coincidan con los eventos seleccionados y que los dirijan a los destinos para realizar alguna acción. También puede utilizar reglas para realizar acciones en una programación predeterminada. Para más información, consulte la Guía del usuario de Amazon EventBridge.

Para programar operaciones de la API de datos con EventBridge, el rol de IAM asociado debe confiar en la entidad principal de CloudWatch Events (events.amazonaws.com). Este rol debería tener el equivalente a la política administrada `AmazonEventBridgeFullAccess` adjunta. Además, debería contar con los permisos de la política `AmazonRedshiftDataFullAccess` que administra la API de datos. Puede crear un rol de IAM con estos permisos en la consola de IAM. Al crear un rol en la consola de IAM, elija la entidad de confianza del servicio de AWS para CloudWatch Events. Especifique el rol de IAM en el valor JSON `RoleArn` del destino de EventBridge. Para obtener más información sobre cómo crear un rol de IAM, consulte Creación de un rol para un servicio de AWS (consola) en la Guía del usuario de IAM.

La regla `name` que cree en Amazon EventBridge debe coincidir con el `StatementName` en los `RedshiftDataParameters`.

En los siguientes ejemplos, se muestran las variaciones de la creación de reglas de EventBridge con una o varias instrucciones SQL y con un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor como almacenamiento de datos.

Llamada con una sola instrucción SQL y un clúster

En el siguiente ejemplo, se utiliza la AWS CLI a fin de crear una regla de EventBridge que se use para ejecutar una instrucción SQL en un clúster de Amazon Redshift.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

A continuación, se crea un objetivo de EventBridge para que se ejecute en la programación especificada en la regla.

```
aws events put-targets
--cli-input-json file://data.json
```

El archivo data.json de entrada es así. La clave JSON `Sql` indica que hay una sola instrucción SQL. El valor JSON `Arn` contiene un identificador de clúster. El valor JSON `RoleArn` contiene el rol de IAM que se utiliza para ejecutar el código SQL, tal como se describió anteriormente.

```
{
    "Rule": "test-redshift-cluster-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "DbUser": "root",
                "Sql": "select 1;",
                "StatementName": "test-redshift-cluster-data",
                "WithEvent": true
            }
        }
    ]
}
```

Llamada con una sola instrucción SQL y un grupo de trabajo

En el siguiente ejemplo, se utiliza la AWS CLI a fin de crear una regla de EventBridge que se use para ejecutar una instrucción SQL en un grupo de trabajo de Amazon Redshift sin servidor.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

A continuación, se crea un objetivo de EventBridge para que se ejecute en la programación especificada en la regla.

```
aws events put-targets
--cli-input-json file://data.json
```

El archivo data.json de entrada es así. La clave JSON `Sql` indica que hay una sola instrucción SQL. El valor JSON `Arn` contiene un nombre de grupo de trabajo. El valor JSON `RoleArn` contiene el rol de IAM que se utiliza para ejecutar el código SQL, tal como se describió anteriormente.

```
{
    "Rule": "test-redshift-serverless-workgroup-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "Sql": "select 1;",
                "StatementName": "test-redshift-serverless-workgroup-data",
                "WithEvent": true
            }
        }
    ]
}
```

Llamada con varias instrucciones SQL y un clúster

En el siguiente ejemplo, se utiliza la AWS CLI a fin de crear una regla de EventBridge que se use para ejecutar varias instrucciones SQL en un clúster de Amazon Redshift.

```
aws events put-rule
--name  test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

A continuación, se crea un objetivo de EventBridge para que se ejecute en la programación especificada en la regla.

```
aws events put-targets
--cli-input-json file://data.json
```

El archivo data.json de entrada es así. La clave JSON `Sqls` indica que hay varias instrucciones SQL. El valor JSON `Arn` contiene un identificador de clúster. El valor JSON `RoleArn` contiene el rol de IAM que se utiliza para ejecutar el código SQL, tal como se describió anteriormente.

```
{
    "Rule": "test-redshift-cluster-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "Sqls": ["select 1;", "select 2;", "select 3;"],
                "StatementName": "test-redshift-cluster-data",
                "WithEvent": true
            }
        }
    ]
}
```

Llamada con varias instrucciones SQL y un grupo de trabajo

En el siguiente ejemplo, se utiliza la AWS CLI a fin de crear una regla de EventBridge que se use para ejecutar varias instrucciones SQL en un grupo de trabajo de Amazon Redshift sin servidor.

```
aws events put-rule
--name  test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

A continuación, se crea un objetivo de EventBridge para que se ejecute en la programación especificada en la regla.

```
aws events put-targets
--cli-input-json file://data.json
```

El archivo data.json de entrada es así. La clave JSON `Sqls` indica que hay varias instrucciones SQL. El valor JSON `Arn` contiene un nombre de grupo de trabajo. El valor JSON `RoleArn` contiene el rol de IAM que se utiliza para ejecutar el código SQL, tal como se describió anteriormente.

```
{
    "Rule": "test-redshift-serverless-workgroup-data",
    "EventBusName": "default",
    "Targets": [
        {
            "Id": "2",
            "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
            "RedshiftDataParameters": {
                "Database": "dev",
                "Sqls": ["select 1;", "select 2;", "select 3;"],
                "StatementName": "test-redshift-serverless-workgroup-data",
                "WithEvent": true
            }
        }
    ]
}
```

Monitoreo de la API de datos

El monitoreo es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de la API de datos y de sus otras soluciones de AWS. AWS proporciona las siguientes herramientas de monitoreo para vigilar la API de datos, informar cuando algo va mal y realizar acciones de manera automática cuando sea necesario:

- Amazon EventBridge puede utilizarse para automatizar los servicios de AWS y responder automáticamente a eventos del sistema, como problemas de disponibilidad de las aplicaciones o cambios en los recursos. Los eventos de los servicios de AWS se envían a EventBridge casi en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulte la Guía del usuario de Amazon EventBridge.
- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información sobre

cómo Amazon Redshift se integra con AWS CloudTrail, consulte Registro con CloudTrail. Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Temas

- Monitoreo de eventos para la API de datos de Amazon Redshift en Amazon EventBridge

Monitoreo de eventos para la API de datos de Amazon Redshift en Amazon EventBridge

Puede monitorear los eventos de la API de datos en EventBridge, lo que envía un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS. EventBridge dirige esos datos a los objetivos, como AWS Lambda y Amazon SNS. Estos eventos son los mismos que los que aparecen en CloudWatch Events, lo que proporciona un flujo de eventos del sistema casi en tiempo real que describen los cambios en los recursos de AWS. Los eventos se envían a la cuenta donde se encuentra la base de datos de Amazon Redshift. Por ejemplo, si se asume un rol en otra cuenta, los eventos se envían a esa cuenta. Para obtener más información, consulte los Eventos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Los eventos de la API de datos se envían cada vez que la operación `ExecuteStatement` o `BatchExecuteStatement` de la API establece la opción `WithEvent` como `true`. El campo `state` del evento contiene uno de los siguientes valores.

- ABORTED: el usuario ha detenido la ejecución de la consulta.
- FAILED: se produce un error en la ejecución de la consulta.
- FINISHED: se completó la ejecución de la consulta.

Los eventos se entregan de forma garantizada. Para obtener más información, consulte Eventos de servicios de AWS en la Guía del usuario de Amazon EventBridge.

Ejemplo de evento terminado de la API de datos

En el siguiente ejemplo, se muestra un evento de la API de datos en el momento en que la operación `ExecuteStatement` de la API se completa. En este ejemplo, una instrucción denominada `test.testtable` completó la ejecución.

```
{
```

```
    "version": "0",
    "id": "18e7079c-dd4b-dd64-caf9-e2a31640dab0",
    "detail-type": "Redshift Data Statement Status Change",
    "source": "aws.redshift-data",
    "account": "123456789012",
    "time": "2020-10-01T21:14:26Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:redshift:us-east-1:123456789012:cluster:redshift-cluster-1"
    ],
    "detail": {
        "principal": "arn:aws:iam::123456789012:user/myuser",
        "statementName": "test.testtable",
        "statementId": "dd2e1ec9-2ee3-49a0-819f-905fa7d75a4a",
        "redshiftQueryId": -1,
        "state": "FINISHED",
        "rows": 1,
        "expireAt": 1601673265
    }
}
```

Grupos de parámetros de Amazon Redshift

Información general

En Amazon Redshift, puede asociar un grupo de parámetros con cada clúster que cree. Un grupo de parámetros es un grupo de parámetros que se aplican a todas las bases de datos que crea en el clúster. Estos parámetros establecen la configuración de la base de datos, como el tiempo de espera de consulta y el estilo de fecha.

Acerca de los grupos de parámetros

Cada grupo de parámetros tiene varios parámetros para la configuración de ajustes de la base de datos. La lista de parámetros disponibles depende de la familia de grupos de parámetros a la que el grupo de parámetros pertenece. La familia de grupos de parámetros es la versión del motor de Amazon Redshift a la que se aplican los parámetros del grupo de parámetros. El formato del nombre de la familia de grupos de parámetros es `redshift-`*`version`*, donde *`version`* es la versión del motor. Por ejemplo, la versión actual del motor es `redshift-1.0`.

Amazon Redshift proporciona un grupo de parámetros predeterminado para cada familia de grupos de parámetros. El grupo de parámetros predeterminado tiene valores preestablecidos para cada uno de sus parámetros y no pueden modificarse. El formato del nombre del grupo de parámetros predeterminado es `default.`*`parameter_group_family`*, donde *`parameter_group_family`* es la versión del motor al que pertenece el grupo de parámetros. Por ejemplo, el grupo de parámetros predeterminado para la versión `redshift-1.0` se llama `default.redshift-1.0`.

> **Note**
>
> En este momento, `redshift-1.0` es la única versión del motor de Amazon Redshift. Por lo tanto, `default.redshift-1.0` es el único grupo de parámetros predeterminado.

Si desea utilizar valores de parámetros diferentes a los del grupo de parámetros predeterminado, debe crear un grupo de parámetros personalizado y luego asociar el clúster a él. Inicialmente, los valores de los parámetros de un grupo de parámetros personalizado son los mismos que los de un grupo de parámetros predeterminado. El `source` inicial para todos los parámetros es `engine-`

`default`, ya que los valores los establece previamente Amazon Redshift. Luego de cambiar un valor de parámetro, el `source` cambia a `user` para indicar que su valor predeterminado se ha modificado.

> **Note**
>
> La consola de Amazon Redshift no muestra el `source` de cada parámetro. Debe utilizar la API de Amazon Redshift, la AWS CLI o uno de los AWS SDK para ver el `source`.

Si se trata de grupos de parámetros creados por usted, puede modificar el valor de parámetro en cualquier momento o puede restablecer los valores de parámetros a sus valores predeterminados. También puede asociar un grupo de parámetros diferente a un clúster. En algunos casos, podrá modificar los valores del parámetro en un grupo de parámetros que ya está asociado a un clúster o asociar un grupo de parámetros diferentes a un clúster. En estos casos, quizás tenga que reiciar el clúster para que se aplique los valores de los parámetros actualizados. Si el clúster falla y Amazon Redshift lo reinicia, los cambios se aplican en ese momento. Si el clúster se reinicia durante el mantenimiento, no se aplican los cambios. Para obtener más información, consulte Propiedades dinámicas y estáticas de WLM.

Valores de parámetros predeterminados

En la siguiente tabla se muestran los valores de parámetros predeterminados junto con enlaces a información más exhaustiva acerca de cada parámetro. Estos son los valores predeterminados para la familia de grupos de parámetros `redshift-1.0`.

Nombre del parámetro	Valor	Más información
auto_analyze	true	auto_analyze en la Guía para desarrolladores de bases de datos de Amazon Redshift
auto_mv	true	Vistas materializadas automatizadas en la Guía para desarrolladores de bases de datos de Amazon Redshift
datestyle	ISO, MDY	datestyle en laGuía para desarrolladores de bases de datos de Amazon Redshift

Nombre del parámetro	Valor	Más información
enable_case_sensitive_identifier	false	enable_case_sensitive_identifier en laGuía para desarrolladores de bases de datos de Amazon Redshift
enable_user_activity_logging	false	Registro de auditoría de bases de datos en esta guía
extra_float_digits	0	extra_float_digits en la Guía para desarrolladores de bases de datos de Amazon Redshift
max_concurrency_scaling_clusters	1	max_concurrency_scaling_clusters en la Guía para desarrolladores de bases de datos Amazon Redshift
query_group	predeterminada	query_group en la Guía para desarrolladores de bases de datos de Amazon Redshift
require_ssl	false	Configuración de las opciones de seguridad para las conexiones en esta guía
search_path	$user, public	search_path en la Guía para desarrolladores de bases de datos de Amazon Redshift
statement_timeout	0	statement_timeout en la Guía para desarrolladores de bases de datos Amazon Redshift
wlm_json_configuration	[{"auto_wlm":true}]	Configuración de la administración de cargas de trabajo en esta guía
use_fips_ssl	false	Habilite el modo SSL compatible con FIPS solo si el sistema debe ser compatible con FIPS.

Note

El parámetro `max_cursor_result_set_size` no está disponible. Para obtener más información acerca del tamaño de conjuntos de resultados de cursores, consulte

Restricciones del cursor en la Guía para desarrolladores de bases de datos Amazon Redshift.

Puede anular un parámetro temporalmente utilizando el comando SET en la base de datos. El comando SET anula el parámetro solamente durante el tiempo de la sesión actual. Además de los parámetros mencionados en la tabla anterior, también puede ajustar de manera temporal el número de slots estableciendo `wlm_query_slot_count` en la base de datos. El parámetro `wlm_query_slot_count` no está disponible para su configuración en grupos de parámetros. Para obtener más información acerca del ajuste del número de slots, consultewlm_query_slot_count en la Guía para desarrolladores de bases de datos de Amazon Redshift. Para obtener más información acerca de la anulación temporal de otros parámetros, consulte Modificación de la configuración del servidor en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Configuración de los valores de parámetros mediante la AWS CLI

Si desea configurar los parámetros de Amazon Redshift con la AWS CLI, utilice el comando `modify-cluster-parameter-group` en un grupo de parámetros específico. Especifique el grupo de parámetros a modificar en `parameter-group-name`. Utilice el parámetro `parameters` (para el comando `modify-cluster-parameter-group`) para especificar los pares de nombre/valor de cada parámetro que desea modificar en el grupo de parámetros.

> **Note**
>
> Existen consideraciones especiales cuando se configura el parámetro `wlm_json_configuration` mediante la AWS CLI. Los ejemplos de esta sección aplican a todos los parámetros, excepto `wlm_json_configuration`. Para obtener más información acerca de la configuración de `wlm_json_configuration` mediante la AWS CLI, consulte Configuración de la administración de cargas de trabajo.

Luego de modificar los valores de parámetros, debe reiniciar cualquier clúster que esté asociado al grupo de parámetros modificado. El estado del clúster muestra `applying` para el `ParameterApplyStatus` durante la aplicación de los valores y `pending-reboot` después de que se han aplicado los valores. Luego de reiniciar, la base de datos del clúster comienza a utilizar los nuevos valores de parámetros. Para obtener más información acerca del reinicio de clústeres, consulte Reinicio de un clúster.

> **Note**
>
> El parámetro `wlm_json_configuration` contiene algunas propiedades que son dinámicas y no requieren el reinicio de los clústeres asociados para que se apliquen los cambios. Para obtener más información acerca de las propiedades dinámicas y estáticas, consulte Propiedades dinámicas y estáticas de WLM.

Sintaxis

La siguiente sintaxis muestra cómo utilizar el comando `modify-cluster-parameter-group` para configurar un parámetro. Especifique *`parameter_group_name`* y reemplace *`parameter_name`* y *`parameter_value`* por un parámetro real que desee modificar y un valor para ese parámetro. Si desea modificar más de un parámetro al mismo tiempo, separe con un espacio cada parámetro y valor establecido del siguiente.

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name
 --parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

Ejemplo

En el siguiente ejemplo, se muestra cómo configurar los parámetros `statement_timeout` y `enable_user_activity_logging` para el grupo de parámetros `myclusterparametergroup`.

> **Note**
>
> Por fines de legibilidad, el ejemplo se muestra en varias líneas pero, en la AWS CLI real, se ve en una línea.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
 ParameterName=enable_user_activity_logging,ParameterValue=true
```

Puede administrar grupos de parámetros mediante la consola. Para obtener más información, consulte Administración de grupos de parámetros mediante la consola.

Configuración de la administración de cargas de trabajo

En Amazon Redshift, se utiliza administración de cargas de trabajo (WLM) para definir el número de colas de consultas que están disponibles y cómo se dirigen las consultas a esas colas para su procesamiento. WLM forma parte de la configuración de grupos de parámetros. Un clúster utiliza la configuración de WLM que se especifica en su grupo de parámetros asociados.

Cuando crea un grupo de parámetros, la configuración de WLM predeterminada contiene una cola que puede ejecutar hasta cinco consultas simultáneamente. Puede añadir colas adicionales y configurar las propiedades de WLM en cada una de ellas si desea tener más control en el procesamiento de consultas. Cada cola que añade tiene la misma configuración de WLM predeterminada hasta que configure sus propiedades.

Si añade otras colas, la última cola de la configuración será la cola predeterminada. A menos que la consulta se direccione a otra cola basada en criterios de la configuración de WLM, la consulta se procesa por la cola predeterminada. Puede especificar el modo y el nivel de simultaneidad (slots de consulta) de la cola predeterminada, pero no puede especificar grupos de usuarios ni grupos de consultas para dicha cola.

Como sucede con otros parámetros, usted no puede modificar la configuración de WLM en el grupo de parámetros predeterminado. Los clústeres asociados al grupo de parámetros predeterminado siempre utilizan la configuración de WLM predeterminada. Si desea modificar la configuración de WLM, cree un nuevo grupo de parámetros y asócielo a cualquier clúster que requiera su configuración de WLM personalizada.

Propiedades dinámicas y estáticas de WLM

Las propiedades de configuración de WLM son dinámicas o estáticas. Puede aplicar propiedades dinámicas a la base de datos sin reiniciar el clúster, pero las propiedades estáticas requieren el reinicio del clúster para que los cambios surtan efecto. Para obtener más información sobre las propiedades estáticas y dinámicas, consulte Propiedades de configuración dinámicas y estáticas de WLM.

Propiedades del parámetro wlm_json_configuration

Puede configurar WLM mediante la consola de Amazon Redshift, la AWS CLI, la API de Amazon Redshift o uno de los AWS SDK. La configuración de WLM usa diversas propiedades para definir el comportamiento de la cola, como la asignación de memoria entre colas, el número de consultas que se pueden ejecutar simultáneamente en una cola, etc.

> **Note**
>
> Las siguientes propiedades aparecen en las descripciones con los nombres de la consola de Amazon Redshift y los nombres de las propiedades JSON correspondientes.

La tabla siguiente resume si una propiedad es aplicable a WLM automática o WLM manual.

Propiedad de WLM	WLM automática	WLM manual
Auto WLM (WLM automática)	Sí	Sí
Habilitar aceleración de consultas cortas	Sí	Sí
Tiempo máximo de ejecución de consultas cortas	Sí	Sí
Priority (Prioridad)	Sí	No
Tipo de cola	Sí	Sí
Nombre de la cola	Sí	Sí
Modo de escalado de simultaneidad	Sí	Sí
Simultaneidad	No	Sí
Grupos de usuarios	Sí	Sí
Comodín de grupo de usuarios	Sí	Sí
Grupos de consultas	Sí	Sí
Comodín de grupo de consultas	Sí	Sí
Roles de usuario	Sí	Sí

Propiedad de WLM	WLM automática	WLM manual
Comodín de rol de usuario	Sí	Sí
Tiempo de espera	No	Obsoleto
Memoria	No	Sí
Reglas de monitorización de consultas	Sí	Sí

En la siguiente lista se describen las propiedades de WLM que puede configurar.

Auto WLM (WLM automática)

Auto WLM (WLM automática) establecida en `true` habilita la WLM automática. La WLM automática establece los valores para Concurrency on main (Simultaneidad en el principal) y Memory (%) (Memoria (%)) de `Auto`. Amazon Redshift administra la simultaneidad de consultas y la asignación de memoria. El valor predeterminado es `true`.

Propiedad JSON: `auto_wlm`

Habilitar aceleración de consultas cortas

La aceleración de consultas cortas (SQA) da prioridad a una serie de consultas seleccionadas que se ejecutan rápidamente frente a consultas que tardan más en ejecutarse. SQA ejecuta las consultas cortas en un espacio dedicado, de forma que estas consultas no tienen que esperar en las colas detrás de otras consultas más largas. Con SQA, las consultas cortas se ejecutan con mayor rapidez y los usuarios tardan menos en ver los resultados. Si habilita SQA, también puede especificar el tiempo máximo de ejecución de las consultas cortas. Para habilitar SQA, especifique `true`. El valor predeterminado es `false`. Esta configuración se aplica a cada grupo de parámetros en lugar de a cada cola.

Propiedad JSON: `short_query_queue`

Tiempo máximo de ejecución de consultas cortas

Si habilita SQA, también puede especificar 0 para permitir que WLM establezca de forma dinámica el tiempo máximo de ejecución de las consultas cortas. Si lo desea, también puede especificar un valor entre 1 y 20 segundos, en milisegundos. El valor predeterminado es `0`.

Propiedad JSON: `max_execution_time`

Priority (Prioridad)

La prioridad establece la prioridad de las consultas que se ejecutan en una cola. Para establecer la prioridad, WLM mode (Modo de WLM) debe estar definido en Auto WLM (WLM automática); es decir, `auto_wlm` debe ser `true`. Los valores de prioridad pueden ser `highest`, `high`, `normal`, `low` y `lowest`. El valor predeterminado es `normal`.

Propiedad JSON: `priority`

Tipo de cola

El tipo de cola designa una cola tal como la utiliza Auto WLM (WLM automática) o Manual WLM (WLM manual). Establezca `queue_type` en `auto` o `manual`. Si no se especifica, el valor predeterminado es `manual`.

Propiedad JSON: `queue_type`

Nombre de la cola

El nombre de la cola . Puede establecer el nombre de la cola en función de las necesidades de su empresa. Los nombres de cola deben ser únicos dentro de una configuración WLM, tener hasta 64 caracteres alfanuméricos, guiones bajos o espacios y no pueden contener comillas. Por ejemplo, si tiene una cola para sus consultas ETL, podría denominarla `ETL queue`. Este nombre se utiliza en métricas, valores de tabla del sistema y la consola de Amazon Redshift para identificar la cola. Las consultas e informes que utilizan el nombre a partir de estas fuentes tienen que poder controlar los cambios del nombre. Anteriormente, Amazon Redshift generaba los nombres de cola. Los nombres predeterminados de las colas son `Queue 1`, `Queue 2`, hasta la última cola denominada `Default queue`.

> **Important**
>
> Si cambia el nombre de una cola, también cambia el valor de la dimensión `QueueName` de las métricas de cola WLM (por ejemplo, WLMQueueLength, WLMQueueWaitTime, WLMQueriesCompletedPerSecond, WLMQueryDuration, WLMRunningQueries, etc.). Por lo tanto, si cambia el nombre de una cola, es posible que tenga que cambiar las alarmas de CloudWatch que ha configurado.

Propiedad JSON: `name`

Modo de escalado de simultaneidad

Para habilitar el escalado de simultaneidad en una cola, establezca Concurrency Scaling mode (Modo de escalado de simultaneidad) en `auto`. Cuando el número de consultas enviadas a una cola supera la simultaneidad configurada de la cola, las consultas que cumplen los requisitos se envían al clúster de escalado. Cuando hay slots disponibles, las consultas se ejecutan en el clúster principal. El valor predeterminado es `off`.

Propiedad JSON: `concurrency_scaling`

Concurrency (Simultaneidad)

Número de consultas que pueden ejecutarse simultáneamente en una cola de WLM manual. Esta propiedad solo se aplica al WLM manual. Si el modo de escalado de simultaneidad está habilitado, las consultas que cumplen los requisitos se envían a un clúster de escalado cuando una cola alcanza el nivel de simultaneidad (slots de consulta). Si el escalado de simultaneidad no está habilitado, las consultas esperan en la cola hasta que haya un slot disponible. El rango está entre 1 y 50.

Propiedad JSON: `query_concurrency`

User Groups (Grupos de usuarios)

Una lista de nombres de grupos de usuarios separada por comas. Cuando los miembros del grupo de usuarios ejecutan consultas en la base de datos, estas se direccionan a la cola que está asociada a su grupo de usuarios.

Propiedad JSON: `user_group`

Carácter comodín de grupos de usuarios

Un valor booleano que indica si se habilitan comodines para los grupos de usuarios. Si el valor es 0, los comodines están desactivados y si el valor es 1, los comodines están habilitados. Si los caracteres comodín están habilitados, puede utilizar "*" o "?" para especificar varios grupos de usuarios al ejecutar consultas. Para obtener más información, consulte Wildcards.

Propiedad JSON: `user_group_wild_card`

Grupos de consultas

Una lista de grupos de consultas separada por comas. Cuando los miembros del grupo de consultas ejecutan consultas en la base de datos, estas se direccionan a la cola que está asociada a su grupo de consultas.

Propiedad JSON: `query_group`

Carácter comodín de grupos de consultas

Un valor booleano que indica si se habilitan comodines para los grupos de consultas. Si el valor es 0, los comodines están desactivados y si el valor es 1, los comodines están habilitados. Si los caracteres comodín están habilitados, puede utilizar "*" o "?" para especificar varios grupos de consultas al ejecutar consultas. Para obtener más información, consulte Wildcards.

Propiedad JSON: `query_group_wild_card`

Roles de usuario

Una lista separada por comas de roles de usuarios. Cuando los miembros con ese rol de usuario ejecutan consultas en la base de datos, las consultas se dirigen a la cola que está asociada al rol de los usuarios. Para obtener más información sobre los roles de usuario, consulte Control de acceso basado en roles (RBAC).

Propiedad JSON: `user_role`

Comodín de roles de usuarios

Un valor booleano que indica si se habilitan comodines para los grupos de consultas. Si el valor es 0, los comodines están desactivados y si el valor es 1, los comodines están habilitados. Si los caracteres comodín están habilitados, puede utilizar "*" o "?" para especificar varios grupos de consultas al ejecutar consultas. Para obtener más información, consulte Wildcards.

Propiedad JSON: `user_role_wild_card`

Tiempo de espera (ms)

El tiempo de espera de WLM (`max_execution_time`) no está disponible. Si no está disponible cuando se utiliza WLM automática. En su lugar, cree una regla de monitorización de consultas (QMR) utilizando `query_execution_time` para limitar el tiempo de ejecución transcurrido de una consulta. Para obtener más información, consulte Reglas de monitoreo de consultas de WLM.

El tiempo máximo, en milisegundos, en el que se pueden ejecutar las consultas antes de ser canceladas. En algunos casos, una consulta de solo lectura, como por ejemplo una instrucción SELECT, podría cancelarse debido al tiempo de espera de WLM. En estos casos, WLM intenta direccionarla a la siguiente cola coincidente en función de las reglas de asignación de colas de WLM. Si la consulta no coincide con ninguna otra definición de cola, esta no se asigna a la cola predeterminada, sino que se cancela. Para obtener más información, consulte Salto de

cola de consultas de WLM. El tiempo de espera de WLM no aplica a una consulta que haya alcanzado el estado `returning`. Para ver el estado de una consulta, diríjase a la tabla de sistema STV_WLM_QUERY_STATE.

Propiedad JSON: `max_execution_time`

Memory (%) (Porcentaje de memoria)

El porcentaje de memoria para asignar a la cola. Si especifica un porcentaje de memoria para al menos una de las colas, debe especificar un porcentaje para todas las otras colas hasta llegar a un total de 100 por ciento. Si la asignación de memoria es inferior al 100 por cien en todas las colas, el servicio administra la memoria sin asignar. El servicio puede entregar temporalmente esta memoria sin asignar a una cola que solicita memoria adicional para el procesamiento.

Propiedad JSON: `memory_percent_to_use`

Reglas de monitorización de consultas

Puede utilizar las reglas de monitorización de consultas de WLM para monitorear de forma continua las colas de WLM de consultas basadas en criterios o predicados que usted especificó. Por ejemplo, es posible que monitoree consultas que tiendan a consumir recursos excesivos del sistema y luego inicie una acción especificada cuando la consulta exceda los límites de rendimiento especificados.

> **Note**
>
> Si decide crear reglas mediante programación, recomendamos encarecidamente utilizar la consola para generar el JSON que incluirá en la definición del grupo de parámetros.

Asocie una regla de monitorización de consultas a una cola de consultas específica. Puede tener hasta 25 reglas por cola y el límite total para todas las colas es 25 reglas.

Propiedad JSON: `rules`

Jerarquía de propiedades JSON:

```
rules
    rule_name
    predicate
        metric_name
```

```
        operator
        value
    action
        value
```

Especifique las siguientes propiedades para cada regla:

- `rule_name`: los nombres de reglas deben ser únicos en la configuración de WLM. Los nombres de reglas pueden tener un máximo de 32 caracteres alfanuméricos o guiones bajos y no pueden contener espacios ni comillas. Puede disponer de hasta ocho reglas por cola y el límite total para todas las colas es de ocho reglas.
  - `predicate`: puede tener hasta tres predicados por regla. Especifique las siguientes propiedades para cada predicado:
    - `metric_name`: para obtener una lista de métricas, consulte Métricas de monitoreo de consultas en la Guía para desarrolladores de bases de datos de Amazon Redshift.
    - `operator`: las operaciones son =, < y >.
    - `value`: el valor de límite de la métrica especificada que desencadena una acción.
- `action`: cada regla está asociada a una acción. Las acciones válidas son:
  - `log`
  - hop (solo disponible con WLM manual)
  - `abort`
  - `change_query_priority` (solo disponible con WLM automática)

En el siguiente ejemplo se muestra el JSON para una regla de monitorización de consultas de WLM denominada `rule_1`, con dos predicados y la acción hop.

```
"rules": [
          {
            "rule_name": "rule_1",
            "predicate": [
              {
                "metric_name": "query_execution_time",
                "operator": ">",
                "value": 100000
              },
              {
                "metric_name": "query_blocks_read",
                "operator": ">",
                "value": 1000
```

```
            }
          ],
          "action": "hop"
        }
      ]
```

Para obtener más información acerca de cada una de estas propiedades y estrategias para la configuración de colas de consultas, consulte Implementación de administración de cargas de trabajo en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Configuración del parámetro wlm_json_configuration mediante la AWS CLI

Para configurar WLM, modifique el parámetro `wlm_json_configuration`. El tamaño máximo del valor de la propiedad `wlm_json_configuration` es de 8000 caracteres. El valor tiene el formato de JavaScript Object Notation (JSON). Si configura WLM a través de la AWS CLI, la API de Amazon Redshift o uno de los AWS SDK, utilice el resto de esta sección para aprender a crear la estructura JSON del parámetro `wlm_json_configuration`.

> **Note**
>
> Si configura WLM mediante la consola de Amazon Redshift, no necesitará comprender el formato JSON, ya que la consola proporciona una forma sencilla de agregar colas y configurar sus propiedades. Para obtener más información acerca de la configuración de WLM mediante la consola, consulte Modificación de un grupo de parámetros.

Ejemplo

En el siguiente ejemplo se muestra la configuración de WLM predeterminada, que define una cola con la WLM automática.

```
{
   "auto_wlm": true
}
```

Ejemplo

En el siguiente ejemplo, se muestra una configuración de WLM personalizada que define una cola de WLM manual con un nivel de simultaneidad (slots de consulta) de cinco.

```
{
   "query_concurrency":5
}
```

Sintaxis

La configuración de WLM predeterminada es muy sencilla, tiene cola única y una propiedad. Puede añadir más colas y configurar varias propiedades para cada cola en la estructura JSON. La siguiente sintaxis representa la estructura JSON que se utiliza para configurar varias colas con varias propiedades:

```
[
   {
      "ParameterName":"wlm_json_configuration", "ParameterValue":
         "[
             {
                "q1_first_property_name":"q1_first_property_value",
                "q1_second_property_name":"q1_second_property_value",
                ...
             },
             {
                "q2_first_property_name":"q2_first_property_value",
                "q2_second_property_name":"q2_second_property_value",
                ...
             }
             ...

         ]"
   }
]
```

En el ejemplo anterior, las propiedades representativas que comienzan con q1 son objetos de una matriz de la primera cola. Cada uno de estos objetos es un par de nombre/valor. `name` y `value` establecen juntos las propiedades de WLM para la primera cola. Las propiedades representativas que comienzan con q2 son objetos de una matriz de la segunda cola. Si necesita más colas, añada otra matriz para cada cola adicional y establezca las propiedades de cada objeto.

Cuando modifica la configuración de WLM, debe incluir toda la estructura para las colas, aunque solo desee cambiar una propiedad dentro de una cola. Esto se debe a que toda la estructura JSON se transfiere en forma de cadena como el valor para el parámetro `wlm_json_configuration`.

Formateo del comando de AWS CLI

El parámetro `wlm_json_configuration` requiere un formato específico cuando utiliza la AWS CLI. El formato que utilice depende del sistema operativo del cliente. Los sistemas operativos tienen formas diferentes de delimitar la estructura JSON para que se transfiera correctamente desde la línea de comando. Para ver detalles acerca de cómo construir el comando adecuado en los sistemas operativos de Windows, Mac OS X y Linux, consulte las siguientes secciones. Para obtener más información acerca de las diferencias en la delimitación de estructuras de datos JSON en la AWS CLI en general, consulte Entrecomillado de cadenas en la Guía del usuario de AWS Command Line Interface.

Ejemplos

En el comando de ejemplo siguiente se configura WLM manual para un grupo de parámetros denominado `example-parameter-group`. La configuración permite la aceleración de las consultas cortas con un tiempo de ejecución máximo establecido en 0, lo que le indica a WLM que debe establecer el valor dinámicamente. El valor de `ApplyType` es `dynamic`. Esta opción significa que cualquier cambio que se realice en las propiedades dinámicas del parámetro se aplicarán de inmediato, a menos que se hayan realizado otros cambios estáticos en la configuración. La configuración define tres colas con lo siguiente:

- La primera cola permite a los usuarios especificar `report` como una etiqueta (como se especifica en la propiedad `query_group`) en sus consultas para ayudar a direccionar las consultas a esa cola. Se pueden realizar búsquedas con caracteres comodín de la etiqueta `report*`, por lo que no es necesario que la etiqueta sea exacta para que las consultas se direccionen a la cola. Por ejemplo, `reports` y `reporting` también coincidirán con este grupo de consultas. La cola tiene asignado el 25 por ciento del total de memoria entre todas las colas y puede ejecutar hasta cuatro consultas al mismo tiempo. Las consultas se limitan a un tiempo máximo de 20.000 milisegundos (ms). El modo se establece en automático, por tanto cuando los slots de consulta de la cola cumplen los requisitos las consultas se envían a un clúster de escalado.
- La segunda cola habilita a los usuarios miembros de grupos `admin` o `dba` en la base de datos a que sus consultas se direccionen a la cola para su procesamiento. Las búsquedas de comodín están desactivadas para los grupos de usuarios, por lo que los usuarios deben coincidir de forma exacta con los grupos de la base de datos para que sus consultas se direccionen a la cola. La cola tiene asignado el 40 por ciento del total de memoria entre todas las colas y puede ejecutar hasta cinco consultas al mismo tiempo. El modo se establece como desactivado, de forma que todas las consultas enviadas por miembros del administrador o grupos de dba se ejecutan en el clúster principal.

- La última cola de la configuración es la cola predeterminada. A esta cola se le asigna el 35 por ciento del total de memoria entre todas las colas y puede procesar hasta cinco consultas a la vez. El modo se establece en automático.

> **Note**
>
> El ejemplo se muestra en varias líneas por fines ilustrativos. Los comandos reales no deben tener saltos de línea.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name example-parameter-group
--parameters
'[
  {
    "query_concurrency": 4,
    "max_execution_time": 20000,
    "memory_percent_to_use": 25,
    "query_group": ["report"],
    "query_group_wild_card": 1,
    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "memory_percent_to_use": 40,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [
      "admin",
      "dba"
    ],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "off",
    "queue_type": "manual"
```

```
  },
  {
    "query_concurrency": 5,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {"short_query_queue": true}
]'
```

A continuación se muestra un ejemplo de configuración de las reglas de monitorización de consultas de WLM para una configuración de WLM automática. El ejemplo crea un grupo de parámetros denominado `example-monitoring-rules`. La configuración define las tres mismas colas que las del ejemplo anterior, pero `query_concurrency` y `memory_percent_to_use` ya no se especifican. La configuración añade además las siguientes reglas y prioridades de consulta:

- La primera cola define una regla denominada `rule_1`. La regla tiene dos predicados: `query_cpu_time > 10000000` y `query_blocks_read > 1000`. La acción de la regla es `log`. La prioridad de esta cola es `Normal`
- La segunda cola define una regla denominada `rule_2`. La regla tiene dos predicados: `query_execution_time > 600000000` y `scan_row_count > 1000000000`. La acción de la regla es `abort`. La prioridad de esta cola es `Highest`
- La última cola de la configuración es la cola predeterminada. La prioridad de esta cola es `Low`

> **Note**
>
> El ejemplo se muestra en varias líneas por fines ilustrativos. Los comandos reales no deben tener saltos de línea.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name example-monitoring-rules
--parameters
'[ {
```

```
  "query_group" : [ "report" ],
  "query_group_wild_card" : 1,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "auto",
  "rules" : [{
    "rule_name": "rule_1",
    "predicate": [{
      "metric_name": "query_cpu_time",
      "operator": ">",
      "value": 1000000 },
      { "metric_name": "query_blocks_read",
      "operator": ">",
      "value": 1000
    } ],
    "action" : "log"
  } ],
   "priority": "normal",
   "queue_type": "auto"
}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ "admin", "dba" ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "off",
  "rules" : [ {
    "rule_name": "rule_2",
    "predicate": [
      {"metric_name": "query_execution_time",
      "operator": ">",
      "value": 600000000},
      {"metric_name": "scan_row_count",
      "operator": ">",
      "value": 1000000000}],
      "action": "abort"}],
   "priority": "high",
   "queue_type": "auto"

}, {
  "query_group" : [ ],
```

```
  "query_group_wild_card" : 0,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "auto",
  "priority": "low",
  "queue_type": "auto",
  "auto_wlm": true
}, {
  "short_query_queue" : true
} ]'
```

Configuración de WLM mediante la AWS CLI en la línea de comandos con un archivo JSON

Puede modificar el parámetro `wlm_json_configuration` utilizando la AWS CLI y pasarlo al valor del argumento `parameters` como un archivo JSON.

```
aws redshift modify-cluster-parameter-group --parameter-group-name
 myclusterparaametergroup --parameters file://modify_pg.json
```

Los argumentos de `--parameters` se almacenan en el archivo `modify_pg.json`: La ubicación del archivo se especifica en el formato del sistema operativo. Para obtener más información, consulte Carga de parámetros desde un archivo. A continuación, se muestran ejemplos del contenido del archivo JSON `modify_pg.json`.

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"user_group\":\"example_user_group1\",\"query_group\":
 \"example_query_group1\", \"query_concurrency\":7},{\"query_concurrency\":5}]"
    }
]
```

```
[
    {
        "ParameterName": "wlm_json_configuration",
        "ParameterValue": "[{\"query_group\":[\"reports\"],\"query_group_wild_card\":0,
\"query_concurrency\":4,\"max_execution_time\":20000,\"memory_percent_to_use\":25},
{\"user_group\":[\"admin\",\"dba\"],\"user_group_wild_card\":1,\"query_concurrency\":5,
```

```
\"memory_percent_to_use\":40},{\"query_concurrency\":5,\"memory_percent_to_use\":35},
{\"short_query_queue\": true, \"max_execution_time\": 5000 }]",
        "ApplyType": "dynamic"
    }
]
```

Reglas para la configuración de WLM mediante la AWS CLI en la línea de comandos de los sistemas operativos Mac OS X y Linux

Siga estas reglas para ejecutar un comando de la AWS CLI con parámetros en una sola línea:

- Toda la estructura JSON debe estar separada por comillas simples (') y un conjunto de corchetes ([ ]).
- Todos los nombres y valores de los parámetros deben estar separados por comillas dobles (").
- Dentro del valor `ParameterValue`, debe separar toda la estructura anidada por comillas dobles (") y corchetes ([ ]).
- Dentro de la estructura anidada, cada una de las propiedades y los valores para cada cola deben estar separados por llaves ({ }).
- Dentro de la estructura anidada, debe utilizar el carácter de escape de barra oblicua inversa (\) antes de cada comilla doble (").
- Para los pares de nombre/valor, los dos puntos (:) separan cada propiedad de su valor.
- Cada par nombre/valor se separa del otro por una coma (,).
- Las colas múltiples se separan con una coma (,) entre el final de la llave de una cola (}) y el comienzo de la siguiente llave de la cola ({).

Reglas para la configuración de WLM mediante la AWS CLI en Windows PowerShell para los sistemas operativos Microsoft Windows

Siga estas reglas para ejecutar un comando de la AWS CLI con parámetros en una sola línea:

- Toda la estructura JSON debe estar separada por comillas simples (') y un conjunto de corchetes ([ ]).
- Todos los nombres y valores de los parámetros deben estar separados por comillas dobles (").
- Dentro del valor `ParameterValue`, debe separar toda la estructura anidada por comillas dobles (") y corchetes ([ ]).
- Dentro de la estructura anidada, cada una de las propiedades y los valores para cada cola deben estar separados por llaves ({ }).

- Dentro de la estructura anidada, debe utilizar el carácter de escape de barra oblicua inversa (\) antes de cada comilla doble (") y su carácter de escape de barra oblicua inversa (\). Este requisito significa que utilizará tres barras inversas y una comilla doble para asegurarse de que las propiedades se transfieran correctamente (\\\").
- Para los pares de nombre/valor, los dos puntos (:) separan cada propiedad de su valor.
- Cada par nombre/valor se separa del otro por una coma (,).
- Las colas múltiples se separan con una coma (,) entre el final de la llave de una cola (}) y el comienzo de la siguiente llave de la cola ({).

Reglas para la configuración de WLM mediante el símbolo del sistema en los sistemas operativos Windows

Siga estas reglas para ejecutar un comando de la AWS CLI con parámetros en una sola línea:

- Toda la estructura JSON debe estar separada por comillas dobles (") y un conjunto de corchetes ([ ]).
- Todos los nombres y valores de los parámetros deben estar separados por comillas dobles (").
- Dentro del valor `ParameterValue`, debe separar toda la estructura anidada por comillas dobles (") y corchetes ([ ]).
- Dentro de la estructura anidada, cada una de las propiedades y los valores para cada cola deben estar separados por llaves ({ }).
- Dentro de la estructura anidada, debe utilizar el carácter de escape de barra oblicua inversa (\) antes de cada comilla doble (") y su carácter de escape de barra oblicua inversa (\). Este requisito significa que utilizará tres barras inversas y una comilla doble para asegurarse de que las propiedades se transfieran correctamente (\\\").
- Para los pares de nombre/valor, los dos puntos (:) separan cada propiedad de su valor.
- Cada par nombre/valor se separa del otro por una coma (,).
- Las colas múltiples se separan con una coma (,) entre el final de la llave de una cola (}) y el comienzo de la siguiente llave de la cola ({).

Administración de grupos de parámetros mediante la consola

Puede ver, crear, modificar y eliminar grupos de parámetros en la consola de Amazon Redshift.

Puede consultar cualquier grupo de parámetros de para ver un resumen de los valores de los parámetros y la configuración de administración de cargas de trabajo (WLM). Los grupos de parámetros se muestran en la pestaña Parameters (Parámetros) y las colas de carga de trabajo se muestran en la pestaña Workload Management (Administración de cargas de trabajo).

Creación de un grupo de parámetros

Si desea establecer valores de parámetros diferentes a los del grupo de parámetros predeterminado, puede crear un grupo de parámetros personalizado.

Para crear un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione Create (Crear) para mostrar la ventana de Create parameter group (Crear grupo de parámetros).
4. Introduzca un valor para Parameter group name (Nombre de grupo de parámetros) y Description (Descripción).
5. Haga clic en Create (Crear) para crear el grupo de parámetros,.

Modificación de un grupo de parámetros

Puede modificar parámetros para cambiar la configuración de los parámetros y las propiedades de la configuración de WLM.

> **Note**
>
> No puede modificar el grupo de parámetros predeterminado.

Para modificar un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione el grupo de parámetros que desee modificar para mostrar la página de detalles con pestañas para Parameters (Parámetros) y Workload management (Administración de la carga de trabajo).
4. Haga clic en la pestaña Parameters (Parámetros) para ver la configuración de parámetros actual.
5. Haga clic en Edit parameters (Editar parámetros) para permitir cambiar la configuración de estos parámetros:

   - `auto_analyze`
   - `auto_mv`
   - `datestyle`
   - `enable_case_sensitive_identifier`
   - `enable_user_activity_logging`
   - `extra_float_digits`
   - `max_concurrency_scaling_clusters`
   - `max_cursor_result_set_size`
   - `query_group`
   - `require_ssl`
   - `search_path`
   - `statement_timeout`
   - `use_fips_ssl`

   Para obtener más información sobre estos parámetros, consulte Grupos de parámetros de Amazon Redshift.
6. Introduzca sus cambios y luego haga clic en Save (Guardar) para actualizar el grupo de parámetros.

Para modificar la configuración de WLM en un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione el grupo de parámetros que desee modificar para mostrar la página de detalles con pestañas para Parameters (Parámetros) y Workload management (Administración de la carga de trabajo).
4. Seleccione la pestaña Workload management (Administración de cargas de trabajo) para ver la configuración actual de WLM.
5. Para modificar la configuración de WLM, seleccione Edit workload queues (Editar colas de cargas de trabajo).
6. (Opcional) Seleccione Enable short query acceleration (Habilitar aceleración de consultas cortas, SQA) para habilitarlas.

   Si se habilita SQA, Maximum run time for short queries (1 to 20 seconds) [Tiempo máximo de ejecución para consultas cortas (de 1 a 20 segundos)] se establece en Dynamic (Dinámico) de forma predeterminada. Para establecer el tiempo de ejecución máximo en un valor fijo, elija un valor comprendido entre 1 y 20.
7. Realice una o más de las siguientes acciones para modificar la configuración de la cola:

   - Elija Switch WLM mode (Cambiar modo de WLM) para elegir entre Auto WLM (WLM automática) y Manual WLM (WLM manual).

     Con Auto WLM (WLM automática), los valores de Memory (Memoria) and Concurrency on main (Simultaneidad en principal) se establecen en auto (automático).
   - Para crear una cola, seleccione Edit workload queues (Editar colas de cargas de trabajo) y seleccione Add Queue (Añadir cola).
   - Para modificar una cola, cambie los valores de propiedad en la tabla. En función del tipo de cola, las propiedades pueden incluir las siguientes:
     - Queue name (Nombre de cola) no se puede cambiar.
     - Memory (%) (Porcentaje de memoria)
     - Concurrency on main cluster (Simultaneidad en clúster principal)

- El valor de Concurrency Scaling mode (Modo de escalado de simultaneidad) puede ser off (desactivado) o auto (automático).
- Tiempo de espera (ms)
- User groups (Grupos de usuarios)
- Query groups (Grupos de consultas)
- Roles de usuario

Para obtener más información sobre estas propiedades, consulte Propiedades del parámetro wlm_json_configuration.

> **Important**
>
> Si cambia el nombre de una cola, también cambia el valor de la dimensión `QueueName` de las métricas de cola WLM (por ejemplo, WLMQueueLength, WLMQueueWaitTime, WLMQueriesCompletedPerSecond, WLMQueryDuration, WLMRunningQueries, etc.). Por lo tanto, si cambia el nombre de una cola, es posible que tenga que cambiar las alarmas de CloudWatch que ha configurado.

- Para cambiar el orden de las colas, seleccione los botones de las flechas Up (Arriba) y Down (Abajo).
- Para eliminar una cola, seleccione el botón Delete (Eliminar) en la fila de la cola de la tabla.

8. (Opcional) Seleccione Defer dynamic changes until reboot (Aplazar cambios dinámicos hasta reiniciar). para que se apliquen los cambios a los clústeres hasta el próximo reinicio.

> **Note**
>
> Algunos cambios requieren un reinicio del clúster independientemente de esta configuración. Para obtener más información, consulte Propiedades dinámicas y estáticas de WLM.

9. Elija Guardar.

Creación o modificación de una regla de monitoreo de consultas mediante la consola

Puede usar la consola de Amazon Redshift para crear y modificar reglas de monitoreo de consultas de WLM. Las reglas de monitorización de consultas forman parte del parámetro de configuración de WLM para un grupo de parámetros. Si se modifica una regla de monitoreo de consultas (QMR), el cambio se produce automáticamente sin necesidad de modificar el clúster. Para obtener más información, consulte Reglas de monitoreo de consultas de WLM.

Cuando crea une regla, define el nombre de la regla, uno o más predicados y una acción.

Cuando guarda configuración de WLM que incluye una regla, puede ver el código JSON para la definición de la regla como parte del JSON para el parámetro de configuración de WLM.

Para crear una regla de monitorización de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione el grupo de parámetros que desee modificar para mostrar la página de detalles con pestañas para Parameters (Parámetros) y Workload management (Administración de la carga de trabajo).
4. Seleccione la pestaña Workload management (Administrar cargas de trabajo) y seleccione Edit workload queues (Editar colas de cargas de trabajo) para editar la configuración de WLM,
5. Añada una nueva regla utilizando una plantilla predefinida o desde cero.

   Para usar una plantilla predefinida, haga lo siguiente:

   1. Seleccione Add rule from template (Añadir regla desde plantilla) en el grupo Query monitoring rules (Reglas de monitorización de consultas). Se muestra la lista de plantillas de regla.
   2. Seleccione una o varias plantillas de regla. Cuando selecciona Save (Guardar), WLM crea una regla para cada plantilla que selecciona.
   3. Introduzca o confirme los valores de la regla, incluyendo Rule names (Nombres de regla), Predicates (Predicados) y Actions (Acciones).

4. Elija Guardar.

Para añadir una nueva regla desde cero, haga lo siguiente:

1. Para añadir predicados adicionales, seleccione Add predicate (Añadir predicado). Puede tener hasta tres predicados por regla. Si se cumplen todos los predicados, WLM desencadena la acción asociada.
2. Seleccione una acción en Action (Acción). Cada regla tiene una acción.
3. Elija Guardar.

Amazon Redshift genera su parámetro de configuración WLM en formato JSON y lo muestra en la sección JSON.

Eliminación de un grupo de parámetros

Puede eliminar un grupo de parámetros si ya no lo necesita y si no está asociado a clústeres. Solo puede eliminar grupos de parámetros personalizados.

Para eliminar un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. En Parameter groups (Grupos de parámetros), seleccione el grupo de parámetros que desea modificar.

   > **Note**
   >
   > No puede eliminar el grupo de parámetros predeterminado.

4. Seleccione Action (Acción) y confirme que desea eliminar el grupo de parámetros.

Asociación de un grupo de parámetros con un clúster

Cuando lanza un clúster, debe asociarlo a un grupo de parámetros. Si desea cambiar el grupo de parámetros en otro momento, puede modificar el clúster y seleccionar un grupo de parámetros diferente.

Administración de grupos de parámetros mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de Amazon Redshift en la AWS CLI para administrar los grupos de parámetros.

- create-cluster-parameter-group
- delete-cluster-parameter-group
- describe-cluster-parameters
- describe-cluster-parameter-groups
- describe-default-cluster-parameters
- modify-cluster-parameter-group
- reset-cluster-parameter-group

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar los grupos de parámetros.

- CreateClusterParameterGroup
- DeleteClusterParameterGroup
- DescribeClusterParameters
- DescribeClusterParameterGroups
- DescribeDefaultClusterParameters
- ModifyClusterParameterGroup
- ResetClusterParameterGroup

Integración de Amazon Redshift a un socio de AWS

Si trabaja con Amazon Redshift, puede integrarse a los socios de AWS desde la página Cluster details (Detalles del clúster) en la consola de Amazon Redshift. En la página Cluster details (Detalles del clúster), puede acelerar la incorporación de datos a su almacenamiento de datos de Amazon Redshift con las aplicaciones de los socios de AWS. También puede combinar y analizar los datos de diferentes orígenes junto con los datos existentes en el clúster. Antes de completar la integración con Informatica, debe agregar las direcciones IP del socio a la lista de direcciones permitidas del tráfico entrante. Los siguientes socios de AWS pueden integrarse a Amazon Redshift:

- Datacoral
- Etleap
- Fivetran
- SnapLogic
- Acomodar
- Upsolver
- Matillion (versión preliminar)
- Sisense (versión preliminar)
- Thoughtspot

Los socios de AWS pueden integrarse a Amazon Redshift mediante operaciones de la AWS CLI o la API de Amazon Redshift. Para obtener más información, consulte la Referencia de comandos de la AWS CLI o la Referencia de la API de Amazon Redshift.

Integración a un socio de AWS usando la consola de Amazon Redshift

Utilice el siguiente procedimiento para integrar un clúster a un socio de AWS.

Para integrar un clúster de Amazon Redshift a un socio de AWS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres).

3. Elija el clúster que desee integrar.
4. Elija Add partner integration (Agregar integración de socio). La página Choose partner (Elegir socio) se abre con los detalles de los socios de AWS disponibles.
5. Elija un socio de AWS y, a continuación, Next (Siguiente).

   Aparecerán más detalles sobre el socio de AWS elegido, junto con información acerca del clúster que integrará. La sección Cluster details (Detalles del clúster) incluye la información que usted proporciona en el sitio web del socio de AWS, como el identificador del clúster, el punto de enlace, el nombre de base de datos y el nombre de usuario (que es un nombre de usuario de base de datos). Esta información se envía al socio que usted eligió.
6. Elija Add partner (Agregar socio) para abrir el sitio web del socio de AWS.
7. Configure la integración a su clúster de Amazon Redshift en el sitio web del socio. En el sitio web del socio, puede seleccionar y configurar los orígenes de datos que se cargarán en el clúster de Amazon Redshift. También puede definir transformaciones adicionales de extracción, carga y transformación (ELT) para procesar los datos de su empresa, combinarlos con otros conjuntos de datos y crear vistas consolidadas para llevar a cabo análisis y generar informes.

Puede ver y administrar las integraciones a socios de AWS desde la pestaña de detalles del clúster Properties (Propiedades). En la sección Integrations (Integraciones), se muestra el nombre del socio que puede utilizar para vincularse al sitio web del socio de AWS, el estado de la integración, la base de datos que recibe los datos y la última conexión exitosa que podría haber actualizado el clúster.

Los valores posibles de los estados son los siguientes:

- Activo: el socio de AWS puede conectarse al clúster y completar las tareas configuradas.
- Inactivo: la integración al socio de AWS no existe.
- Error de tiempo de ejecución: el socio de AWS puede conectarse al clúster, pero no puede completar las tareas configuradas.
- Error de conexión: el socio de AWS no puede conectarse al clúster.

Después de eliminar la integración de un socio de AWS a Amazon Redshift, los datos continúan fluyendo hacia su clúster. Complete la eliminación en el sitio web del socio.

Carga de datos con socios de AWS

Además de integrar un socio con un clúster de Amazon Redshift, también puede mover datos de más de 30 orígenes al clúster de Amazon Redshift mediante las herramientas de carga de datos de nuestro socio. Antes de hacerlo, debe agregar las direcciones IP del socio (que encontrará más abajo) a la lista de reglas de entrada permitidas. Para obtener más información acerca de cómo se agregan las reglas a un grupo de seguridad de Amazon EC2, consulte Autorizar tráfico entrante para sus instancias en la Guía del usuario de Amazon EC2 para las instancias de Linux. Tenga en cuenta que, aunque la herramienta Informatica Data Loader es gratuita, podrían aplicarse cargos por la entrada de datos en función de los orígenes de datos y los destinos que elija.

Puede cargar datos de los siguientes socios:

- Informatica: direcciones IP

Para integrar un clúster de Amazon Redshift con Informatica

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija la integración de socios de AWS y, a continuación, el socio con el que desea integrar el clúster.
3. Elija Complete <partner-name> integration (Completar la integración de <nombre-del-socio>). Se le redirigirá al sitio de integración del socio.
4. Ingrese los datos necesarios en el sitio del socio y complete la integración.

Adquisición de nodos reservados de Amazon Redshift

Información general

En AWS, los cargos que se acumulan por usar Amazon Redshift se basan en los nodos informáticos. Cada nodo de computación se factura según una tarifa por hora. La tarifa por hora varía según factores como región, tipo de nodo y si el nodo recibe precio de nodo bajo pedido o precio de nodo reservado.

El precio de los nodos bajo demanda es la opción más costosa, pero también la más flexible de Amazon Redshift. Con tarifas bajo pedido, se le facturan únicamente los nodos de computación que tenga en un clúster en ejecución. Si cierra o elimina un clúster, ya no se le cobrará por los nodos de computación que estaban en ese clúster. Solo se le factura por los nodos de computación que utilice, no más. La tarifa por hora que se le cobra por cada nodo de computación varía según factores como región y tipo de nodo.

El precio de nodo reservado es menos costoso que el precio bajo pedido, ya que los nodos de computación se facturan a un precio por hora con descuento. No obstante, para recibir estas tarifas con descuento, debe comprar ofertas de nodos reservados. Cuando compra una oferta, hace una reserva. La reserva establece una tarifa con descuento para cada nodo que reserve por la duración de la reserva. La tarifa con descuento en una oferta varía según factores como región, tipo de nodo, duración y opción de pago.

Puede designar un nodo como nodo reservado llamando a la operación `PurchaseReservedNodeOffering` de la API o eligiendo Comprar nodos reservados en la consola de Amazon Redshift. Al comprar un nodo reservado, debe especificar una región de AWS, un tipo de nodo, un plazo, una cantidad de nodos y un tipo de oferta para el tipo de nodo reservado aplicable. El nodo reservado solo puede utilizarse en la región de AWS designada.

En este tema, se analiza qué son las ofertas de nodos reservados y cómo puede comprarlas para reducir el costo de ejecutar sus clústeres de Amazon Redshift. En este tema, se analizan las tarifas en términos generales, por ejemplo bajo pedido o con descuento, para que pueda comprender los conceptos de precios y cómo estos afectan la facturación. Para obtener más información sobre tarifas específicas, visite Precios de Amazon Redshift.

Consideraciones sobre ofertas de nodos reservados

Si desea que su clúster de Amazon Redshift se siga ejecutando continuamente durante un periodo prolongado, considere la posibilidad de comprar ofertas de nodos reservados. Estas ofertas ofrecen ahorros importantes sobre el precio bajo pedido, pero requieren que reserve nodos de computación y se comprometa a pagar por esos nodos durante un año o tres años.

Los nodos reservados son un concepto de facturación que se utiliza estrictamente para determinar la tarifa de facturación por los nodos. Reservar un nodo, en realidad, no crea ningún nodo para usted. Se le cobra por los nodos reservados independientemente del uso, lo que significa que debe pagar por cada nodo que reserve por la duración de la reserva, tenga o no nodos en un clúster en ejecución al que se aplique la tarifa con descuento.

En la fase de evaluación del proyecto o cuando desarrolla una prueba de concepto, el precio bajo demanda le brinda flexibilidad para pagar por uso, solo por lo que use, y dejar de pagar en cualquier momento al cerrar o eliminar clústeres. Después de establecer las necesidades del entorno de producción y comenzar la fase de implementación, debe considerar reservar nodos de computación al adquirir una o más ofertas.

Una oferta puede aplicarse a uno o más nodos de computación. Usted especifica la cantidad de nodos de computación que reservará cuando adquiere la oferta. Puede elegir adquirir una oferta para distintos nodos de computación o puede elegir adquirir varias ofertas y especificar una determinada cantidad de nodos de computación en cada oferta.

Por ejemplo, cualquiera de las siguientes son formas válidas de adquirir una oferta para tres nodos de computación:

- Adquirir una oferta y especificar tres nodos de computación.
- Adquirir dos ofertas y especificar un nodo de computación para la primera oferta y dos nodos de computación para la segunda oferta.
- Adquirir tres ofertas y especificar un nodo de computación para cada una.

Comparación del precio entre ofertas de nodos reservados

Amazon Redshift proporciona distintas opciones de pago para las ofertas. La opción de pago que elija afectará el cronograma de pagos y la tarifa con descuento que se le cobre por la reserva. Mientras más pague inicialmente por la reserva, mayor será el ahorro general que obtenga.

Las siguientes opciones de pago están disponibles para las ofertas. Las ofertas se indican en orden de menor a mayor ahorro sobre tarifas bajo pedido.

> **Note**
>
> Se le cobra la tarifa por hora aplicable por cada hora en la duración especificada de la reserva, independientemente de si usa el nodo reservado o no. La opción de pago solamente determina la frecuencia de los pagos y el descuento que se aplicará. Para obtener más información, consulte Consideraciones sobre ofertas de nodos reservados.

Comparación de ofertas de nodos reservados

Opción de pago	Cronograma de pagos	Comparación de ahorros	Duración	Cargos iniciales	Cargos mensuales recurrentes
Sin pago inicial	Cuotas mensuales para la duración de la reserva. Sin pagos iniciales.	Aproximadamente, un 20% de descuento sobre tarifas bajo pedido.	Término de un año o tres años	Ninguna	Sí
Pago inicial parcial	Pago inicial parcial y cuotas mensuales por la duración de la reserva.	Hasta un 41% a un 73% de descuento según la duración.	Término de un año o tres años	Sí	Sí
Pago inicial total	Pago inicial completo para la reserva. Sin cargos mensuales.	Hasta un 42% a un 76% de descuento según la duración.	Término de un año o tres años	Sí	Ninguna

Las opciones y las duraciones específicas están sujetas a disponibilidad.

> **Note**
>
> Si anteriormente compró ofertas de utilización intensa para Amazon Redshift, la oferta comparable es la oferta de pago inicial parcial.

Cómo funcionan los nodos reservados

Con ofertas de nodo reservado, usted paga según los términos de pago, como se indicó en la sección anterior. De esta manera, debe pagar ya sea que tenga un clúster en ejecución o que lance un clúster después de una reserva.

Cuando compra una oferta, la reserva tiene el estado payment-pending (pendiente de pago) hasta que se procesa. Si la reserva no se puede procesar, el estado es payment-failed (error al pagar) y puede intentar el proceso nuevamente. Cuando la reserva se procesa con éxito, el estado cambia a active (activa). La tarifa con descuento aplicable a la reserva no se hace efectiva en la factura hasta que el estado cambia a active (activa). Una vez que transcurre la duración de la reserva, el estado cambia a retired (retirada), pero puede seguir obteniendo acceso a la información relacionada con la reserva para consultar el historial. Cuando el estado de una reserva es retired (retirada), los clústeres continúan ejecutándose, pero es posible que se apliquen los precios bajo pedido, a menos que tenga otra reserva que aplique un precio con descuento a los nodos.

Los nodos reservados son específicos de la región en la cual compra la oferta. Si compra una oferta a través de la consola de Amazon Redshift, seleccione la región de AWS en la que desea comprar una oferta y, luego, complete el proceso de reserva. Si compra una oferta mediante programación, la región se determina con el punto de enlace de Amazon Redshift al que se conecta. Para obtener más información acerca de las regiones de Amazon Redshift, visite Regiones y puntos de conexión en la Referencia general de Amazon Web Services.

Para asegurarse de que se aplique la tarifa con descuento a todos los nodos cuando lanza un clúster, asegúrese de que la región, el tipo de nodo y la cantidad de nodos que seleccione coincidan con una o más reservas activas. De lo contrario, se le cobrará una tarifa bajo demanda por los nodos que no coincidan con una reserva activa.

En un clúster en ejecución, si supera la cantidad de nodos que tiene reservados, comienza a acumular cargos por esos nodos adicionales a una tarifa bajo pedido. Esta acumulación significa que es posible que se le cobren tarifas variables por los nodos de un mismo clúster, según la cantidad de nodos que haya reservado. Puede adquirir otra oferta para cubrir esos nodos adicionales y la tarifa

con descuento se aplicará a esos nodos en lo que reste de la duración una vez que el estado de la reserva sea active (activa).

Si redimensiona el clúster en un tipo de nodo diferente y no tiene nodos reservados de ese tipo, se le cobrará la tarifa bajo pedido. Puede comprar otra oferta con el tipo de nodo nuevo para el que desea recibir tarifas con descuento para su clúster redimensionado. Sin embargo, también continúa pagando por la reserva original hasta que transcurra su duración. Si necesita cambiar las reservas antes de que se venza el plazo, cree un caso de soporte a través de la consola de AWS.

Nodos reservados y facturación unificada

Los beneficios de precio de nodos reservados se comparten cuando la cuenta de adquisición es parte de un conjunto de cuentas facturadas en una sola cuenta del pagador de facturación consolidada. El uso por hora entre todas las subcuentas se acumula mensualmente en la cuenta del pagador. Por lo general, esta modalidad es útil para empresas en las que hay diferentes equipos o grupos funcionales; de este modo, se aplica la lógica normal de nodos reservados para calcular la factura. Para obtener más información, consulte Facturación unificada en la Guía del usuario de AWS Billing.

Ejemplos de nodos reservados

En los escenarios de esta sección, se demuestra de qué manera los nodos acumulan cargos según tarifas bajo pedido o con descuento utilizando los siguientes detalles de reserva:

- Región: EE. UU. Oeste (Oregón)
- Tipo de nodo: ra3.xlplus
- Opción de pago: sin pagos iniciales
- Duración: un año
- Cantidad de nodos reservados: 16

Ejemplo 1

Tiene un clúster en la región Oeste de EE. UU. (Oregón) con 20 nodos.

En este escenario, 16 de los nodos reciben la tarifa con descuento de la reserva, pero los 4 nodos adicionales en el clúster se facturan a una tarifa bajo pedido.

Ejemplo 2

Tiene un clúster en la región Oeste de EE. UU. (Oregón) con 12 nodos.

En este escenario, los 12 nodos del clúster reciben la tarifa con descuento de la reserva. No obstante, también paga por los nodos reservados restantes en la reserva, aunque actualmente no tenga un clúster en ejecución donde aplicarlos.

Ejemplo 3

Tiene un clúster en la región Oeste de EE. UU. (Oregón) con 12 nodos. Usted ejecuta el clúster durante varios meses con esta configuración y, luego, necesita añadir nodos al clúster. Redimensiona el clúster, elige el mismo tipo de nodo y especifica un total de 16 nodos.

En este escenario, se le factura la tarifa con descuento por los 16 nodos. Los cargos permanecen iguales durante todo el año de duración porque la cantidad de nodos que tiene en el clúster es igual a la cantidad de nodos que tiene reservados.

Ejemplo 4

Tiene un clúster en la región Oeste de EE. UU. (Oregón) con 16 nodos. Usted ejecuta el clúster durante varios meses con esta configuración y, luego, necesita añadir nodos. Redimensiona el clúster, elige el mismo tipo de nodo y especifica un total de 20 nodos.

En este escenario, se le factura la tarifa con descuento por todos los nodos antes del redimensionamiento. Luego del redimensionamiento, se le factura la tarifa con descuento por 16 de los nodos para el resto del año, y se le factura una tarifa bajo pedido para los 4 nodos adicionales que añadió al clúster.

Ejemplo 5

Tiene dos clústeres en la región Oeste de EE. UU. (Oregón). Uno de los clústeres tiene 6 nodos y el otro, 10 nodos.

En este escenario, se le factura tarifa con descuento para todos los nodos porque la cantidad total de nodos en ambos clústeres es igual a la cantidad de nodos que tiene reservados.

Ejemplo 6

Tiene dos clústeres en la región Oeste de EE. UU. (Oregón). Uno de los clústeres tiene 4 nodos y el otro, 6 nodos.

En este escenario, se le factura la tarifa con descuento para los 10 nodos que tiene en clústeres en ejecución y también paga la tarifa con descuento para los 6 nodos adicionales que tiene reservados, aunque actualmente no los aplique a ningún clúster en ejecución.

Adquisición de una oferta de nodo reservado con la consola de Amazon Redshift

Utilice la página Reserved Nodes (Nodos reservados) de la consola de Amazon Redshift para adquirir ofertas de nodos reservados y ver las reservas pasadas y actuales.

Después de adquirir una oferta, en la lista Reserved Node (Nodo reservado) se muestran las reservas y los detalles de cada una, como el tipo de nodo, la cantidad de nodos y el estado del proceso de reserva. Para obtener más información acerca de los detalles de las reservas, consulte Cómo funcionan los nodos reservados.

Para adquirir un nodo reservado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija Reserved nodes (Nodos reservados) para mostrar la lista de nodos reservados.
3. Seleccione Purchase reserved nodes (Adquirir nodos reservados) para mostrar la página para seleccionar las propiedades del nodo que quiere adquirir.
4. Entre en las propiedades del nodo y seleccione Purchase reserved nodes (Comprar nodos reservados)

Para actualizar un nodo reservado, use AWS CLI.

No puede convertir todos los tipos de nodos en nodos reservados, y también es posible que un nodo reservado existente no esté disponible para su renovación. Esto puede deberse a que el tipo de nodo ya no esté disponible. Póngase en contacto con el servicio de atención al cliente para renovar un tipo de nodo que ya no esté disponible.

Actualizar nodos reservados con AWS CLI

Para actualizar una reserva de nodo reservado con AWS CLI

1. Obtenga una lista de ReservedNodeOfferingID de ofertas que cumplan los requisitos de tipo de pago, plazo y cargos. En el siguiente ejemplo, se ilustra este paso.

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxx
{
    "ReservedNodeOfferings": [
        {
            "Duration": 31536000,
            "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
            "UsagePrice": 0.0,
            "NodeType": "dc2.large",
            "RecurringCharges": [
                {
                    "RecurringChargeFrequency": "Hourly",
                    "RecurringChargeAmount": 0.2
                }
            ],
            "CcurrencyCode": "USD",
            "OfferingType": "No Upfront",
            "ReservedNodeOfferingType": "Regular",
            "FixedPrice": 0.0
        }
    ]
}
```

2. Llame a `accept-reserved-node-exchange` y proporcione el ID del nodo reservado DC1 que quiere intercambiar junto con el ReservedNodeOfferingID que ha obtenido en el paso anterior.

   En el siguiente ejemplo, se ilustra este paso.

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-
xxxx-xxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyy-yyyy-yyyy-yyyy-
yyyyyyyyyyyy
{
    "ExchangedReservedNode": {
```

```
        "UsagePrice": 0.0,
        "OfferingType": "No Upfront",
        "State": "exchanging",
        "FixedPrice": 0.0,
        "CurrencyCode": "USD",
        "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzz",
        "NodeType": "dc2.large",
        "NodeCount": 1,
        "RecurringCharges": [
            {
                "RecurringChargeFrequency": "Hourly",
                "RecurringChargeAmount": 0.2
            }
        ],
        "ReservedNodeOfferingType": "Regular",
        "StartTime": "2018-06-27T18:02:58Z",
        "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
        "Duration": 31536000
    }
}
```

Puede confirmar que el intercambio se ha completado llamando a describe-reserved-nodes y comprobando el valor de `Node type`.

Adquisición de una oferta de nodo reservado mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de AWS CLI para adquirir las ofertas de nodos reservados.

- purchase-reserved-node-offering
- describe-reserved-node-offerings
- describe-orderable-cluster-options

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para adquirir las ofertas de nodos reservados.

- PurchaseReservedNodeOffering
- DescribeReservedNodeOfferings

- DescribeOrderableClusterOptions

No puede convertir todos los tipos de nodos en nodos reservados, y también es posible que un nodo reservado existente no esté disponible para su renovación. Esto puede deberse a que el tipo de nodo ya no esté disponible.

Seguridad en Amazon Redshift

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y el usuario. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS AWS también proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que corresponde aplicar a Amazon Redshift, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

El acceso a los recursos de Amazon Redshift se controla en cuatro niveles:

- Administración de clústeres: la capacidad para crear, configurar y eliminar clústeres se controla mediante los permisos que se conceden al usuario o la cuenta asociados a las credenciales de seguridad de AWS. Los usuarios con los permisos correspondientes pueden usar la AWS Management Console, la AWS Command Line Interface (CLI) o la interfaz de programación de aplicaciones (API) de Amazon Redshift para administrar sus clústeres. Este acceso se administra con políticas de IAM.

  > **Important**
  >
  > Amazon Redshift tiene una serie de prácticas recomendadas para administrar los permisos, las identidades y el acceso seguro. Le recomendamos que se familiarice con estos elementos cuando comience a utilizar Amazon Redshift. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

- Conectividad de los clústeres: los grupos de seguridad de Amazon Redshift especifican las instancias de AWS que tienen autorización para conectarse a un clúster de Amazon Redshift en

formato CIDR (enrutamiento entre dominios sin clases). Para obtener más información sobre cómo crear grupos de seguridad de Amazon Redshift, Amazon EC2 y Amazon VPC, y cómo asociarlos a los clústeres, consulte Grupos de seguridad del clúster de Amazon Redshift.

- Acceso a la base de datos: la capacidad para obtener acceso a objetos de la base de datos, como tablas y vistas, se controla con las cuentas de usuario de la base de datos de Amazon Redshift. Los usuarios solo pueden obtener acceso a los recursos de la base de datos para los cuales sus cuentas de usuario han recibido permiso. Las cuentas de usuario de Amazon Redshift y los permisos de administración se crean mediante las instrucciones CREATE USER, CREATE GROUP, GRANT y REVOKE de SQL. Para obtener más información, consulte Administración de la seguridad de bases de datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Credenciales temporales de bases de datos e inicio de sesión único: además de crear y administrar los usuarios de las bases de datos a través de comandos SQL, como CREATE USER y ALTER USER, puede configurar el cliente SQL con controladores personalizados JDBC u ODBC de Amazon Redshift. Estos controladores administran el proceso de creación de usuarios de bases de datos y contraseñas temporales como parte del proceso de inicio de sesión en la base de datos.

  Los controladores autentican a los usuarios de la base de datos en función de la autenticación de AWS Identity and Access Management (IAM). Si ya administra las identidades de los usuarios fuera de AWS, puede utilizar un proveedor de identidad (IdP) conforme con SAML 2.0 para administrar el acceso a los recursos de Amazon Redshift. Puede utilizar un rol de IAM para configurar el proveedor de identidad y AWS para permitir que los usuarios federados generen credenciales de base de datos temporales e inicien sesión en bases de datos de Amazon Redshift. Para obtener más información, consulte Uso de la autenticación de IAM para generar credenciales de usuario de base de datos.

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon Redshift. En los siguientes temas, se le mostrará cómo configurar Amazon Redshift para cumplir sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que ayudan a monitorear y proteger los recursos de Amazon Redshift.

Temas

- Protección de los datos en Amazon Redshift
- Administración de identidades y accesos en Amazon Redshift

- Administración de las contraseñas de administrador de Amazon Redshift mediante AWS Secrets Manager
- Registro y monitoreo en Amazon Redshift
- Validación de la conformidad para Amazon Redshift
- Resiliencia en Amazon Redshift
- Seguridad de la infraestructura de Amazon Redshift
- Configuración y análisis de vulnerabilidades en Amazon Redshift

Protección de los datos en Amazon Redshift

El Modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Redshift. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta la totalidad de Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog Modelo de responsabilidad compartida y GDPR de AWS en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. reSe recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.

- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon Redshift u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

La protección de los datos se refiere a salvaguardarlos mientras se encuentran en tránsito (cuando se desplazan desde y hacia Amazon Redshift) y en reposo (cuando están almacenados en los discos de los centros de datos de Amazon Redshift). Los datos en tránsito se pueden proteger mediante el uso de SSL o cifrado del lado del cliente. Dispone de las siguientes opciones para proteger los datos en reposo en Amazon Redshift.

- Uso del cifrado del lado del servidor: solicita a Amazon Redshift que cifre sus datos antes de guardarlos en los discos de sus centros de datos y que los descifre cuando descargue los objetos.
- Uso del cifrado del lado del cliente: puede cifrar los datos del lado del cliente y cargar los datos cifrados en Amazon Redshift. En este caso, administra el proceso de cifrado, las claves de cifrado y las herramientas relacionadas.

Cifrado en reposo

El cifrado del lado del servidor representa el cifrado de datos en reposo; esto implica que Amazon Redshift cifra opcionalmente los datos a medida que los escribe en sus centros de datos y los descifra cuando accede a ellos. Siempre que autentique su solicitud y tenga permiso de acceso, no existe diferencia alguna en la forma de obtener acceso a datos cifrados o sin cifrar.

Amazon Redshift protege los datos en reposo a través del cifrado. De forma opcional, puede proteger todos los datos almacenados en los discos en un clúster y todas las copias de seguridad en Amazon S3 con Advanced Encryption Standard AES-256.

Para administrar las claves que se usan para cifrar y descifrar los recursos de Amazon Redshift, utiliza AWS Key Management Service (AWS KMS). AWS KMS combina hardware y software seguros y de gran disponibilidad para proporcionar un sistema de administración de claves con escala para la nube. Si utiliza AWS KMS, puede crear claves de cifrado y definir las políticas que controlan cómo se pueden utilizar dichas claves. AWS KMS es compatible con AWS CloudTrail, lo que permite auditar el uso de claves para comprobar que las claves se utilizan de forma adecuada. Puede utilizar las claves de AWS KMS en combinación con Amazon Redshift y los servicios admitidos de AWS. Para obtener una lista de los servicios que admiten AWS KMS, consulte Cómo los servicios de AWS usan AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Si decide administrar el clúster aprovisionado o la contraseña de administrador del espacio de nombres sin servidor con AWS Secrets Manager, Amazon Redshift también acepta una clave de AWS KMS adicional que AWS Secrets Manager utiliza para cifrar sus credenciales. Esta clave adicional puede ser una clave generada automáticamente en AWS Secrets Manager o una clave personalizada proporcionada por usted.

El editor de consultas v2 de Amazon Redshift almacena de forma segura la información introducida en el editor de consultas de la siguiente manera:

- el nombre de recurso de Amazon (ARN) de la clave KMS que se utiliza para cifrar los datos del editor de consultas v2
- la información de conexión de base de datos
- los nombres y el contenido de archivos y carpetas

El editor de consultas v2 de Amazon Redshift cifra la información mediante el cifrado del nivel del bloque con su clave KMS o la clave KMS de la cuenta del servicio. El cifrado de los datos de Amazon Redshift se controla mediante las propiedades del clúster de Amazon Redshift.

Temas

- Cifrado de la base de datos de Amazon Redshift

Cifrado de la base de datos de Amazon Redshift

En Amazon Redshift, puede habilitar el cifrado de la base de datos de los clústeres para proteger los datos en reposo. Cuando habilita el cifrado para un clúster, se cifran los bloques de datos y metadatos del sistema para el clúster y sus instantáneas.

Puede habilitar el cifrado al lanzar el clúster o puede modificar un clúster sin cifrar para que utilice el cifrado AWS Key Management Service (AWS KMS). Para ello, puede usar una clave administrada por AWS o una clave administrada por el cliente. Cuando modifica su clúster para habilitar el cifrado de AWS KMS, Amazon Redshift migra sus datos de manera automática a un nuevo clúster cifrado. Las instantáneas creadas a partir del clúster cifrado también se cifran. También puede migrar un clúster cifrado a un clúster sin cifrar modificando el clúster y cambiando la opción Encrypt database (Cifrar base de datos). Para obtener más información, consulte Cambio del cifrado del clúster.

Si bien el cifrado es una configuración opcional en Amazon Redshift, le recomendamos habilitarlo para los clústeres que contengan información confidencial. Además, es posible que sea obligatorio utilizar cifrado según las directrices o regulaciones que rigen los datos. Por ejemplo, el Estándar de seguridad de datos (Data Security Standard, DSS) del sector de tarjetas de pago (Payment Card Industry, PCI), la Ley de Sarbanes-Oxley (SOX), la Ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) y otras regulaciones similares proporcionan directrices para el manejo de tipos específicos de datos.

Amazon Redshift utiliza una jerarquía de claves de cifrado para cifrar la base de datos. Puede usar AWS Key Management Service (AWS KMS) o un módulo de seguridad por hardware (HSM) para administrar las claves de cifrado de nivel superior en esta jerarquía. El proceso que utiliza Amazon Redshift para el cifrado varía según la manera en que usted administra las claves. Amazon Redshift se integra automáticamente a AWS KMS, pero no a un HSM. Cuando utilice un HSM, deberá usar certificados de cliente y servidor para configurar una conexión segura entre Amazon Redshift y el HSM.

Mejoras en el proceso de cifrado para mejorar el rendimiento y la disponibilidad

Cifrado con nodos RA3

Las actualizaciones del proceso de cifrado de los nodos RA3 han mejorado mucho la experiencia. Las consultas de lectura y las de escritura se pueden ejecutar durante el proceso con un menor impacto en el rendimiento del cifrado. Además, el cifrado finaliza mucho más rápido. Los pasos del proceso actualizado incluyen una operación de restauración y la migración de los metadatos del clúster a un clúster de destino. La experiencia mejorada se aplica a tipos de cifrado como AWS KMS,

por ejemplo. Cuando tiene volúmenes de datos a escala de petabytes, la operación se ha reducido de semanas a días.

Antes de cifrar el clúster, si tiene previsto seguir ejecutando cargas de trabajo de bases de datos, puede mejorar el rendimiento y acelerar el proceso agregando nodos con un cambio de tamaño elástico. No puede utilizar el cambio de tamaño elástico cuando el cifrado está en proceso, así que hágalo antes de cifrar. Tenga en cuenta que agregar nodos suele generar un costo más alto.

Cifrado con otros tipos de nodos

Al cifrar un clúster con nodos DC2 o DS2, no tiene la capacidad de ejecutar consultas de escritura, como ocurre con los nodos RA3. Solo se pueden ejecutar consultas de lectura.

Notas de uso para el cifrado con nodos RA3

La siguiente información y los recursos le ayudan a prepararse para el cifrado y a monitorear el proceso.

- Ejecución de consultas después de iniciar el cifrado: una vez iniciado el cifrado, las lecturas y escrituras están disponibles en unos quince minutos. El tiempo que tarda todo el proceso de cifrado en completarse depende de la cantidad de datos del clúster y de los niveles de carga de trabajo.
- ¿Cuánto tarda el cifrado? - El tiempo necesario para cifrar los datos depende de varios factores: entre ellos, la cantidad de cargas de trabajo en ejecución, los recursos informáticos que se utilizan, la cantidad de nodos y el tipo de nodos. Le recomendamos que primero realice el cifrado en un entorno de pruebas. Como regla general, si trabaja con volúmenes de datos en petabytes, es probable que el cifrado tarde entre 1 y 3 días en completarse.
- ¿Cómo sé que el cifrado ha finalizado? - Tras habilitar el cifrado, al completar la primera instantánea se confirma que el cifrado se ha completado.
- Revertir el cifrado: si necesita revertir la operación de cifrado, la mejor forma de hacerlo es restaurar desde la copia de seguridad más reciente realizada antes de iniciar el cifrado. Deberá volver a aplicar las actualizaciones nuevas (actualizaciones/eliminaciones/inserciones) después de la última copia de seguridad.
- Realizar una restauración de tablas: tenga en cuenta que no puede restaurar una tabla de un clúster no cifrado a un clúster cifrado.
- Cifrado de un clúster de un solo nodo: el cifrado de un clúster de un solo nodo tiene limitaciones de rendimiento. Se tarda más que el cifrado en un clúster de varios nodos.

- Creación de una copia de seguridad después del cifrado: al cifrar los datos del clúster, no se crea una copia de seguridad hasta que el clúster esté completamente cifrado. El tiempo que dure puede variar. El tiempo necesario para realizar la copia de seguridad puede ser de horas a días, en función del tamaño del clúster. Una vez completo el cifrado, es posible que se produzca un retraso antes de que pueda crear una copia de seguridad.

  Tenga en cuenta que como durante el proceso de cifrado se produce una operación de copia de seguridad y restauración, las tablas o vistas materializadas creadas con `BACKUP NO` no se retienen. Para obtener más información, consulte CREATE TABLE o CREATE MATERIALIZED VIEW.

Temas

- Cifrado de la base de datos de Amazon Redshift con AWS KMS
- Cifrado de Amazon Redshift con módulos de seguridad de hardware
- Rotación de claves de cifrado en Amazon Redshift
- Cambio del cifrado del clúster
- Configuración del cifrado de la base de datos mediante la consola
- Configuración del cifrado de la base de datos con la y la API de Amazon Redshift AWS CLI

Cifrado de la base de datos de Amazon Redshift con AWS KMS

Cuando elige AWS KMS para administrar las claves con Amazon Redshift, hay una jerarquía de cuatro niveles en las claves de cifrado. Estas claves, en orden jerárquico, son la clave raíz, una clave de cifrado de clúster (CEK), una clave de cifrado de base de datos (DEK) y claves de cifrado de datos.

Cuando lanza el clúster, Amazon Redshift devuelve una lista de AWS KMS keys que su cuenta de AWS ha creado o tiene permiso para usar en AWS KMS. Seleccione una clave KMS para utilizar como la clave raíz en la jerarquía de cifrado.

De forma predeterminada, Amazon Redshift selecciona la clave predeterminada como la clave raíz. La clave predeterminada es una clave administrada por AWS que se crea para la cuenta de AWS, la cual se utilizará en Amazon Redshift. AWS KMS crea esta clave la primera vez que lanza un clúster cifrado en una región de AWS y elige la clave predeterminada.

Si no desea utilizar la clave predeterminada, debe tener (o crear) una clave KMS administrada por el cliente por separado en AWS KMS antes de lanzar su clúster en Amazon Redshift. Las claves

administradas por el cliente le ofrecen una mayor flexibilidad, incluida la opción de crear, rotar, desactivar, definir los controles de acceso y auditar las claves de cifrado que se utilizan para proteger los datos. Para obtener más información sobre la creación de claves KMS, consulte Creating Keys (Creación de claves) en la Guía para desarrolladores de AWS Key Management Service.

Si desea utilizar una clave de AWS KMS de otra cuenta de AWS, debe tener permiso para utilizar la clave y especificar su nombre de recurso de Amazon (ARN) en Amazon Redshift. Para obtener más información acerca del acceso a las claves en AWS KMS, consulte Control del acceso a sus claves en la Guía para desarrolladores de AWS Key Management Service.

Después de elegir una clave raíz, Amazon Redshift le solicitará a AWS KMS que genere una clave de datos y la cifre con la clave raíz seleccionada. Esta clave de datos se utiliza como la CEK en Amazon Redshift. AWS KMS exporta la CEK cifrada a Amazon Redshift, donde se almacena internamente en el disco en una red separada del clúster junto con la autorización de la clave KSM y el contexto de cifrado de la CEK. Solo se exporta la CEK cifrada a Amazon Redshift; la clave KMS permanece en AWS KMS. Amazon Redshift también transmite la CEK cifrada a través de un canal seguro al clúster y la carga en la memoria. Luego, Amazon Redshift llama a AWS KMS para descifrar la CEK y carga la CEK descifrada en la memoria. Para obtener más información acerca de las autorizaciones, el contexto de cifrado y otros conceptos relacionados con AWS KMS, consulte Conceptos en la Guía para desarrolladores de AWS Key Management Service.

A continuación, Amazon Redshift genera aleatoriamente una clave para utilizarla como la DEK y la carga en la memoria del clúster. La CEK descifrada se utiliza para cifrar la DEK, que luego se transmite a través de un canal seguro desde el clúster para que la almacene internamente Amazon Redshift en el disco a través de una red separada del clúster. Como sucede con la CEK, ambas versiones cifradas y descifradas de la DEK se cargan en la memoria del clúster. La versión descifrada de la DEK se utiliza posteriormente para cifrar las claves de cifrado individuales que se generan aleatoriamente para cada bloque de datos de la base de datos.

Cuando se reinicia el clúster, Amazon Redshift comienza a funcionar con las versiones cifradas de la CEK y la DEK almacenadas internamente, las vuelve a cargar en la memoria y, luego, llama a AWS KMS para que descifre de nuevo la CEK con la clave KSM para poder cargarla en la memoria. La CEK descifrada se utiliza posteriormente para descifrar la DEK nuevamente, y la DEK descifrada se carga en la memoria y se utiliza para cifrar y descifrar las claves de bloque de datos según sea necesario.

Para obtener más información acerca de la creación de clústeres de Amazon Redshift que están cifrados con claves de AWS KMS, consulte Creación de un clúster y Administración de clústeres mediante la AWS CLI y la API de Amazon Redshift.

Copia de instantáneas cifradas por AWS KMS en otra región de AWS

Las claves de AWS KMS son específicas de una región de AWS. Si habilita la copia de instantáneas de Amazon Redshift en otra región de AWS, y el clúster de origen y sus instantáneas están cifrados con una clave raíz de AWS KMS, deberá configurar una autorización para que Amazon Redshift pueda utilizar una clave raíz en la región de AWS de destino. Esta autorización permite a Amazon Redshift cifrar instantáneas en la región de AWS de destino. Para obtener más información acerca de la copia de instantáneas entre regiones, consulte Copia de instantáneas a otra región de AWS.

> **Note**
>
> Si habilita la copia de instantáneas desde un clúster cifrado y utiliza AWS KMS como la clave raíz, no puede cambiar el nombre del clúster, ya que el nombre del clúster es parte del contexto de cifrado. Si debe cambiar el nombre del clúster, puede desactivar la copia de instantáneas en la región de AWS de origen, cambiar el nombre del clúster y, luego, configurar y habilitar de nuevo la copia de instantáneas.

A continuación se detalla el proceso para configurar la autorización para la copia de instantáneas.

1. En la región de AWS de destino, cree una autorización de copia de instantáneas llevando a cabo las siguientes acciones:
   - Si no dispone de una clave de AWS KMS, cree una. Para obtener más información sobre cómo crear claves de AWS KMS, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service.
   - Especifique un nombre para la autorización de copia de instantáneas. Este nombre debe ser único en esa región de AWS para su cuenta de AWS.
   - Especifique el ID de la clave de AWS KMS para la que crea la autorización. Si no especifica un ID de clave, la autorización se aplica a la clave predeterminada.
2. En la región de AWS de origen, habilite la copia de instantáneas y especifique el nombre de la autorización de copia de instantáneas que creó en la región de AWS de destino.

Este proceso anterior solo es necesario si habilita la copia de instantáneas a través de la AWS CLI, la API de Amazon Redshift o los SDK. Si utiliza la consola, Amazon Redshift proporciona el flujo de trabajo adecuado para configurar la autorización cuando usted habilita la copia de instantáneas entre regiones. Para obtener más información acerca de la configuración para copiar instantáneas entre

regiones con clústeres cifrados por AWS KMS mediante la consola, consulte Configurar la copia de instantáneas entre regiones para un clúster cifrado en AWS KMS.

Antes de copiar la instantánea en la región de AWS de destino, Amazon Redshift descifra la instantánea con la clave raíz en la región de AWS de origen y la vuelve a cifrar temporalmente utilizando una clave de RSA generada de forma aleatoria que Amazon Redshift administra de manera interna. Luego, Amazon Redshift copia la instantánea a través de un canal seguro en la región de AWS de destino, descifra la instantánea con la clave de RSA administrada internamente y, a continuación, vuelve a cifrar la instantánea con la clave raíz en la región de AWS de destino.

Para obtener más información acerca de la configuración de autorizaciones para copiar instantáneas de clústeres cifrados con AWS KMS, consulte Configuración de Amazon Redshift de manera que utilice las claves de cifrado de AWS KMS con la AWS CLI y la API de Amazon Redshift.

Cifrado de Amazon Redshift con módulos de seguridad de hardware

Si no utiliza AWS KMS para la administración de las claves, puede usar un módulo de seguridad de hardware (HSM) para administrar las claves con Amazon Redshift.

> **Important**
>
> No se admite el cifrado de HSM para los tipos de nodos DC2 y RA3.

Los HSM son dispositivos que proporcionan control directo de la generación y administración de claves. Proporcionan más seguridad, ya que separan la administración de claves de las capas de aplicación y base de datos. Amazon Redshift admite AWS CloudHSM Classic para la administración de claves. El proceso de cifrado es diferente cuando usa HSM para administrar las claves de cifrado en lugar de AWS KMS.

> **Important**
>
> Amazon Redshift solo es compatible con AWS CloudHSM Classic. No se admite el servicio AWS CloudHSM más reciente.
> AWS CloudHSM Classic está cerrado para los clientes nuevos. Para obtener más información, consulte Precios de CloudHSM Classic. AWS CloudHSM Classic no está disponible en todas las regiones de AWS. Para obtener más información acerca de las regiones de AWS disponibles, consulte la Tabla de regiones de AWS.

Cuando configura el clúster para utilizar un HSM, Amazon Redshift envía una solicitud al HSM para generar y almacenar una clave para utilizarla como la CEK. Sin embargo, a diferencia de AWS KMS, el HSM no exporta la CEK a Amazon Redshift. En cambio, Amazon Redshift genera aleatoriamente la DEK en el clúster y la transmite al HSM para que se cifre con la CEK. El HSM devuelve la DEK cifrada a Amazon Redshift, donde se cifra aún más utilizando una clave raíz interna que se genera de forma aleatoria y se almacena internamente en el disco en una red separada del clúster. Amazon Redshift también carga la versión descifrada de la DEK en la memoria del clúster para que se pueda utilizar para cifrar y descifrar las claves individuales de los bloques de datos.

Si se reinicia el clúster, Amazon Redshift descifra la DEK con doble cifrado que se almacenó de forma interna con la clave raíz interna para que la DEK almacenada de forma interna vuelva al estado cifrado por la CEK. Luego, la DEK cifrada por la CEK se transmite al HSM para que se descifre y transfiera de nuevo a Amazon Redshift, donde se puede cargar en la memoria otra vez para utilizarla con las claves individuales de los bloques de datos.

Configuración de una conexión segura entre Amazon Redshift y un HSM

Cuando elige utilizar un HSM para la administración de la clave del clúster, debe configurar un enlace de red seguro entre Amazon Redshift y el HSM. Para hacerlo, necesita configurar los certificados de cliente y servidor. La conexión segura se utiliza para transmitir las claves de cifrado entre el HSM y Amazon Redshift durante las operaciones de cifrado y descifrado.

Amazon Redshift crea un certificado público de cliente a partir de un par de claves, una privada y otra pública generadas aleatoriamente. Estas se cifran y almacenan internamente. Descargue y registre el certificado de cliente público en el HSM, y asígnelo a la partición de HSM aplicable.

Tiene que proporcionar a Amazon Redshift la dirección IP del HSM, el nombre de partición del HSM, la contraseña de partición del HSM y un certificado de servidor del HSM público, que se cifra utilizando una clave raíz interna. Amazon Redshift completa el proceso de configuración y verifica que puede conectarse al HSM. Si no puede conectarse, el clúster se coloca en el estado INCOMPATIBLE_HSM y no se crea. En este caso, debe eliminar el clúster incompleto y volver a intentarlo.

> **Important**
>
> Cuando modifica el clúster para que use una partición de HSM diferente, Amazon Redshift verifica que pueda conectarse a la nueva partición, pero no verifica si existe una clave de cifrado válida. Antes de usar la nueva partición, debe replicar las claves en la nueva partición. Si el clúster se reinicia y Amazon Redshift no puede encontrar una clave válida, el reinicio

produce un error. Para obtener más información, consulte Replicación de claves en varios HSM.

Después de la configuración inicial, si Amazon Redshift no puede conectarse al HSM, se registra un evento. Para obtener más información acerca de estos eventos, consulte Notificaciones de eventos de Amazon Redshift.

Rotación de claves de cifrado en Amazon Redshift

En Amazon Redshift, puede rotar las claves de cifrado de los clústeres cifrados. Cuando inicia el proceso de rotación de claves, Amazon Redshift rota la CEK del clúster especificado y de cualquier instantánea automatizada o manual del clúster. Amazon Redshift también rota la DEK del clúster especificado, pero no puede rotar la DEK de las instantáneas mientras están almacenadas internamente en Amazon Simple Storage Service (Amazon S3) y permanecen cifradas con la DEK existente.

Mientras la rotación está en curso, el clúster entra en el estado ROTATING_KEYS hasta que finaliza el proceso, momento en el que vuelve al estado AVAILABLE. Amazon Redshift administra el descifrado y el recifrado durante el proceso de rotación de claves.

> **Note**
>
> No puede cambiar claves para instantáneas que no tienen un clúster de origen. Antes de eliminar un clúster, verifique si sus instantáneas dependen de una rotación de claves.

Debido a que el clúster no está disponible momentáneamente durante el proceso de rotación de claves, debe cambiar las claves solo cuando lo requieran los datos o cuando sospeche que las claves están en riesgo. Como práctica recomendada, debe revisar el tipo de datos que almacena y planificar la frecuencia con la que cambia las claves que cifran esos datos. La frecuencia de la rotación de claves varía según las políticas corporativas de seguridad de datos y cualquier estándar que se refiera a información confidencial y conformidad normativa. Asegúrese de que el plan equilibre las necesidades de seguridad con las consideraciones de disponibilidad para el clúster.

Para obtener más información acerca de rotación de claves, consulte Rotación de las claves de cifrado con la consola de Amazon Redshift y Rotación de las claves de cifrado con la y la API de Amazon Redshift AWS CLI.

Cambio del cifrado del clúster

Puede modificar un clúster no cifrado para que use el cifrado de AWS Key Management Service (AWS KMS), mediante una clave administrada por AWS o una clave administrada por el cliente. Cuando modifica su clúster para habilitar el cifrado de AWS KMS, Amazon Redshift migra sus datos de manera automática a un nuevo clúster cifrado. También puede migrar un clúster no cifrado a un clúster cifrado modificando el clúster.

Durante la operación de migración, el clúster se encuentra disponible en modo de solo lectura y su estado es resizing (cambiando tamaño).

Si el clúster está configurado para permitir la copia de instantáneas entre regiones de AWS, debe desactivarla antes de cambiar el cifrado. Para obtener más información, consulte Copia de instantáneas a otra región de AWS y Configurar la copia de instantáneas entre regiones para un clúster cifrado en AWS KMS. No puede habilitar el cifrado de Hardware Security Module (HSM, Módulo de seguridad de hardware) modificando el clúster. En lugar de ello, debe crear un nuevo clúster cifrado con HSM y migrar los datos al nuevo clúster. Para obtener más información, consulte Migración a un clúster cifrado con HSM.

Para modificar el cifrado de la base de datos en un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el clúster del cual desea modificar el cifrado.
3. Seleccione Propiedades.
4. En la sección Database configurations (Configuraciones de las bases de datos), elija Edit (Editar) y, luego, Edit encryption (Editar cifrado).
5. Elija alguna de las opciones de cifrado y seleccione Save changes (Guardar cambios).

Para cambiar el cifrado de un clúster mediante la CLI

Para modificar su clúster no cifrado para usar AWS KMS, ejecute el comando de la CLI `modify-cluster` y especifique `--encrypted`, tal como se muestra a continuación. De forma predeterminada, se utiliza la clave de KMS predeterminada. Para especificar una clave administrada por el cliente, incluya la opción `--kms-key-id`.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id
 <value>
```

Para quitar el cifrado de su clúster, ejecute el siguiente comando de la CLI.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

Migración a un clúster cifrado con HSM

Para migrar un clúster sin cifrar a un clúster cifrado mediante un módulo de seguridad de hardware (HSM), debe crear un nuevo clúster cifrado y trasladar los datos al nuevo clúster. No puede realizar una migración a un clúster cifrado con HSM modificando el clúster.

Para migrar de un clúster sin cifrar a un clúster cifrado con HSM, primero debe descargar los datos del clúster de origen existente. A continuación, vuelva a cargar los datos en un clúster nuevo, o clúster de destino, con la configuración de cifrado que desee. Para obtener más información sobre cómo lanzar un clúster cifrado, consulte Cifrado de la base de datos de Amazon Redshift.

Durante el proceso de migración, el clúster de origen está disponible para consultas de solo lectura hasta el último paso. El último paso consiste en cambiar el nombre de los clústeres de destino y de origen, lo que cambia los puntos de enlace para que todo el tráfico se dirija al nuevo clúster de destino. El clúster de destino no está disponible hasta que se reinicia después de cambiarle el nombre. Suspenda todas las cargas de datos y otras operaciones de escritura en el clúster de origen mientras durante la transferencia de los datos.

Para preparar la migración

1. Identifique todos los sistemas dependientes que interactúan con Amazon Redshift, por ejemplo, las herramientas de inteligencia empresarial (BI) y los sistemas de extracción, transformación y carga (ETL).
2. Identifique las consultas de validación que permiten probar la migración.

   Por ejemplo, puede utilizar la consulta siguiente para buscar el número de tablas definidas por el usuario.

   ```
   select count(*)
   from pg_table_def
   where schemaname != 'pg_catalog';
   ```

La consulta siguiente devuelve una lista de todas las tablas definidas por el usuario y el número de filas de cada tabla.

```
select "table", tbl_rows
from svv_table_info;
```

3. Elija un buen momento para la migración. Para encontrar un momento en el que el uso del clúster sea mínimo, monitorice las métricas del clúster, como la utilización de la CPU y el número de conexiones a la base de datos. Para obtener más información, consulte Visualización de datos de rendimiento del clúster.
4. Elimine las tablas que no se utilicen.

   Para crear una lista de tablas con el número de veces que se ha consultado cada tabla, ejecute la consulta siguiente.

```
select database,
schema,
table_id,
"table",
round(size::float/(1024*1024)::float,2) as size,
sortkey1,
nvl(s.num_qs,0) num_qs
from svv_table_info t
left join (select tbl,
perm_table_name,
count(distinct query) num_qs
from stl_scan s
where s.userid > 1
and   s.perm_table_name not in ('Internal worktable','S3')
group by tbl,
perm_table_name) s on s.tbl = t.table_id
where t."schema" not in ('pg_internal');
```

5. Lance un clúster cifrado nuevo.

   Utilice el mismo número de puerto para el clúster de destino que para el clúster de origen. Para obtener más información sobre cómo lanzar un clúster cifrado, consulte Cifrado de la base de datos de Amazon Redshift.
6. Configure el proceso de descarga y carga.

Puede utilizar la utilidad Unload/Copy de Amazon Redshift para facilitar la migración de datos entre clústeres. La utilidad exporta los datos del clúster de origen a una ubicación en Amazon S3. Los datos se cifran con AWS KMS. A continuación, la utilidad importa automáticamente los datos en el clúster de destino. También puede usar la utilidad para limpiar Amazon S3 una vez finalizada la migración.

7. Ejecute una prueba para verificar el proceso y estimar durante cuánto tiempo deben suspenderse las operaciones de escritura.

   Durante las operaciones de descarga y carga, mantenga la consistencia de los datos suspendiendo las cargas de datos y otras operaciones de escritura. Ejecute el proceso de descarga y carga usando una de sus tablas más grandes para realizar una estimación del tiempo.

8. Cree los objetos de base de datos, como esquemas, vistas y tablas. Los scripts de AdminViews del repositorio GitHub de AWS pueden ayudarlo a generar las instrucciones de lenguaje de definición de datos (DDL) necesarias.

Para migrar el clúster

1. Detenga todos los procesos ETL en el clúster de origen.

   Para confirmar que no hay operaciones de escritura en proceso, utilice la consola de administración de Amazon Redshift para monitorear las IOPS de escritura. Para obtener más información, consulte Visualización de datos de rendimiento del clúster.

2. Ejecute las consultas de validación que identificó anteriormente para recopilar información sobre el clúster de origen sin cifrar antes de la migración.

3. (Opcional) Cree una cola de administración de cargas de trabajo (WLM) para utilizar el máximo de recursos disponibles, tanto en el clúster de origen como en el de destino. Por ejemplo, cree una cola denominada `data_migrate` y configúrela con una memoria del 95 por ciento y una simultaneidad de 4. Para obtener más información, consulte Enrutamiento de consultas a las colas en función de los grupos de usuarios y consultas en la Guía para desarrolladores de bases de datos de Amazon Redshift.

4. Ejecute UnloadCopyUtility utilizando la cola `data_migrate`.

   Monitoree el proceso de UNLOAD y COPY a través de la consola de Amazon Redshift.

5. Vuelva a ejecutar las consultas de validación y verifique que los resultados coinciden con los del clúster de origen.

6. Cambie el nombre de los clústeres de origen y de destino para intercambiar los puntos de enlace. Para evitar interrupciones, realice esta operación fuera del horario normal de trabajo.
7. Compruebe que puede conectarse al clúster de destino utilizando todos sus clientes SQL, como las herramientas de ETL y de generación de informes.
8. Cierre el clúster de origen sin cifrar.

Configuración del cifrado de la base de datos mediante la consola

Puede utilizar la consola de Amazon Redshift para configurar este servicio de modo que utilice un HSM y rote las claves de cifrado. Para obtener más información sobre cómo crear clústeres con claves de cifrado de AWS KMS, consulte Creación de un clúster y Administración de clústeres mediante la AWS CLI y la API de Amazon Redshift.

Para modificar el cifrado de la base de datos en un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y elija el clúster del que desea mover las instantáneas.
3. En Actions (Acciones), seleccione Modify (Modificar) para mostrar la página de configuración.
4. En la sección de Database configuration (Configuración de la base de datos), elija la configuración de Encryption (Cifrado) y luego seleccione Modify cluster (Modificar clúster).

Rotación de las claves de cifrado con la consola de Amazon Redshift

Puede utilizar el siguiente procedimiento para rotar las claves de cifrado con la consola de Amazon Redshift.

Rotar las claves de cifrado de un clúster.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el clúster del cual desea actualizar las claves de cifrado.
3. Para Actions (Acciones), haga clic en Rotate encryption (Rotar cifrado) para mostrar la página Rotate encryption keys (Rotar claves de cifrado).

4. En la página Rotate encryption keys (Rotar claves de cifrado), haga clic en Rotate encryption keys (Rotar claves de cifrado).

Configuración del cifrado de la base de datos con la y la API de Amazon Redshift AWS CLI

Utilice la AWS Command Line Interface (AWS CLI) y la API de Amazon Redshift para configurar las opciones de claves de cifrado de las bases de datos de Amazon Redshift. Para obtener más información acerca del cifrado de la base de datos, consulte Cifrado de la base de datos de Amazon Redshift.

Configuración de Amazon Redshift de manera que utilice las claves de cifrado de AWS KMS con la AWS CLI y la API de Amazon Redshift

Puede realizar las siguientes acciones de la API de Amazon Redshift para configurar dicho servicio de manera que utilice las claves de cifrado de AWS KMS.

- CreateCluster
- CreateSnapshotCopyGrant
- DescribeSnapshotCopyGrants
- DeleteSnapshotCopyGrant
- DisableSnapshotCopy
- EnableSnapshotCopy

Puede efectuar las siguientes operaciones de la CLI de Amazon Redshift para configurar dicho servicio de manera que utilice las claves de cifrado de AWS KMS.

- create-cluster
- create-snapshot-copy-grant
- describe-snapshot-copy-grants
- delete-snapshot-copy-grant
- disable-snapshot-copy
- enable-snapshot-copy

Configuración de Amazon Redshift con la y la API de Amazon Redshift de manera que utilice un HSM AWS CLI

Puede realizar las siguientes acciones de la API de Amazon Redshift para administrar los módulos de seguridad de hardware.

- CreateHsmClientCertificate
- CreateHsmConfiguration
- DeleteHsmClientCertificate
- DeleteHsmConfiguration
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

Puede utilizar las siguientes operaciones de la AWS CLI para administrar los módulos de seguridad de hardware.

- create-hsm-client-certificate
- create-hsm-configuration
- delete-hsm-client-certificate
- delete-hsm-configuration
- describe-hsm-client-certificates
- describe-hsm-configurations

Rotación de las claves de cifrado con la y la API de Amazon Redshift AWS CLI

Puede utilizar las siguientes acciones de la API de Amazon Redshift para rotar las claves de cifrado.

- RotateEncryptionKey

Puede utilizar las siguientes operaciones de la AWS CLI para rotar las claves de cifrado.

- rotate-encryption-key

Cifrado en tránsito

Puede configurar su entorno para proteger los datos sobre confidencialidad e integridad en tránsito.

Cifrado de datos en tránsito entre un clúster de Amazon Redshift y clientes SQL a través de JDBC/ODBC:

- Puede conectarse a clústeres de Amazon Redshift desde herramientas de cliente SQL mediante conexiones Java Database Connectivity (JDBC) y Open Database Connectivity (ODBC).
- Amazon Redshift admite las conexiones de capa de conexión segura (SSL) para cifrar datos y los certificados de servidor para validar el certificado del servidor al que se conecta el cliente. El cliente se conecta al nodo principal de un clúster de Amazon Redshift. Para obtener más información, consulte Configuración de las opciones de seguridad para las conexiones.
- Para admitir las conexiones SSL, Amazon Redshift crea e instala los certificados emitidos por AWS Certificate Manager (ACM) en cada clúster. Para obtener más información, consulte Migración a certificados de ACM para las conexiones SSL.
- Para proteger los datos en tránsito dentro de la nube de AWS, Amazon Redshift usa SSL con aceleración por hardware para comunicarse con Amazon S3 o Amazon DynamoDB en las operaciones de COPY, UNLOAD, copia de seguridad y restauración.

Cifrado de datos en tránsito entre un clúster de Amazon Redshift y Amazon S3 o DynamoDB:

- Amazon Redshift usa SSL con aceleración por hardware para comunicarse con Amazon S3 o DynamoDB en las operaciones de COPY, UNLOAD, copia de seguridad y restauración.
- Redshift Spectrum admite el cifrado del lado del servidor (SSE) de Amazon S3 mediante el uso de la clave predeterminada de su cuenta administrada por AWS Key Management Service (KMS).
- Cifre las cargas de Amazon Redshift con Amazon S3 y AWS KMS. Para obtener más información, consulte Encrypt Your Amazon Redshift Loads with Amazon S3 and AWS KMS.

Cifrado y firma de datos en tránsito entre los clientes de la AWS CLI, el SDK o la API, y los puntos de enlace de Amazon Redshift:

- Amazon Redshift proporciona puntos de enlace HTTPS para cifrar datos en tránsito.
- Para proteger la integridad de las solicitudes de la API a Amazon Redshift, las llamadas a la API deben estar firmadas por la persona que llama. Las llamadas se firman con un certificado X.509 o con la clave de acceso secreta de AWS del cliente, según el proceso de firma de Signature Version 4 (Sigv4). Para obtener más información, consulte Proceso de firma Signature Version 4 en la Referencia general de AWS.

- Use la AWS CLI o alguno de los AWS SDK para efectuar solicitudes a AWS. Estas herramientas firman automáticamente las solicitudes con la clave de acceso especificada al configurar las herramientas.

Cifrado de datos en tránsito entre los clústeres de Amazon Redshift y el editor de consultas v2 de Amazon Redshift

- Los datos se transmiten entre el editor de consultas v2 y los clústeres de Amazon Redshift a través de un canal con cifrado de TLS.

Administración de claves

Puede configurar su entorno para proteger los datos con las claves.

- Amazon Redshift se integra automáticamente a AWS Key Management Service (AWS KMS) para la administración de claves. AWS KMS utiliza el cifrado de sobres. Para obtener más información, consulte Cifrado de sobre.
- Cuando las claves de cifrado se administran en AWS KMS, Amazon Redshift usa una arquitectura de cuatro niveles basada en claves para el cifrado. La arquitectura consta de claves de cifrado de datos AES-256 generadas aleatoriamente, una clave de base de datos, una clave de clúster y una clave raíz. Para obtener más información, consulte Cómo Amazon Redshift usa AWS KMS.
- Puede crear su propia clave administrada por el cliente en AWS KMS. Para obtener más información, consulte Creación de claves.
- También puede importar su propio material de claves para las nuevas AWS KMS keys. Para obtener más información, consulte Importación de material de claves en AWS Key Management Service (AWS KMS).
- Amazon Redshift admite la administración de claves de cifrado en módulos de seguridad de hardware (HSM) externos. El HSM puede estar ubicado en las instalaciones o ser AWS CloudHSM. Cuando utilice un HSM, deberá usar certificados de cliente y servidor para configurar una conexión segura entre Amazon Redshift y el HSM. Amazon Redshift solo admite AWS CloudHSM Classic para la administración de claves. Para obtener más información, consulte Cifrado de Amazon Redshift con módulos de seguridad de hardware. Para obtener más información sobre AWS CloudHSM, consulte ¿Qué es AWS CloudHSM?
- Puede cambiar las claves de cifrado para los clústeres cifrados. Para obtener más información, consulte Rotación de claves de cifrado en Amazon Redshift.

Tokenización de datos

La tokenización es el proceso que consiste en reemplazar valores reales con valores opacos con fines de seguridad de datos. Las aplicaciones que tienen muchos requisitos en torno a la seguridad utilizan la tokenización para reemplazar la información confidencial, como la información de identificación personal (PII) o la información de salud protegida (PHI), con tokens para reducir los riesgos de seguridad. La destokenización revierte los tokens con valores reales para los usuarios autorizados con las políticas de seguridad adecuadas.

Para la integración a servicios de tokenización de terceros, puede utilizar las funciones definidas por el usuario (UDF) de Amazon Redshift que cree con AWS Lambda. Para obtener más información, consulte Funciones de Lambda definidas por el usuario en la Guía para desarrolladores de bases de datos de Amazon Redshift. Por ejemplo, consulte Protegrity.

Amazon Redshift envía solicitudes de tokenización a un servidor de tokenización al que se accede a través de una API REST o un punto de enlace predefinido. Dos o más funciones de Lambda complementarias procesan las solicitudes de tokenización y destokenización. Para este procesamiento, puede usar las funciones de Lambda proporcionadas por un proveedor de tokenización externo. También puede utilizar las funciones de Lambda que registre como las UDF de Lambda en Amazon Redshift.

Por ejemplo, supongamos que se envía una consulta que invoca una UDF de tokenización o destokenización en una columna. El clúster de Amazon Redshift almacena las filas de argumentos aplicables y envía en paralelo esas filas a través de lotes a la función de Lambda. Las transferencias de datos entre los nodos informáticos de Amazon Redshift y Lambda se efectúan a través de una conexión de red independiente y aislada que no es accesible para los clientes. La función de Lambda transfiere los datos al punto de enlace del servidor de tokenización. El servidor de tokenización tokeniza o destokeniza los datos según sea necesario y los devuelve. A continuación, las funciones de Lambda transmiten los resultados al clúster de Amazon Redshift para continuar su procesamiento, si fuera necesario, y luego devuelven los resultados de la consulta.

Privacidad del tráfico entre redes

Para dirigir el tráfico entre Amazon Redshift y los clientes y las aplicaciones de una red corporativa:

- Configure una conexión privada entre su nube virtual privada (VPC) y su red corporativa. Configure una conexión de VPN IPsec a través de Internet o una conexión física privada usando la conexión de AWS Direct Connect. AWS Direct Connect le permite establecer una interfaz virtual privada desde la red en las instalaciones directamente hacia su VPC de Amazon VPC, lo que le

proporciona una conexión de red privada con un ancho de banda alto entre la red y la VPC. Con varias interfaces virtuales, puede incluso establecer conectividad privada con varias VPC al tiempo que mantiene aislada la red. Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN? y ¿Qué es AWS Direct Connect?

Para dirigir el tráfico entre un clúster de Amazon Redshift de una VPC y buckets de Amazon S3 ubicados en la misma región de AWS:

- Configure un punto de enlace de la VPC privado de Amazon S3 para acceder a los datos de Amazon S3 de forma privada desde una carga o descarga de ETL. Para obtener más información, consulte Puntos de enlace para Amazon S3.
- Habilite “Enhanced VPC routing” (Enrutamiento mejorado de VPC) para un clúster de Amazon Redshift y especifique un punto de enlace de la VPC de Amazon S3 de destino. A continuación, el tráfico generado por los comandos COPY, UNLOAD o CREATE LIBRARY de Amazon Redshift pasará por el punto de enlace privado. Para obtener más información, consulte Enhanced VPC Routing.

Administración de identidades y accesos en Amazon Redshift

El acceso a Amazon Redshift requiere credenciales que AWS puede utilizar para autenticar las solicitudes. Estas credenciales deben tener permisos para obtener acceso a los recursos de AWS, como un clúster de Amazon Redshift. En las siguientes secciones, se proporcionan detalles acerca del uso de AWS Identity and Access Management (IAM) y Amazon Redshift para ayudar a proteger los recursos controlando quién puede obtener acceso a ellos:

- Autenticación con identidades
- Control de acceso

> **Important**
>
> Este tema contiene una colección de prácticas recomendadas para administrar los permisos, las identidades y el acceso seguro. Le recomendamos que se familiarice con las prácticas recomendadas para usar IAM con Amazon Redshift. Entre ellas se incluye el uso de roles de IAM para aplicar permisos. Conocer bien estas secciones le ayudará a mantener un almacenamiento de datos de Amazon Redshift más seguro.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS Single Sign-On Los usuarios (del Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso de AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren

que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad de tu Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Console cambiando de roles. Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para

federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS Single Sign-On.

- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Rol vinculado a servicio: un rol vinculado a servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su

nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Control de acceso

Aunque disponga de credenciales válidas para autenticar las solicitudes, si no tiene permisos, no podrá crear recursos de Amazon Redshift ni obtener acceso a ellos. Por ejemplo, debe tener permisos para crear un clúster de Amazon Redshift, crear una instantánea, agregar una suscripción a eventos, etc.

En las siguientes secciones, se describe cómo administrar los permisos de Amazon Redshift. Recomendamos que lea primero la información general.

- Información general sobre la administración de los permisos de acceso a los recursos de Amazon Redshift
- Uso de políticas basadas en identidad (políticas de IAM) para Amazon Redshift

Información general sobre la administración de los permisos de acceso a los recursos de Amazon Redshift

Cada recurso de AWS pertenece a una cuenta de AWS, y los permisos para crear u obtener acceso a los recursos se rigen por las políticas de permisos. Los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y roles). Algunos servicios (como AWS Lambda) también permiten asociar políticas de permisos a recursos.

> **Note**
>
> Un administrador de cuentas (o usuario administrador) es un usuario que tiene privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

Operaciones y recursos de Amazon Redshift

Amazon Redshift proporciona claves de contexto de condición, acciones y recursos específicos del servicio para su uso en las políticas de permisos de IAM.

Permisos de acceso a Amazon Redshift, Amazon Redshift sin servidor, API de datos de Amazon Redshift y editor de consultas de Amazon Redshift v2

Cuando configura Control de acceso, escribe políticas de permisos que puede adjuntar a una identidad de IAM (políticas basadas en identidad). Para obtener más información detallada de referencia, consulte los siguientes temas en la Referencia de autorizaciones de servicio:

- Para Amazon Redshift, consulte Acciones, recursos y claves de condiciones para Amazon Redshift que utilizan el prefijo `redshift:`.
- Para Amazon Redshift sin servidor, consulte Acciones, recursos y claves de condiciones para Amazon Redshift sin servidor que utilizan el prefijo `redshift-serverless:`.
- Para la API de datos de Amazon Redshift, consulte Acciones, recursos y claves de condiciones para la API de datos de Amazon Redshift que utilizan el prefijo `redshift-data:`.
- Para el editor de consultas de Amazon Redshift v2, consulte Acciones, recursos y claves de condición para AWS SQL Workbench (editor de consultas de Amazon Redshift v2) que utilizan el prefijo `sqlworkbench:`.

  El editor de consultas v2 incluye acciones de solo permiso que no se corresponden directamente con una operación de API. Estas acciones se indican en la Referencia de autorización de servicio con `[permission only]`.

Esta referencia de autorización del servicio contiene información sobre las operaciones de la API que se pueden utilizar en una política de IAM. También incluye el recurso de AWS para el que puede

conceder los permisos y las claves de condición que puede incluir para controlar el acceso con mayor precisión. Para obtener más información acerca de las condiciones, consulte Usar condiciones de las políticas de IAM para control de acceso preciso.

Las acciones se especifican en el campo `Action` de la política, el valor del recurso en el campo `Resource` de la política y las condiciones en el campo `Condition` de la política. Para especificar una acción para Amazon Redshift, use el prefijo `redshift:` seguido del nombre de operación de la API (por ejemplo, `redshift:CreateCluster`).

Titularidad de los recursos

El propietario del recurso es la cuenta de AWS que ha creado el recurso. Es decir, el propietario de los recursos es la cuenta de AWS de la entidad principal (cuenta raíz, usuario de IAM o rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza las credenciales de la cuenta raíz de su cuenta de AWS para crear un clúster de base de datos, su cuenta de AWS será la propietaria del recurso de Amazon Redshift.
- Si crea un rol de IAM en su cuenta de AWS con permisos para crear recursos de Amazon Redshift, cualquier persona que pueda asumir el rol podrá crear recursos de Amazon Redshift. La cuenta de AWS a la que pertenece el rol será la propietaria de los recursos de Amazon Redshift.
- Si crea un usuario de IAM en su cuenta de AWS y le concede permisos para crear recursos de Amazon Redshift, ese usuario también podrá crear recursos de Amazon Redshift. No obstante, su cuenta de AWS, a la que pertenece el usuario, será la propietaria de los recursos de Amazon Redshift. En la mayoría de los casos, no se recomienda este método. Recomendamos crear un rol de IAM y adjuntar permisos al rol y, después, asignarlo a un usuario.

Administrar el acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección, se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección, también se explica el uso de IAM en el contexto de Amazon Redshift. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte What is IAM? (¿Qué es IAM?) en la Guía del usuario de IAM.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas del IAM, consulte Referencia de políticas de AWS IAM en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. Amazon Redshift solo admite políticas basadas en identidad (políticas del IAM).

Políticas basadas en identidades (políticas de IAM)

Puede asignar permisos adjuntando políticas a una función de IAM y, a continuación, asignando esa función a un usuario o grupo. A continuación, se ofrece un ejemplo de una política que contiene permisos para crear, eliminar, modificar y reiniciar clústeres de Amazon Redshift para su cuenta de AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowManageClusters",
      "Effect":"Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource":"*"
    }
  ]
}
```

Para obtener más información acerca del uso de políticas basadas en identidades con Amazon Redshift, consulte Uso de políticas basadas en identidad (políticas de IAM) para Amazon Redshift. Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. Amazon Redshift no admite políticas basadas en recursos.

Especificación de elementos de política: acciones, efectos, recursos y entidades principales

En cada recurso de Amazon Redshift (consulte Operaciones y recursos de Amazon Redshift), el servicio define un conjunto de operaciones de la API (consulte Acciones). Para conceder permisos para estas operaciones de la API, Amazon Redshift define un conjunto de acciones que usted puede especificar en una política. Para realizar una operación API pueden ser necesarios permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte Operaciones y recursos de Amazon Redshift.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, el permiso `redshift:DescribeClusters` concede a los usuarios permiso para realizar la operación `DescribeClusters` de Amazon Redshift.
- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Amazon Redshift no admite políticas basadas en recursos.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas del IAM, consulte Referencia de políticas de AWS IAM en la Guía del usuario de IAM.

Para ver una tabla con todas las acciones de la API de Amazon Redshift y los recursos a los que se aplican, consulte Permisos de acceso a Amazon Redshift, Amazon Redshift sin servidor, API de datos de Amazon Redshift y editor de consultas de Amazon Redshift v2.

Especificar las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información acerca de cómo especificar condiciones en un lenguaje de la política de acceso, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Para identificar las condiciones en las que se aplica una política de permisos, incluya un elemento de `Condition` en su política de permisos de IAM. Por ejemplo, puede crear una política que le permita a un usuario crear un clúster mediante el uso de la acción `redshift:CreateCluster` y puede agregar un elemento de `Condition` para limitar al usuario a que lo haga solamente en una región específica. Para obtener más información, consulte Usar condiciones de las políticas de IAM para control de acceso preciso. Para ver una lista con todos los valores de clave de condición y las acciones y los recursos de Amazon Redshift a los que se aplican, consulte Permisos de acceso a Amazon Redshift, Amazon Redshift sin servidor, API de datos de Amazon Redshift y editor de consultas de Amazon Redshift v2.

Usar condiciones de las políticas de IAM para control de acceso preciso

En Amazon Redshift, puede usar claves de condición para restringir el acceso a los recursos en función de las etiquetas para tales recursos. A continuación, se muestran claves de condición de Amazon Redshift comunes.

Clave de condición	Descripción
`aws:RequestTag`	Requiere que los usuarios incluyan una clave de etiqueta (nombre) y un valor cada vez que crean un recurso. Para obtener más información, consulte aws:RequestTag en la Guía del usuario de IAM.
`aws:ResourceTag`	Restringe el acceso del usuario a los recursos, en función de claves de etiqueta y valores específicos. Para obtener más información, consulte aws:ResourceTag en la Guía del usuario de IAM.

Clave de condición	Descripción
`aws:TagKeys`	Utilice esta clave para comparar las claves de etiqueta de una solicitud con las claves que especifique en la política. Para obtener más informaci ón, consulte aws:TagKeys en la Guía del usuario de IAM.

Para obtener información acerca de etiquetas, consulte Información general del proceso de etiquetado.

Para obtener una lista de las acciones de API compatibles con las claves de condición `redshift:RequestTag` y `redshift:ResourceTag`, consulte Permisos de acceso a Amazon Redshift, Amazon Redshift sin servidor, API de datos de Amazon Redshift y editor de consultas de Amazon Redshift v2.

Las siguientes claves de condición se pueden usar con la acción GetClusterCredentials de Amazon Redshift.

Clave de condición	Descripción
`redshift: DurationS econds`	Limita el número de segundos que se puede especificar para la duración.
`redshift:DbName`	Restringe los nombres de base de datos que se pueden especificar.
`redshift:DbUser`	Restringe los nombres de usuarios de base de datos que se pueden especificar.

Ejemplo 1: restricción del acceso mediante el uso de la clave de condición aws:ResourceTag

Use la siguiente política de IAM para permitir que un usuario pueda modificar a un clúster de Amazon Redshift solo de una cuenta de AWS específica en la región `us-west-2` con una etiqueta denominada `environment` con el valor de etiqueta `test`.

```
{
    "Version": "2012-10-17",
    "Statement": {
```

```
        "Sid": "AllowModifyTestCluster",
        "Effect": "Allow",
        "Action": "redshift:ModifyCluster",
        "Resource": "arn:aws:redshift:us-west-2:123456789012:cluster:*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/environment": "test"
            }
        }
    }
}
```

Ejemplo 2: restricción del acceso mediante el uso de la clave de condición aws:RequestTag

Use la siguiente política de IAM para permitir que un usuario pueda crear un clúster de Amazon Redshift solo si el comando para crear el clúster contiene una etiqueta denominada `usage` y el valor de etiqueta `production`. La condición con `aws:TagKeys` y el modificador `ForAllValues` especifica que solo las claves `costcenter` y `usage` se pueden especificar en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "AllowCreateProductionCluster",
        "Effect": "Allow",
        "Action": [
            "redshift:CreateCluster",
            "redshift:CreateTags"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/usage": "production"
            },
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "costcenter",
                    "usage"
                ]
            }
        }
    }
}
```

Uso de políticas basadas en identidad (políticas de IAM) para Amazon Redshift

Este tema contiene ejemplos de políticas basadas en identidades, donde los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, a usuarios, grupos y funciones).

> **Important**
>
> Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de Amazon Redshift. Para obtener más información, consulte Información general sobre la administración de los permisos de acceso a los recursos de Amazon Redshift.

A continuación se muestra un ejemplo de una política de permisos. La política le permite a un usuario crear, eliminar, modificar y reiniciar todos los clústeres y, luego, le deniega permiso para eliminar o modificar todo clúster cuyo identificador comience con `production` en Región de AWS `us-west-2` y Cuenta de AWS `123456789012`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"DenyDeleteModifyProtected",
      "Action": [
        "redshift:DeleteCluster",
```

```
        "redshift:ModifyCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:production*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

La política tiene dos instrucciones:

- La primera instrucción concede permisos para que un usuario cree, elimine, modifique y reinicie clústeres. La instrucción especifica un carácter comodín (*) como el valor de `Resource`, por lo que la política se aplica a todos los recursos de Amazon Redshift que son propiedad de la cuenta raíz de AWS.
- La segunda instrucción deniega el permiso para eliminar o modificar un clúster. La instrucción especifica un Amazon Resource Name (ARN, Nombre de recurso de Amazon) de clúster para el valor de `Resource` que incluye un carácter comodín (*). Como resultado, la instrucción se aplica a todos los clústeres de Amazon Redshift que son propiedad de la cuenta raíz de AWS en la que el identificador del clúster comienza por `production`.

Políticas administradas por AWS para Amazon Redshift

AWS aborda muchos casos de uso comunes dando políticas de IAM independientes creadas y administradas por AWS. Las políticas administradas conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

También puede crear sus propias políticas de IAM personalizadas para permitir las operaciones y los recursos de la API de Amazon Redshift. Puede asociar estas políticas personalizadas a los roles o grupos de IAM que requieran esos permisos.

En las siguientes secciones, se describen políticas administradas por AWS, que se pueden adjuntar a los usuarios de la cuenta y son específicas de Amazon Redshift.

AmazonRedshiftReadOnlyAccess

Concede acceso de solo lectura a todos los recursos de Amazon Redshift a una cuenta de AWS.

Puede encontrar la política AmazonRedShiftReadOnlyAccess en la consola de IAM y AmazonRedshiftReadOnlyAccess en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftFullAccess

Concede acceso completo a todos los recursos de Amazon Redshift a una cuenta de AWS. Además, esta política concede acceso total a todos los recursos de Amazon Redshift Serverless.

Puede encontrar la política AmazonRedshiftFullAccess en la consola de IAM y AmazonRedshiftFullAccess en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftQueryEditor

Concede acceso completo al editor de consultas en la consola de Amazon Redshift.

Puede encontrar la política AmazonRedshiftQueryEditor en la consola de IAM y AmazonRedshiftQueryEditor en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftDataFullAccess

Concede acceso completo a todos los recursos y las operaciones de la API de datos de Amazon Redshift a una cuenta de AWS.

Puede encontrar la política AmazonRedshiftDataFullAccess en la consola de IAM y AmazonRedshiftDataFullAccess en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftQueryEditorV2FullAccess

Concede acceso completo a todos los recursos y las operaciones del editor de consultas v2 de Amazon Redshift. Esta política también concede acceso a otros servicios requeridos.

Puede encontrar la política AmazonRedshiftQueryEditorV2FullAccess en la consola de IAM y AmazonRedshiftQueryEditorV2FullAccess en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftQueryEditorV2NoSharing

Permite trabajar con el editor de consultas v2 de Amazon Redshift sin compartir recursos. Esta política también concede acceso a otros servicios requeridos. La entidad principal que utiliza esta

política no puede etiquetar sus recursos (como consultas) para compartirlos con otras entidades principales en la misma Cuenta de AWS.

Puede encontrar la política AmazonRedshiftQueryEditorV2NoSharing en la consola de IAM y AmazonRedshiftQueryEditorV2NoSharing en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftQueryEditorV2ReadSharing

Permite trabajar con el editor de consultas v2 de Amazon Redshift con uso compartido limitado de los recursos. Esta política también concede acceso a otros servicios requeridos. La entidad principal que utiliza esta política puede etiquetar sus recursos (como consultas) para compartirlos con otras entidades principales en la misma Cuenta de AWS. La entidad principal concedida puede leer los recursos compartidos con su equipo, pero no puede actualizarlos.

Puede encontrar la política AmazonRedshiftQueryEditorV2ReadSharing en la consola de IAM y AmazonRedshiftQueryEditorV2ReadSharing en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftQueryEditorV2ReadWriteSharing

Permite trabajar con el editor de consultas v2 de Amazon Redshift y compartir recursos. Esta política también concede acceso a otros servicios requeridos. La entidad principal que utiliza esta política puede etiquetar sus recursos (como consultas) para compartirlos con otras entidades principales en la misma Cuenta de AWS. La entidad principal concedida puede leer y actualizar los recursos compartidos con su equipo.

Puede encontrar la política AmazonRedshiftQueryEditorV2ReadWriteSharing en la consola de IAM y AmazonRedshiftQueryEditorV2ReadWriteSharing en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftServiceLinkedRolePolicy

No puede adjuntar AmazonRedshiftServiceLinkedRolePolicy a las entidades de IAM. Esta política se adjunta a un rol vinculado a servicio que permite a Amazon Redshift acceder a los recursos de la cuenta. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Redshift.

Puede encontrar la política AmazonRedshiftServiceLinkedRolePolicy en la consola de IAM y AmazonRedshiftServiceLinkedRolePolicy en la Guía de referencia de las políticas administradas por AWS.

AmazonRedshiftAllCommandsFullAccess

Permite utilizar el rol de IAM creado desde la consola de Amazon Redshift y configurarlo como predeterminado para que el clúster ejecute los comandos COPY desde Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION y CREATE MODEL. La política también concede permisos para ejecutar instrucciones SELECT para servicios relacionados, como Amazon S3, CloudWatch Logs, Amazon SageMaker o AWS Glue.

Puede encontrar la política AmazonRedshiftAllCommandsFullAccess en la consola de IAM y AmazonRedshiftAllCommandsFullAccess en la Guía de referencia de las políticas administradas por AWS.

También puede crear sus propias políticas de IAM personalizadas para permitir las operaciones y los recursos de la API de Amazon Redshift. Puede asociar estas políticas personalizadas a los roles o grupos de IAM que requieran esos permisos.

Actualizaciones de Amazon Redshift en las políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Amazon Redshift debido a que este servicio comenzó a realizar un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Amazon Redshift.

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2FullAccess: actualización de una política actual	Se agregó permiso para las acciones `redshift-serverless:ListNamespaces` y `redshift-serverless:ListWorkgroups` a la política administrada. Al agregarlo, se concede permiso para enumerar los espacios de nombres sin servidor y grupos de trabajo sin servidor en el	21 de febrero de 2024

Cambio	Descripción	Fecha
	almacenamiento de datos de Amazon Redshift.	
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Se agregó permiso para las acciones `redshift-serverless:ListNamespaces` y `redshift-serverless:ListWorkgroups` a la política administrada. Al agregarlo, se concede permiso para enumerar los espacios de nombres sin servidor y grupos de trabajo sin servidor en el almacenamiento de datos de Amazon Redshift.	21 de febrero de 2024
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Se agregó permiso para las acciones `redshift-serverless:ListNamespaces` y `redshift-serverless:ListWorkgroups` a la política administrada. Al agregarlo, se concede permiso para enumerar los espacios de nombres sin servidor y grupos de trabajo sin servidor en el almacenamiento de datos de Amazon Redshift.	21 de febrero de 2024

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Se agregó permiso para las acciones `redshift-serverless:ListNamespaces` y `redshift-serverless:ListWorkgroups` a la política administrada. Al agregarlo, se concede permiso para enumerar los espacios de nombres sin servidor y grupos de trabajo sin servidor en el almacenamiento de datos de Amazon Redshift.	21 de febrero de 2024
AmazonRedshiftReadOnlyAccess: actualización de una política actual	Se agregó permiso para la acción `redshift:ListRecommendations` a la política administrada. Esto concede permiso para publicar las recomendaciones de Amazon Redshift Advisor.	7 de febrero de 2024
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Se agregó permiso para las acciones `ec2:AssignIpv6Addresses` y `ec2:UnassignIpv6Addresses` a la política administrada. Al agregarlas, se otorga permiso para asignar y desasignar direcciones IP.	31 de octubre de 2023

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Se agregó permiso para las acciones `sqlworkbench:GetAutocompletionMetadata` y `sqlworkbench:GetAutocompletionResource` a la política administrada. Al agregarlo, se concede permiso para generar y recuperar información de la base de datos para completar automáticamente SQL mientras se editan las consultas.	16 de agosto de 2023
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Se agregó permiso para las acciones `sqlworkbench:GetAutocompletionMetadata` y `sqlworkbench:GetAutocompletionResource` a la política administrada. Al agregarlos, se adjudica permiso para generar y recuperar información de la base de datos para completar automáticamente SQL mientras se editan las consultas.	16 de agosto de 2023

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Se agregó permiso para las acciones `sqlworkbench:GetAutocompletionMetadata` y `sqlworkbench:GetAutocompletionResource` a la política administrada. Al agregarlos, se adjudica permiso para generar y recuperar información de la base de datos para completar automáticamente SQL mientras se editan las consultas.	16 de agosto de 2023

Cambio	Descripción	Fecha
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Los permisos para las acciones en AWS Secrets Manager para crear y administrar secretos se agregan a la política administrada. Los permisos añadidos son los siguientes: • `secretsmanager:GetRandomPassword` • `secretsmanager:DescribeSecret` • `secretsmanager:PutSecretValue` • `secretsmanager:UpdateSecret` • `secretsmanager:UpdateSecretVersionStage` • `secretsmanager:RotateSecret` • `secretsmanager:DeleteSecret`	14 de agosto de 2023

Cambio	Descripción	Fecha
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Los permisos para las acciones de Amazon EC2 para crear y administrar grupos de seguridad y reglas de enrutamiento se eliminan de la política administrada. Estos permisos se referían a la creación de subredes y VPC. Los permisos eliminados son los siguientes: • `ec2:AuthorizeSecurityGroupEgress` • `ec2:AuthorizeSecurityGroupIngress` • `ec2:UpdateSecurityGroupRuleDescriptionsEgress` • `ec2:ReplaceRouteTableAssociation` • `ec2:CreateRouteTable` • `ec2:AttachInternetGateway` • `ec2:UpdateSecurityGroupRuleDescriptionsIngress` • `ec2:AssociateRouteTable` • `ec2:RevokeSecurityGroupIngress` • `ec2:CreateRoute`	8 de mayo de 2023

Cambio	Descripción	Fecha
	• `ec2:CreateSecurityGroup` • `ec2:RevokeSecurityGroupEgress` • `ec2:ModifyVpcAttribute` • `ec2:CreateSubnet` • `ec2:CreateInternetGateway` • `ec2:CreateVpc` Estaban asociados con la etiqueta de recurso Purpose:RedshiftMigrateToVpc. La etiqueta limitaba el alcance de los permisos para tareas de migración de Amazon EC2 Classic a VPC de Amazon EC2. Para obtener más información sobre las etiquetas de recursos, consulte Control del acceso a los recursos de AWS mediante etiquetas.	

Cambio	Descripción	Fecha
AmazonRedshiftDataFullAccess: actualización de una política actual	Se agregó permiso para la acción `redshift:GetClusterCredentialsWithIAM` a la política administrada. Al agregarlo, concede permiso para obtener credenciales temporales mejoradas para acceder a una base de datos de Amazon Redshift a través de la Cuenta de AWS especificada.	7 de abril de 2023
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Los permisos para las acciones de Amazon EC2 para la creación y la administración de reglas de grupos de seguridad se agregan a la política administrada. Estos grupos y reglas de seguridad están asociados específicamente a la etiqueta de recursos `aws:RequestTag/Redshift` de Amazon Redshift. Esto limita el alcance de los permisos a recursos de Amazon Redshift específicos.	6 de abril de 2023

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:GetSchemaInference` a la política administrada. Al agregarlo, concede permiso para obtener las columnas y los tipos de datos deducidos a partir de un archivo.	21 de marzo de 2023
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:GetSchemaInference` a la política administrada. Al agregarlo, concede permiso para obtener las columnas y los tipos de datos deducidos a partir de un archivo.	21 de marzo de 2023
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:GetSchemaInference` a la política administrada. Al agregarlo, concede permiso para obtener las columnas y los tipos de datos deducidos a partir de un archivo.	21 de marzo de 2023

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:AssociateNotebookWithTab` a la política administrada. Al agregarlo, se adjudica permiso para crear y actualizar pestañas enlazadas al bloc de notas del usuario.	2 de febrero de 2023
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:AssociateNotebookWithTab` a la política administrada. Al agregarlo, se adjudica permiso para crear y actualizar pestañas enlazadas al bloc de notas del usuario o a un bloc de notas que se comparta con él.	2 de febrero de 2023
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:AssociateNotebookWithTab` a la política administrada. Al agregarlo, se adjudica permiso para crear y actualizar pestañas enlazadas al bloc de notas del usuario o a un bloc de notas que se comparta con él.	2 de febrero de 2023

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	A fin de conceder permiso para utilizar cuadernos, Amazon Redshift agregó permiso para las siguientes acciones: • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent`	17 de octubre de 2022

Cambio	Descripción	Fecha
	• sqlworkbench:UpdateNotebookCellLayout • sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench:DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook	

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	A fin de conceder permiso para utilizar cuadernos, Amazon Redshift agregó permiso para las siguientes acciones: • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent`	17 de octubre de 2022

Cambio	Descripción	Fecha
	• sqlworkbench:UpdateNotebookCellLayout • sqlworkbench:BatchGetNotebookCell • sqlworkbench:ListNotebookVersions • sqlworkbench:CreateNotebookVersion • sqlworkbench:GetNotebookVersion • sqlworkbench:DeleteNotebookVersion • sqlworkbench:RestoreNotebookVersion • sqlworkbench:ExportNotebook	

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	A fin de conceder permiso para utilizar cuadernos, Amazon Redshift agregó permiso para las siguientes acciones: • `sqlworkbench:ListNotebooks` • `sqlworkbench:CreateNotebook` • `sqlworkbench:DuplicateNotebook` • `sqlworkbench:CreateNotebookFromVersion` • `sqlworkbench:ImportNotebook` • `sqlworkbench:GetNotebook` • `sqlworkbench:UpdateNotebook` • `sqlworkbench:DeleteNotebook` • `sqlworkbench:CreateNotebookCell` • `sqlworkbench:DeleteNotebookCell` • `sqlworkbench:UpdateNotebookCellContent`	17 de octubre de 2022

Cambio	Descripción	Fecha
	• `sqlworkbench:UpdateNotebookCellLayout` • `sqlworkbench:BatchGetNotebookCell` • `sqlworkbench:ListNotebookVersions` • `sqlworkbench:CreateNotebookVersion` • `sqlworkbench:GetNotebookVersion` • `sqlworkbench:DeleteNotebookVersion` • `sqlworkbench:RestoreNotebookVersion` • `sqlworkbench:ExportNotebook`	
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Amazon Redshift agregó el espacio de nombres `AWS/Redshift` para permitir la publicación de métricas en CloudWatch.	7 de septiembre de 2022
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Permiso de Amazon Redshift agregado a las acciones `sqlworkbench:ListQueryExecutionHistory` y `sqlworkbench:GetQueryExecutionHistory`. Esto otorga permiso para ver el historial de consultas.	30 de agosto de 2022

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Permiso de Amazon Redshift agregado a las acciones `sqlworkbench:ListQueryExecutionHistory` y `sqlworkbench:GetQueryExecutionHistory`. Esto otorga permiso para ver el historial de consultas.	30 de agosto de 2022
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Permiso de Amazon Redshift agregado a las acciones `sqlworkbench:ListQueryExecutionHistory` y `sqlworkbench:GetQueryExecutionHistory`. Esto otorga permiso para ver el historial de consultas.	30 de agosto de 2022
AmazonRedshiftFullAccess: actualización de una política actual	Los permisos para Amazon Redshift Serverless se agregan a la política administrada AmazonRedshiftFullAccess existente.	22 de julio de 2022

Cambio	Descripción	Fecha
AmazonRedshiftDataFullAccess: actualización de una política actual	Amazon Redshift actualizó la condición de alcance predeterminada `redshift-serverless:GetCredentials` del permiso de etiqueta `aws:ResourceTag/RedshiftDataFullAccess` de `StringEquals` a `StringLike` para conceder acceso a recursos etiquetados con la clave de etiqueta `RedshiftDataFullAccess` y cualquier valor de etiqueta.	11 de julio de 2022
AmazonRedshiftDataFullAccess: actualización de una política actual	Amazon Redshift agregó permisos nuevos para permitir a `redshift-serverless:GetCredentials` obtener credenciales temporales de Amazon Redshift Serverless.	8 de julio de 2022
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Permiso de Amazon Redshift agregado a la acción `sqlworkbench:GetAccountSettings`. Otorga permiso para obtener una configuración de cuenta.	15 de junio de 2022

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Permiso de Amazon Redshift agregado a la acción `sqlworkbench:GetAccountSettings` . Otorga permiso para obtener una configuración de cuenta.	15 de junio de 2022
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Permiso de Amazon Redshift agregado a la acción `sqlworkbench:GetAccountSettings` . Otorga permiso para obtener una configuración de cuenta.	15 de junio de 2022
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Para habilitar el acceso público a los nuevos puntos de conexión de Amazon Redshift Serverless, Amazon Redshift asigna y asocia direcciones IP elásticas a la interfaz de red elástica del punto de conexión de la VPC en la cuenta del cliente. Esto lo hace mediante los permisos proporcionados a través del rol vinculado al servicio. Para habilitar este caso de uso, se agregan acciones para asignar y liberar una dirección IP elástica al rol vinculado al servicio de Amazon Redshift Serverless.	26 de mayo de 2022

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2FullAccess: actualización de una política actual	Permisos para la acción `sqlworkbench:ListTaggedResources` . Se dirige específicamente a los recursos del editor de consultas v2 de Amazon Redshift. Esta actualización de la política proporciona derecho a llamar a `tag:GetResources` solo a través del editor de consultas v2.	22 de febrero de 2022
AmazonRedshiftQueryEditorV2NoSharing: actualización de una política actual	Permisos para la acción `sqlworkbench:ListTaggedResources` . Se dirige específicamente a los recursos del editor de consultas v2 de Amazon Redshift. Esta actualización de la política proporciona derecho a llamar a `tag:GetResources` solo a través del editor de consultas v2.	22 de febrero de 2022
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Permisos para la acción `sqlworkbench:ListTaggedResources` . Se dirige específicamente a los recursos del editor de consultas v2 de Amazon Redshift. Esta actualización de la política proporciona derecho a llamar a `tag:GetResources` solo a través del editor de consultas v2.	22 de febrero de 2022

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2ReadWriteSharing: actualización de una política actual	Permisos para la acción `sqlworkbench:ListTaggedResources` . Se dirige específicamente a los recursos del editor de consultas v2 de Amazon Redshift. Esta actualización de la política proporciona derecho a llamar a `tag:GetResources` solo a través del editor de consultas v2.	22 de febrero de 2022
AmazonRedshiftQueryEditorV2ReadSharing: actualización de una política actual	Se agregó permiso para la acción `sqlworkbench:AssociateQueryWithTab` a la política administrada. Agregarlo permite que los clientes puedan crear pestañas del editor vinculadas a una consulta que se comparta con ellos.	22 de febrero de 2022
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Amazon Redshift agregó permisos para nuevas acciones para permitir la administración de los recursos de red y VPC de Amazon Redshift.	22 de noviembre de 2021

Cambio	Descripción	Fecha
AmazonRedshiftAllCommandsFullAccess: política nueva	Amazon Redshift agregó una nueva política para permitir el uso del rol de IAM creado desde la consola de Amazon Redshift y configurarlo como predeterminado para que el clúster ejecute los comandos COPY desde Amazon S3, UNLOAD, CREATE EXTERNAL SCHEMA, CREATE EXTERNAL FUNCTION, CREATE MODEL o CREATE LIBRARY.	18 de noviembre de 2021
AmazonRedshiftServiceLinkedRolePolicy: actualización de una política actual	Amazon Redshift agregó permisos para nuevas acciones para permitir la administración de grupos de registros de CloudWatch y flujos de registros de Amazon Redshift, incluida la exportación de registros de auditoría.	15 de noviembre de 2021
AmazonRedshiftFullAccess: actualización de una política actual	Amazon Redshift agregó nuevos permisos para permitir la explicabilidad del modelo, DynamoDB, Redshift Spectrum y federación de Amazon RDS.	07 de octubre de 2021
AmazonRedshiftQueryEditorV2FullAccess: política nueva	Amazon Redshift agregó una nueva política para permitir el acceso completo al editor de consultas v2 de Amazon Redshift.	24 de septiembre de 2021

Cambio	Descripción	Fecha
AmazonRedshiftQueryEditorV2NoSharing: política nueva	Amazon Redshift agregó una nueva política para permitir el uso del editor de consultas v2 de Amazon Redshift sin compartir recursos.	24 de septiembre de 2021
AmazonRedshiftQueryEditorV2ReadSharing: política nueva	Amazon Redshift agregó una nueva política para permitir el uso compartido de lectura dentro del editor de consultas v2 de Amazon Redshift.	24 de septiembre de 2021
AmazonRedshiftQueryEditorV2ReadWriteSharing: política nueva	Amazon Redshift agregó una nueva política para permitir el uso compartido de lectura y actualización dentro del editor de consultas v2 de Amazon Redshift.	24 de septiembre de 2021
AmazonRedshiftFullAccess: actualización de una política actual	Amazon Redshift agregó permisos nuevos para permitir `sagemaker:*Job*` .	18 de agosto de 2021
AmazonRedshiftDataFullAccess: actualización de una política actual	Amazon Redshift agregó permisos nuevos para permitir `AuthorizeDataShare` .	12 de agosto de 2021
AmazonRedshiftDataFullAccess: actualización de una política actual	Amazon Redshift agregó permisos nuevos para permitir `BatchExecuteStatement` .	27 de julio de 2021
Amazon Redshift comenzó a realizar un seguimiento de los cambios	Amazon Redshift comenzó a realizar un seguimiento de los cambios de las políticas administradas por AWS.	27 de julio de 2021

Permisos necesarios para usar Redshift Spectrum

Amazon Redshift Spectrum requiere permisos para que otros servicios de AWS tengan acceso a los recursos. Para obtener más información acerca de los permisos en las políticas de IAM para Redshift Spectrum, consulte Políticas de IAM para Amazon Redshift Spectrum en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Permisos necesarios para usar la consola de Amazon Redshift

Para que un usuario pueda trabajar con la consola de Amazon Redshift, ese usuario debe tener un conjunto mínimo de permisos que le permitan describir los recursos de Amazon Redshift para su cuenta de AWS. Estos permisos también deben permitir al usuario describir otra información relacionada, incluida información de red, Amazon CloudWatch, Amazon SNS, y seguridad de Amazon EC2.

Si crea una política de IAM que sea más restrictiva que el mínimo de permisos necesarios, la consola no funciona del modo esperado para los usuarios con esa política de IAM. Para asegurarse de que esos usuarios puedan seguir usando la consola de Amazon Redshift, adjunte también la política administrada `AmazonRedshiftReadOnlyAccess` al usuario. En Políticas administradas por AWS para Amazon Redshift, se muestra cómo hacer esto.

Para obtener información acerca de cómo conceder a un usuario acceso al editor de consultas en la consola de Amazon Redshift, consulte Permisos necesarios para usar el editor de consultas de la consola de Amazon Redshift.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de Amazon Redshift.

Permisos necesarios para usar el editor de consultas de la consola de Amazon Redshift

Para que un usuario pueda trabajar con el editor de consultas de Amazon Redshift, ese usuario debe tener un conjunto mínimo de permisos para las operaciones de la API de datos de Amazon Redshift y Amazon Redshift. Para conectarse a una base de datos con un secreto, también debe tener permisos de Secrets Manager.

Para conceder a un usuario acceso al editor de consultas en la consola de Amazon Redshift, adjunte las políticas `AmazonRedshiftQueryEditor` y `AmazonRedshiftReadOnlyAccess` administradas por AWS. La política `AmazonRedshiftQueryEditor` otorga al usuario permiso para recuperar solo

los resultados de sus propias instrucciones SQL. Es decir, las instrucciones enviadas por el mismo `aws:userid`, como se muestra en esta sección de la política `AmazonRedshiftQueryEditor` administrada por AWS.

```
{
    "Sid": "DataAPIIAMSessionPermissionsRestriction",
    "Action": [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "redshift-data:statement-owner-iam-userid": "${aws:userid}"
        }
    }
}
```

Para permitir que un usuario recupere los resultados de las instrucciones SQL de otras personas en el mismo rol de IAM, cree su propia política sin la condición de limitar el acceso al usuario actual. Limite también el acceso para cambiar una política a un administrador.

Permisos necesarios para usar del editor de consultas v2

Para que un usuario pueda trabajar con el editor de consultas v2 de Amazon Redshift, debe tener un conjunto mínimo de permisos para las operaciones del editor de consultas v2 de Amazon Redshift y otros servicios de AWS, tales como AWS Key Management Service, AWS Secrets Manager y servicio de etiquetado.

Para conceder a un usuario acceso completo al editor de consultas v2, adjunte la política `AmazonRedshiftQueryEditorV2FullAccess` administrada por AWS. La política `AmazonRedshiftQueryEditorV2FullAccess` permite al usuario compartir recursos del editor de consultas v2, como consultas con otros miembros del mismo equipo. Para obtener más información sobre cómo se controla el acceso a los recursos del editor de consultas v2, consulte la definición de la política administrada específica para el editor de consultas v2 en la consola de IAM.

Algunas políticas administradas por AWS del Editor de consultas de Amazon Redshift v2 usan etiquetas de AWS en las condiciones para delimitar el acceso a los recursos. En el editor

de consultas v2, el uso compartido de consultas se basa en la clave de etiqueta y el valor `"aws:ResourceTag/sqlworkbench-team": "${aws:PrincipalTag/sqlworkbench-team}"` en la política de IAM adjuntada a la entidad principal (el rol de IAM). Las entidades principales en la misma Cuenta de AWS con el mismo valor de etiqueta (por ejemplo, `accounting-team`), están en el mismo equipo en el editor de consultas v2. Solo se puede asociar a un equipo a la vez. Un usuario con permisos administrativos puede configurar equipos en la consola de IAM dando a todos los miembros del equipo el mismo valor para la etiqueta `sqlworkbench-team`. Si el valor de etiqueta de `sqlworkbench-team` se cambia para un usuario de IAM o un rol de IAM, puede haber un retraso hasta que el cambio se refleje en los recursos compartidos. Si se cambia el valor de etiqueta de un recurso (como una consulta), de nuevo podría haber un retraso hasta que se refleje el cambio. Los miembros del equipo también deben tener el permiso `tag:GetResources` para compartir recursos.

Ejemplo: Para agregar la etiqueta **`accounting-team`** de un rol de IAM

1. Inicie sesión en AWS Management Console y abra la consola IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola, elija Roles (Roles) y, a continuación, elija el nombre de la entidad que desea editar.
3. Elija la pestaña Tags (Etiquetas) y, a continuación, elija Add Tags (Agregar etiquetas).
4. Agregar la clave de etiqueta sqlworkbench-team y el valor `accounting-team`.
5. Elija Save changes (Guardar cambios).

   Ahora, cuando una entidad principal de IAM (con este rol de IAM adjunto) comparte una consulta con el equipo, otras entidades principales con el mismo valor de etiqueta `accounting-team` puede ver la consulta.

Para obtener más información sobre cómo adjuntar una etiqueta a una entidad principal, incluidos los roles de IAM y los usuarios de IAM, consulte Etiquetado de recursos de IAM en la Guía del usuario de IAM.

También puede configurar equipos en el nivel de la sesión mediante un proveedor de identidad (IdP). Esto permite que varios usuarios que utilizan el mismo rol de IAM tengan un equipo diferente. La política de confianza del rol de IAM debe permitir la operación `sts:TagSession`. Para obtener más información, consulte Permisos necesarios para agregar etiquetas de sesión en la Guía del usuario de IAM. Agregue el atributo de etiqueta de la entidad principal a la aserción SAML proporcionada por su IdP.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-
team">
    <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

Siga las instrucciones de su proveedor de identidad (IdP) para rellenar el atributo SAML con el contenido procedente de su directorio. Para obtener más información sobre los proveedores de identidad (IdP) y Amazon Redshift, consulte Uso de la autenticación de IAM para generar credenciales de usuario de base de datos y Proveedores de identidad y federación en la Guía del usuario de IAM.

`sqlworkbench:CreateNotebookVersion` concede permiso para obtener el contenido actual de las celdas de cuaderno y crear una versión de cuaderno en su cuenta. Es decir, en el momento de la creación de la versión, el contenido actual del cuaderno es el mismo que el de la versión. Más adelante, el contenido de las celdas de la versión se mantiene mientras se actualiza el cuaderno actual. `sqlworkbench:GetNotebookVersion` concede permiso para obtener una versión del cuaderno. Un usuario que no tiene el permiso `sqlworkbench:BatchGetNotebookCell` pero tiene los permisos `sqlworkbench:CreateNotebookVersion` y `sqlworkbench:GetNotebookVersion` en un cuaderno tiene acceso a las celdas del cuaderno en la versión. Este usuario sin el permiso `sqlworkbench:BatchGetNotebookCell` sigue pudiendo recuperar el contenido de las celdas de un cuaderno mediante la creación primero de una versión y, a continuación, con la obtención de esta versión creada.

Permisos necesarios para usar el programador de Amazon Redshift

Cuando utiliza el programador de Amazon Redshift, configura un rol de IAM con una relación de confianza con el programador de Amazon Redshift (**`scheduler.redshift.amazonaws.com`**) para permitir que programador asuma los permisos en su nombre. También adjunta una política (permisos) al rol para las operaciones de la API de Amazon Redshift que quiere programar.

En el siguiente ejemplo, se muestra el documento de la política en formato JSON para establecer una relación de confianza entre el programador de Amazon Redshift y Amazon Redshift.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": [
                    "scheduler.redshift.amazonaws.com",
                    "redshift.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Para obtener más información acerca de las entidades de confianza, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.

También debe agregar permisos para las operaciones de Amazon Redshift que desee programar.

Para que el programador utilice la operación `ResizeCluster`, agregue un permiso similar al siguiente a su política de IAM. En función de su entorno, es posible que quiera crear una política más restrictiva.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:ResizeCluster",
            "Resource": "*"
        }
    ]
}
```

Para consultar los pasos necesarios para crear un rol para el programador de Amazon Redshift, consulte Creación de un rol para un servicio de AWS (consola) en la Guía del usuario de IAM. Realice estas elecciones cuando cree un rol en la consola de IAM:

- En Choose the service that will use this role (Elegir el servicio que utilizará este rol): elija Redshift.
- En Select your use case (Seleccione su caso de uso): seleccione Redshift - Scheduler (Redshift - Programador).
- Cree una política o adjúntela al rol que permita programar una operación de Amazon Redshift. Seleccione Create policy (Crear política) o modifique el rol para agregar una política. Introduzca la política JSON para la operación que se va a programar.

- Después de crear el rol, edite la Trust relationship (Relación de confianza) del rol de IAM para incluir el servicio `redshift.amazonaws.com`.

El rol IAM que cree tiene entidades de confianza de `scheduler.redshift.amazonaws.com` y `redshift.amazonaws.com`. También tiene una política adjunta que permite una acción de la API de Amazon Redshift compatible; por ejemplo, `"redshift:ResizeCluster"`.

Permisos necesarios para usar el programador de Amazon EventBridge

Cuando utiliza el programador de Amazon EventBridge, configura un rol de IAM con una relación de confianza con el programador de EventBridge (**`events.amazonaws.com`**) para permitir que el programador asuma los permisos en su nombre. También adjunta una política (permisos) al rol para las operaciones de la API de datos de Amazon Redshift que quiere programar y una política para las operaciones de Amazon EventBridge.

Utilice el programador de EventBridge cuando cree consultas programadas con el editor de consultas de Amazon Redshift en la consola.

Puede crear un rol de IAM para ejecutar consultas programadas en la consola de IAM. En este rol de IAM, adjunte `AmazonEventBridgeFullAccess` y `AmazonRedshiftDataFullAccess`.

En el siguiente ejemplo, se muestra el documento de la política en formato JSON para establecer una relación de confianza con el programador de EventBridge.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Para obtener más información acerca de las entidades de confianza, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.

Para consultar los pasos necesarios para crear un rol para el programador de EventBridge, consulte Creación de un rol para un servicio de AWS (consola) en la Guía del usuario de IAM. Realice estas elecciones cuando cree un rol en la consola de IAM:

- En Choose the service that will use this role (Seleccionar el servicio que utilizará este rol), elija CloudWatch Events.
- En Select your use case (Seleccione su caso de uso), elija CloudWatch Events.
- Adjunte las siguientes políticas de permisos: `AmazonEventBridgeFullAccess` y `AmazonRedshiftDataFullAccess`.

El rol de IAM que crea tiene una entidad de confianza de `events.amazonaws.com`. También tiene una política adjunta que permite acciones de la API de datos de Amazon Redshift compatibles; por ejemplo, `"redshift-data:*"`.

Permisos necesarios para usar machine learning (ML) de Amazon Redshift

A continuación, puede encontrar una descripción de los permisos necesarios para usar el machine learning (ML) de Amazon Redshift para diferentes casos de uso.

Para que los usuarios utilicen Amazon Redshift ML con Amazon SageMaker, cree un rol de IAM con una política más restrictiva que la predeterminada. Puede utilizar la siguiente política. Asimismo, puede modificarla para que se adapte a sus necesidades.

La siguiente política muestra los permisos necesarios para ejecutar SageMaker Autopilot con la explicabilidad del modelo de Amazon Redshift.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:CreateCompilationJob",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeAutoMLJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:DescribeCompilationJob",
                "sagemaker:DescribeProcessingJob",
```

```
                "sagemaker:DescribeTransformJob",
                "sagemaker:ListCandidatesForAutoMLJob",
                "sagemaker:StopAutoMLJob",
                "sagemaker:StopCompilationJob",
                "sagemaker:StopTrainingJob",
                "sagemaker:DescribeEndpoint",
                "sagemaker:InvokeEndpoint",
                "sagemaker:StopProcessingJob",
                "sagemaker:CreateModel",
                "sagemaker:CreateProcessingJob"
            ],
            "Resource": [
                "arn:aws:sagemaker:*:*:model/*redshift*",
                "arn:aws:sagemaker:*:*:training-job/*redshift*",
                "arn:aws:sagemaker:*:*:automl-job/*redshift*",
                "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
                "arn:aws:sagemaker:*:*:processing-job/*redshift*",
                "arn:aws:sagemaker:*:*:transform-job/*redshift*",
                "arn:aws:sagemaker:*:*:endpoint/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "cloudwatch:namespace": [
                        "SageMaker",
                        "/aws/sagemaker/Endpoints",
                        "/aws/sagemaker/ProcessingJobs",
                        "/aws/sagemaker/TrainingJobs",
                        "/aws/sagemaker/TransformJobs"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetAuthorizationToken",
                "ecr:GetDownloadUrlForLayer"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "s3:ExistingObjectTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "redshift.amazonaws.com",
                        "sagemaker.amazonaws.com"
                    ]
                }
            }
        }
    ]
```

```
}
```

La siguiente política muestra los permisos mínimos completos para permitir el acceso a la federación de Amazon DynamoDB, Redshift Spectrum y Amazon RDS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateAutoMLJob",
                "sagemaker:CreateCompilationJob",
                "sagemaker:CreateEndpoint",
                "sagemaker:DescribeAutoMLJob",
                "sagemaker:DescribeTrainingJob",
                "sagemaker:DescribeCompilationJob",
                "sagemaker:DescribeProcessingJob",
                "sagemaker:DescribeTransformJob",
                "sagemaker:ListCandidatesForAutoMLJob",
                "sagemaker:StopAutoMLJob",
                "sagemaker:StopCompilationJob",
                "sagemaker:StopTrainingJob",
                "sagemaker:DescribeEndpoint",
                "sagemaker:InvokeEndpoint",
                "sagemaker:StopProcessingJob",
                "sagemaker:CreateModel",
                "sagemaker:CreateProcessingJob"
            ],
            "Resource": [
                "arn:aws:sagemaker:*:*:model/*redshift*",
                "arn:aws:sagemaker:*:*:training-job/*redshift*",
                "arn:aws:sagemaker:*:*:automl-job/*redshift*",
                "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
                "arn:aws:sagemaker:*:*:processing-job/*redshift*",
                "arn:aws:sagemaker:*:*:transform-job/*redshift*",
                "arn:aws:sagemaker:*:*:endpoint/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
                "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "SageMaker",
                        "/aws/sagemaker/Endpoints",
                        "/aws/sagemaker/ProcessingJobs",
                        "/aws/sagemaker/TrainingJobs",
                        "/aws/sagemaker/TransformJobs"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetAuthorizationToken",
                "ecr:GetDownloadUrlForLayer"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {
```

```
                "s3:ExistingObjectTag/Redshift": "true"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "dynamodb:Scan",
            "dynamodb:DescribeTable",
            "dynamodb:Getitem"
        ],
        "Resource": [
            "arn:aws:dynamodb:*:*:table/*redshift*",
            "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticmapreduce:ListInstances"
        ],
        "Resource": [
            "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "elasticmapreduce:ListInstances"
        ],
        "Resource": "*",
        "Condition": {
            "StringEqualsIgnoreCase": {
                "elasticmapreduce:ResourceTag/Redshift": "true"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": "arn:aws:lambda:*:*:function:*redshift*"
    },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:*:*:table/*redshift*/*",
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:*redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "secretsmanager:GetRandomPassword",
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "secretsmanager:ResourceTag/Redshift": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "redshift.amazonaws.com",
                        "glue.amazonaws.com",
                        "sagemaker.amazonaws.com",
                        "athena.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

De forma opcional, para utilizar una clave AWS KMS de cifrado, agregue los siguientes permisos a la política.

```
{
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": [
```

```
        "arn:aws:kms:<your-region>:<your-account-id>:key/<your-kms-key>"
    ]
}
```

Para permitir que Amazon Redshift y SageMaker asuman el rol de IAM anterior para interactuar con otros servicios, agregue la siguiente política de confianza al rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.amazonaws.com",
          "sagemaker.amazonaws.com",
          "forecast.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El bucket `redshift-downloads/redshift-ml/` de Amazon S3 anterior es el lugar donde se almacenan los datos de muestra utilizados en otros pasos y ejemplos. Puede quitar este bucket si no necesita cargar datos de Amazon S3. O bien, puede reemplazarlo con otros buckets de Amazon S3 que utilice para cargar datos en Amazon Redshift.

Los valores **`your-account-id`**, **`your-role`** y **`your-s3-bucket`** son el ID de cuenta, el rol y el bucket que especifique en el comando CREATE MODEL.

De forma opcional, puede utilizar la sección de claves AWS KMS de la política de muestra si especifica una clave AWS KMS para utilizarla con Amazon Redshift ML. El valor **`your-kms-key`** es la clave que se utiliza como parte del comando CREATE MODEL.

Si especifica una nube virtual privada (VPC) para el trabajo de ajuste de hiperparámetros, agregue los siguientes permisos.

```
{
            "Effect": "Allow",
```

```
            "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteNetworkInterfacePermission",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeVpcs",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
            ]
}
```

Para trabajar con la explicación del modelo, asegúrese de tener los permisos para llamar a las operaciones de la API de SageMaker. Recomendamos utilizar la política administrada `AmazonSageMakerFullAccess`. Si desea crear un rol de IAM que tenga una política más restrictiva, utilice la siguiente política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker::CreateEndpoint",
        "sagemaker::CreateEndpointConfig",
        "sagemaker::DeleteEndpoint",
        "sagemaker::DeleteEndpointConfig",
        "sagemaker::DescribeEndpoint",
        "sagemaker::DescribeEndpointConfig",
        "sagemaker::DescribeModel",
        "sagemaker::InvokeEndpoint",
        "sagemaker::ListTags"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obtener más información sobre la política administrada `AmazonSageMakerFullAccess`, consulte AmazonSageMakerFullAccess en la Guía para desarrolladores de Amazon SageMaker.

Si desea crear modelos de previsión, le recomendamos que utilice la política administrada `AmazonForecastFullAccess`. Si desea usar una política más restrictiva, utilice la siguiente política en el rol de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "forecast:CreateAutoPredictor",
                "forecast:CreateDataset",
                "forecast:CreateDatasetGroup",
                "forecast:CreateDatasetImportJob",
                "forecast:CreateForecast",
                "forecast:CreateForecastExportJob",
                "forecast:DeleteResourceTree",
                "forecast:DescribeAutoPredictor",
                "forecast:DescribeDataset",
                "forecast:DescribeDatasetGroup",
                "forecast:DescribeDatasetImportJob",
                "forecast:DescribeForecast",
                "forecast:DescribeForecastExportJob",
                "forecast:StopResource",
                "forecast:TagResource",
                "forecast:UpdateDatasetGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca de Amazon Redshift ML, consulte Uso de machine learning en Amazon Redshift o CREATE MODEL.

Permisos para la ingesta de streaming

La ingesta de streaming funciona con dos servicios. Se trata de Kinesis Data Streams y Amazon MSK.

Se requieren permisos para usar la ingesta de streaming con Kinesis Data Streams

Encontrará un procedimiento con un ejemplo de política administrada en Introducción a la ingesta de streaming desde Amazon Kinesis Data Streams.

Se requieren permisos para usar la ingesta de streaming con Amazon MSK

Encontrará un procedimiento con un ejemplo de política administrada en Introducción a la ingesta de streaming desde Amazon Managed Streaming para Apache Kafka.

Permisos necesarios para utilizar las operaciones de la API de uso compartido de datos

Para controlar el acceso a las operaciones de la API de uso compartido de datos, utilice políticas basadas en acciones de IAM. Para obtener información sobre cómo administrar las políticas de IAM, consulte Administración de las políticas de IAM en la Guía del usuario de IAM.

En particular, supongamos que el administrador de un clúster productor necesita usar la llamada a `AuthorizeDataShare` para autorizar la salida de un recurso compartido de datos desde una Cuenta de AWS. En este caso, debe configurar una política de IAM basada en acciones para otorgar ese permiso. Use la llamada `DeauthorizeDataShare` para revocar la salida.

Cuando se usan políticas de IAM basadas en acciones, también se puede especificar un recurso de IAM en la política; por ejemplo, `DataShareARN`. A continuación, se muestra el formato y un ejemplo de `DataShareARN`.

```
arn:aws:redshift:region:account-id:datashare:namespace-guid/datashare-name
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
SalesShare
```

Puede restringir el acceso `AuthorizeDataShare` a un datashare específico indicando el nombre del datashare en la política de IAM.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
```

```
      ],
      "Effect": "Deny"
    }
  ]
}
```

También puede restringir la política de IAM a todos los datashares que pertenezcan a un clúster productor específico. Para ello, reemplace el valor **`datashare-name`** en la política con un comodín o un asterisco. Mantenga el valor `namespace-guid` del clúster.

```
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
*
```

A continuación, se presenta la política de IAM que impide que una entidad llame a `AuthorizeDataShare` en los recursos compartidos de datos que sean propiedad de un clúster productor específico.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

`DataShareARN` restringe el acceso en función del nombre del recurso compartido de datos y el ID único global (GUID) del espacio de nombres del clúster propietario. Lo hace especificando el nombre como un asterisco.

Políticas de recursos de GetClusterCredentials

Para conectarse a la base de datos de un clúster mediante una conexión JDBC u ODBC con credenciales de base de datos de IAM o para llamar mediante programación a la acción

`GetClusterCredentials`, necesita, un conjunto mínimo de permisos. Como mínimo, necesita permiso para llamar a la acción `redshift:GetClusterCredentials` con acceso a un recurso `dbuser`.

Si usa una conexión JDBC o ODBC en lugar de `server` y `port`, puede especificar `cluster_id` y `region`, pero para ello la política debe permitir la acción `redshift:DescribeClusters` con acceso al recurso `cluster`.

Si llama a la acción `GetClusterCredentials` con los parámetros opcionales `Autocreate`, `DbGroups` y `DbName`, asegúrese de permitir también las acciones y el acceso a los recursos indicados en la tabla siguiente.

Parámetro GetClusterCredentials	Acción	Recurso
`Autocreate`	`redshift:CreateClusterUser`	`dbuser`
`DbGroups`	`redshift:JoinGroup`	`dbgroup`
`DbName`	N/D	`dbname`

Para obtener más información acerca de recursos, consulte Operaciones y recursos de Amazon Redshift.

También puede incluir las siguientes condiciones en la política:

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

Para obtener más información acerca de las condiciones, consulte Especificar las condiciones de una política.

Ejemplos de políticas administradas por el cliente

En esta sección, encontrará ejemplos de políticas de usuario que conceden permisos para diversas acciones de Amazon Redshift. Estas políticas funcionan cuando se utiliza la API de Amazon Redshift, los AWS SDK o la AWS CLI.

> **Note**
>
> Todos los ejemplos utilizan la región Oeste de EE. UU. (Oregón) (`us-west-2`) y contienen identificadores de cuenta ficticios.

Ejemplo 1: Permitir al usuario obtener acceso completo a todos los recursos y las acciones de Amazon Redshift

La siguiente política permite obtener acceso a todas las acciones de Amazon Redshift en todos los recursos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowRedshift",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

El valor `redshift:*` del elemento `Action` indica todas las acciones de Amazon Redshift.

Ejemplo 2: Denegar a un usuario el acceso a un conjunto de acciones de Amazon Redshift

De manera predeterminada, se deniegan todos los permisos. No obstante, en ocasiones se necesita denegar explícitamente el acceso a una acción o un conjunto de acciones específicas. La siguiente política permite obtener acceso a todas las acciones de Amazon Redshift y deniega explícitamente el acceso a toda acción de Amazon Redshift cuyo nombre empiece por `Delete`. Esta política se aplica a todos los recursos de Amazon Redshift de la región `us-west-2`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowUSWest2Region",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:redshift:us-west-2:*"
    },
   {
     "Sid":"DenyDeleteUSWest2Region",
     "Action": [
        "redshift:Delete*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:redshift:us-west-2:*"
   }
  ]
}
```

Ejemplo 3: Permitirle a un usuario administrar clústeres

La siguiente política le permite a un usuario crear, eliminar, modificar y reiniciar todos los clústeres y, luego, le deniega permiso para eliminar o modificar todo clúster cuyo nombre comience con `protected`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift:DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
```

```
    },
    {
      "Sid":"DenyDeleteProtected",
      "Action": [
        "redshift:DeleteCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:protected*"
      ],
      "Effect": "Deny"
    }
  ]
}
```

Ejemplo 4: Permitirle a un usuario que autorice y revoque la obtención de acceso a instantáneas

La siguiente política le permite a un usuario, por ejemplo el usuario A, hacer lo siguiente:

- Autorizar la obtención de acceso a toda snapshot creada a partir de un clúster denominado `shared`.
- Revocar la obtención de acceso a snapshots para toda snapshot creada a partir del clúster `shared` en el que el nombre de la snapshot comience con `revokable`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowSharedSnapshots",
      "Action": [
        "redshift:AuthorizeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:shared/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"AllowRevokableSnapshot",
      "Action": [
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [
```

```
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/revokable*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Si el usuario A le ha otorgado al usuario B acceso a la snapshot, el usuario B debe tener una política como la siguiente que le permita restaurar un clúster a partir de la snapshot. La siguiente política le permite al usuario B describir y restaurar a partir de snapshots, y crear clústeres. El nombre de estos clústeres debe comenzar con `from-other-account`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowDescribeSnapshots",
      "Action": [
        "redshift:DescribeClusterSnapshots"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"AllowUserRestoreFromSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/*",
        "arn:aws:redshift:us-west-2:444455556666:cluster:from-other-account*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Ejemplo 5: Permitirle a un usuario copiar una instantánea de un clúster y restaurar un clúster a partir de una instantánea

La siguiente política le permite a un usuario copiar cualquier snapshot creada a partir del clúster denominado `big-cluster-1` y restaurar cualquier snapshot cuando el nombre de ella comience con `snapshot-for-restore`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowCopyClusterSnapshot",
      "Action": [
        "redshift:CopyClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:big-cluster-1/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid":"AllowRestoreFromClusterSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/snapshot-for-restore*",
        "arn:aws:redshift:us-west-2:123456789012:cluster:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Ejemplo 6: Permitir a un usuario obtener acceso a Amazon Redshift y a recursos y acciones comunes de servicios de AWS relacionados

La siguiente política de ejemplo permite acceder a todas las acciones y los recursos de Amazon Redshift, Amazon Simple Notification Service (Amazon SNS) y Amazon CloudWatch. También permite acciones especificadas en todos los recursos de Amazon EC2 relacionados en la cuenta.

> **Note**
>
> Para las acciones de Amazon EC2 que se especifican en esta política de ejemplo, no se admiten los permisos en el nivel del recurso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":"AllowRedshift",
      "Effect": "Allow",
      "Action": [
        "redshift:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid":"AllowSNS",
      "Effect": "Allow",
        "Action": [
          "sns:*"
        ],
        "Resource": [
          "*"
        ]
      },
    {
      "Sid":"AllowCloudWatch",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid":"AllowEC2Actions",
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Ejemplo 7: Permitir a un usuario etiquetar recursos con la consola de Amazon Redshift

La siguiente política de ejemplo permite a un usuario etiquetar recursos con la consola de Amazon Redshift mediante la AWS Resource Groups. Esta política puede adjuntarse a un rol de usuario que invoca la consola de Amazon Redshift nueva u original. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos en Amazon Redshift.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Tagging permissions",
            "Effect": "Allow",
            "Action": [
                "redshift:DeleteTags",
                "redshift:CreateTags",
                "redshift:DescribeTags",
                "tag:UntagResources",
                "tag:TagResources"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Política de ejemplo para usar GetClusterCredentials

La política siguiente utiliza estos valores de parámetros de ejemplo:

- Región: `us-west-2`
- Cuenta de AWS: `123456789012`
- Nombre del clúster: `examplecluster`

La política siguiente habilita las acciones `GetCredentials`, `CreateClusterUser` y `JoinGroup`. La política usa claves de condición para permitir las acciones `GetClusterCredentials` y `CreateClusterUser` solo cuando el ID de usuario de AWS concuerde con `"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"`. El acceso de IAM solo se solicita para la base de datos `"testdb"`. La política también permite a los usuarios unirse a un grupo denominado `"common_group"`.

```
{
"Version": "2012-10-17",
  "Statement": [
    {
     "Sid": "GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}",
        "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ],
        "Condition": {
           "StringEquals": {
           "aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
           }
        }
    },
    {
      "Sid": "CreateClusterUserStatement",
      "Effect": "Allow",
```

```
      "Action": [
        "redshift:CreateClusterUser"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid":"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
    {
      "Sid": "RedshiftJoinGroupStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:JoinGroup"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ]
    }
  ]
}
```

Federación de proveedores de identidades (IdP) nativos para Amazon Redshift

La administración de identidades y permisos para Amazon Redshift se facilita con la federación de proveedores de identidades nativos porque aprovecha el proveedor de identidades existente para simplificar la autenticación y la administración de permisos. Para ello, posibilita compartir con Redshift metadatos de identidad del proveedor de identidades. Para la primera iteración de esta característica, el proveedor de identidades admitido es Microsoft Azure Active Directory (Azure AD).

Para configurar Amazon Redshift de modo que pueda autenticar identidades del proveedor de identidades de terceros, debe registrar el proveedor de identidades en Amazon Redshift. De este modo, Redshift puede autenticar usuarios y roles definidos por el proveedor de identidades. Por lo tanto, puede evitar tener que llevar a cabo una administración de identidades detallada tanto en su proveedor de identidades de terceros como en Amazon Redshift porque se comparte información de identidades.

Para obtener información sobre el uso de los roles de sesión que se transfieren desde grupos de proveedores de identidades (IdP), consulte PG_GET_SESSION_ROLES en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Configuración del proveedor de identidades en Amazon Redshift

En esta sección se muestran los pasos para configurar el proveedor de identidades y Amazon Redshift para establecer la comunicación para la federación de proveedores de identidades nativos. Necesita una cuenta activa del proveedor de identidades. Antes de configurar Amazon Redshift, registre Redshift como aplicación en el proveedor de identidades, concediendo permiso como administrador.

Complete los siguientes pasos en Amazon Redshift:

1. Ejecute una instrucción SQL para registrar el proveedor de identidades, incluidas las descripciones de los metadatos de la aplicación de Azure. Para crear el proveedor de identidades en Amazon Redshift, ejecute el siguiente comando después de sustituir los valores de los parámetros issuer, client_id, client_secret y audience. Estos parámetros son específicos de Microsoft Azure AD. Sustituya el nombre del proveedor de identidades por el nombre de su elección y sustituya el espacio de nombres por un nombre exclusivo para contener usuarios y roles del directorio del proveedor de identidades.

   ```
   CREATE IDENTITY PROVIDER oauth_standard TYPE azure
   NAMESPACE 'aad'
   PARAMETERS '{
   "issuer":"https://sts.windows.net/2sdfdsf-d475-420d-b5ac-667adad7c702/",
   "client_id":"<client_id>",
   "client_secret":"BUAH~ewrqewrqwerUUY^%tHe1oNZShoiU7",
   "audience":["https://analysis.windows.net/powerbi/connector/AmazonRedshift"]
   }'
   ```

   El tipo `azure` indica que el proveedor facilita específicamente la comunicación con Microsoft Azure AD. En la actualidad, es el único proveedor de identidades de terceros admitido.

   - issuer: el ID de emisor en el que confiar cuando se recibe un token. El identificador único para tenant_id se adjunta al emisor.
   - client_id: el identificador público único de la aplicación registrado en el proveedor de identidades. Esto se puede denominar ID de aplicación.

- client_secret: un identificador secreto o contraseña, que solo conocen el proveedor de identidades y la aplicación registrada.
- audience: el ID de aplicación que se asigna a la aplicación en Azure.

En lugar de utilizar un secreto de cliente compartido, puede establecer parámetros para especificar un certificado, una clave privada y una contraseña de clave privada al crear el proveedor de identidades.

```
CREATE IDENTITY PROVIDER example_idp TYPE azure
NAMESPACE 'example_aad'
PARAMETERS '{"issuer":"https://sts.windows.net/2sdfdsf-d475-420d-
b5ac-667adad7c702/",
"client_id":"<client_id>",
"audience":["https://analysis.windows.net/powerbi/connector/AmazonRedshift"],
"client_x5t":"<certificate thumbprint>",
"client_pk_base64":"<private key in base64 encoding>",
"client_pk_password":"test_password"}';
```

La contraseña de la clave privada, client_pk_password, es opcional.

2. Opcional: ejecute comandos SQL en Amazon Redshift para crear previamente usuarios y roles. Esto facilita la concesión de permisos por adelantado. El nombre del rol en Amazon Redshift es como el siguiente: <Espacio de nombres>:<GroupName en Azure AD>. Por ejemplo, cuando crea un grupo en Microsoft Azure AD llamado `rsgroup` y un espacio de nombres llamado `aad`, el nombre del rol es `aad:rsgroup`. Los nombres de usuario y rol en Amazon Redshift se definen a partir de estos nombres de usuario y pertenencias a grupos en el espacio de nombres del proveedor de identidades.

   La asignación de roles y usuarios incluye la verificación de su valor `external_id`, para garantizar que esté actualizado. El ID externo se asigna al identificador del grupo o usuario en el proveedor de identidades. Por ejemplo, el ID externo de un rol se asigna al ID de grupo de Azure AD correspondiente. Del mismo modo, el ID externo de cada usuario se asigna a su ID en el proveedor de identidades.

   ```
   create role "aad:rsgroup";
   ```

3. Otorgue los permisos pertinentes a los roles según los requisitos. Por ejemplo:

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. También puede conceder permisos a un usuario específico.

```
GRANT SELECT on table foo to aad:alice@example.com
```

Tenga en cuenta que la pertenencia al rol de un usuario externo federado solo está disponible en la sesión de ese usuario. Esto tiene implicaciones en la creación de objetos de base de datos. Cuando un usuario externo federado crea una vista o un procedimiento almacenado, por ejemplo, no puede delegar el permiso de esos objetos a otros usuarios y roles.

Una explicación de los espacios de nombres

Un espacio de nombres asigna un usuario o rol a un proveedor de identidades específico. Por ejemplo, el prefijo para los usuarios creados en AWS IAM es `iam:`. Este prefijo evita las colisiones de nombres de usuario y posibilita la compatibilidad con varios almacenes de identidades. Si un usuario alice@ejemplo.com del origen de identidad registrado con el espacio de nombres aad inicia sesión, el usuario `aad:alice@example.com` se crea en Redshift si no existe todavía. Tenga en cuenta que un espacio de nombres de rol y usuario tiene una función distinta a la de un espacio de nombres de clúster de Amazon Redshift, que es un identificador único asociado a un clúster.

Cómo funciona el inicio de sesión con la federación de proveedores de identidades (IdP) nativos

Para completar la configuración preliminar entre el proveedor de identidades y Amazon Redshift, realice un par de pasos: en primer lugar, registre Amazon Redshift como aplicación de terceros en su proveedor de identidades, solicitando los permisos de API necesarios. A continuación, cree usuarios y grupos en el proveedor de identidades. Por último, registre el proveedor de identidades en Amazon Redshift mediante instrucciones SQL, que establecen parámetros de autenticación exclusivos del proveedor de identidades. Como parte del registro del proveedor de identidades en Redshift, se asigna un espacio de nombres para asegurarse de que los usuarios y los roles se agrupan correctamente.

Con el proveedor de identidades registrado en Amazon Redshift, se configura la comunicación entre Redshift y el proveedor de identidades. A continuación, un cliente puede pasar tokens y autenticarse en Redshift como entidad de proveedor de identidades. Amazon Redshift utiliza la información de pertenencia a grupos de IdP para la asignación a roles de Redshift. Si el usuario no existe

anteriormente en Redshift, se crea uno. Se crean roles que se asignan a grupos de proveedores de identidades, si no existen. El administrador de Amazon Redshift concede permiso sobre los roles y los usuarios pueden ejecutar consultas y realizar otras tareas de base de datos.

En los siguientes pasos se describe cómo funciona la federación de proveedores de identidades nativos cuando un usuario inicia sesión:

1. Cuando un usuario inicia sesión utilizando la opción de IdP nativo, desde el cliente, el token del proveedor de identidades se envía desde el cliente al controlador.
2. El usuario está autenticado. Si el usuario no existe todavía en Amazon Redshift, se crea uno nuevo. Redshift asigna los grupos de proveedores de identidades del usuario a roles de Redshift.
3. Los permisos se asignan según los roles de Redshift del usuario. Los concede a los usuarios y roles un administrador.
4. El usuario puede consultar a Redshift.

Uso de las herramientas de cliente de escritorio para conectarse a Amazon Redshift

Para obtener instrucciones sobre cómo utilizar la federación de proveedores de identidades nativos para conectarse a Amazon Redshift con Power BI, consulte la publicación del blog Integrate Amazon Redshift native IdP federation with Microsoft Azure Active Directory (AD) and Power BI (Integrar la federación de IdP nativos de Amazon Redshift con Microsoft Azure Active Directory [AD] y Power BI). Describe una implementación paso a paso de la configuración de IdP nativo de Amazon Redshift con Azure AD. Detalla los pasos para configurar la conexión de cliente para el escritorio de Power BI o para el servicio de Power BI. Los pasos incluyen el registro de aplicaciones, la configuración de permisos y la configuración de credenciales.

Para obtener información sobre cómo integrar la federación de IdP nativo de Amazon Redshift con Azure AD, mediante Power BI Desktop y JDBC Client-SQL Workbench/J, vea el siguiente vídeo:

Para obtener instrucciones sobre cómo utilizar la federación de proveedores de identidades nativos para conectarse a Amazon Redshift con un cliente SQL, específicamente DBeaver o SQL Workbench/J, consulte la publicación del blog Integrate Amazon Redshift native IdP federation with Microsoft Azure AD using a SQL client (Integrar la federación de IdP nativos de Amazon Redshift con Microsoft Azure AD mediante un cliente SQL).

Conexión de Redshift con IAM Identity Center para ofrecer a los usuarios una experiencia de inicio de sesión único

Puede administrar el acceso de usuarios y grupos a los almacenamientos de datos de Amazon Redshift mediante la propagación de identidades de confianza. Esto funciona mediante una conexión entre Redshift y AWS IAM Identity Center, que ofrece a los usuarios una experiencia de inicio de sesión único. De este modo puede incorporar usuarios y grupos de su directorio y asignarles permisos directamente. Posteriormente, esta conexión permite vincular herramientas y servicios adicionales. Para ilustrar un caso integral, puede utilizar un panel de Amazon QuickSight o el editor de consultas v2 de Amazon Redshift para acceder a Redshift. En este caso, el acceso se basa en grupos del IAM Identity Center. Redshift puede determinar quién es un usuario y a qué grupos pertenece. IAM Identity Center también permite conectar y administrar identidades mediante un proveedor de identidades (IdP) externo como Okta o PingOne.

Una vez que el administrador haya configurado la conexión entre Redshift y el IAM Identity Center, podrá configurar un acceso detallado en función de los grupos de proveedores de identidad para autorizar el acceso de los usuarios a los datos.

Las ventajas de la integración de Redshift con AWS IAM Identity Center

Usar el IAM Identity Center con Redshift puede beneficiar a su organización de las siguientes maneras:

- Los autores de los paneles en Amazon QuickSight pueden conectarse a los orígenes de datos de Redshift sin tener que volver a introducir las contraseñas ni requerir que un administrador configure roles de IAM con permisos complejos.
- El IAM Identity Center proporciona una ubicación central para sus usuarios en AWS. Puede crear usuarios y grupos directamente en el IAM Identity Center o conectar los usuarios y grupos existentes que administra en un proveedor de identidades basado en estándares, como Okta, PingOne o Microsoft Entra ID (Azure AD). El IAM Identity Center dirige la autenticación hacia el origen de confianza elegido para los usuarios y grupos, y mantiene un directorio de usuarios y grupos al que puede acceder Redshift. Para obtener más información, consulte Administre su fuente de identidad y los Proveedores de identidades compatibles en la Guía del usuario del AWS IAM Identity Center.
- Puede compartir una instancia del IAM Identity Center con varios clústeres y grupos de trabajo de Redshift con una sencilla función de conexión y detección automática. Esto agiliza la adición de clústeres sin el esfuerzo adicional que supone configurar la conexión del IAM Identity Center

para cada uno de ellos, y garantiza que todos los clústeres y grupos de trabajo tengan una visión coherente de los usuarios, sus atributos y grupos. Tenga en cuenta que la instancia del IAM Identity Center de su organización debe estar en la misma región que cualquier recurso compartido de datos de Redshift al que se conecte.

- Como las identidades de los usuarios son conocidas y se registran junto con el acceso a los datos, le resulta más fácil cumplir con las normas de conformidad auditando el acceso de los usuarios en AWS CloudTrail.

Configuración de la integración del IAM Identity Center con Amazon Redshift

El administrador del clúster de Amazon Redshift o el administrador de Amazon Redshift sin servidor debe realizar varios pasos para configurar Redshift como una aplicación habilitada para el IAM Identity Center. Esto permite que Redshift pueda detectar y conectarse automáticamente al IAM Identity Center para recibir los servicios de inicio de sesión y directorio de usuarios. Después, cuando el administrador de Redshift cree un clúster o grupo de trabajo, podrá habilitar el nuevo almacenamiento de datos para que utilice IAM Identity Center para administrar el acceso a la base de datos.

El objetivo de habilitar Redshift como una aplicación administrada por IAM Identity Center es poder controlar los permisos de usuarios y grupos desde el IAM Identity Center o desde un proveedor de identidades externo que esté integrado en él. Cuando los usuarios de la base de datos inician sesión en una base de datos de Redshift, por ejemplo, un analista o un científico de datos, comprueba sus grupos en el IAM Identity Center y si coinciden con los nombres de los roles en Redshift. De esta manera, un grupo que defina el nombre de un rol de base de datos de Redshift podrá acceder a un conjunto de tablas para el análisis de ventas, por ejemplo. En las secciones siguientes se muestra cómo configurarlo.

Requisitos previos

Estos son los requisitos previos para integrar IAM Identity Center con Amazon Redshift:

- Configuración de la cuenta: debe configurar el IAM Identity Center en la cuenta de administración de su organización de AWS si tiene previsto tener casos prácticos de varias cuentas o si usa clústeres de Redshift en cuentas diferentes con la misma instancia de IAM Identity Center. Esto incluye la configuración del origen de la identidad. Para obtener más información, consulte Introducción, Identidades del personal y Proveedores de identidades compatibles en la Guía del usuario del AWS IAM Identity Center. Debe asegurarse de haber creado usuarios o grupos en el

IAM Identity Center o de haber sincronizado los usuarios y grupos de su origen de identidad antes de poder asignarlos a los datos en Redshift.

> **Note**
>
> Tiene la opción de utilizar una instancia de cuenta de IAM Identity Center, siempre que Redshift e IAM Identity Center estén en la misma cuenta. Puede crear esta instancia mediante un widget al crear y configurar un clúster o grupo de trabajo de Redshift.

- Configuración de un emisor de tokens de confianza: en algunos casos, es posible que necesite utilizar un emisor de tokens de confianza, que es una entidad que puede emitir y verificar los tokens de confianza. Antes de hacerlo, deben realizarse unos pasos preliminares antes de que el administrador de Redshift que configure la integración del IAM Identity Center pueda seleccionar el emisor de tokens de confianza y añadir los atributos necesarios para completar la configuración. Esto puede incluir configurar un proveedor de identidades externo para que actúe como emisor de tokens de confianza y añadir sus atributos en la consola del IAM Identity Center. Para completar estos pasos, consulte Setting up a trusted token issuer.

  > **Note**
  >
  > No es necesario configurar un emisor de tokens de confianza para todas las conexiones externas. La conexión a la base de datos de Redshift con el editor de consultas v2 de Amazon Redshift no requiere la configuración de un emisor de tokens de confianza. Sin embargo, puede aplicarse a aplicaciones de terceros, como paneles o aplicaciones personalizadas que se autentican con el proveedor de identidades.

- Configuración de uno o varios roles de IAM: en las secciones siguientes se mencionan los permisos que se deben configurar. Deberá añadir permisos según las prácticas recomendadas de IAM. Los permisos específicos se detallan en los procedimientos siguientes.

Para obtener más información, consulte Getting Started with IAM Identity Center.

Configuración del proveedor de identidades para trabajar con el IAM Identity Center

El primer paso para controlar la administración de identidades de usuarios y grupos consiste en conectarse al IAM Identity Center y configurar el proveedor de identidades. Puede utilizar el propio IAM Identity Center como su proveedor de identidades o puede conectarse a un almacén de identidades de terceros, como Okta. Para obtener más información sobre cómo configurar la

conexión y el proveedor de identidades, consulte Proveedor de identidades externo en la Guía del usuario del IAM Identity Center. Al final de este proceso, asegúrese de añadir un pequeño grupo de usuarios y grupos al IAM Identity Center para realizar pruebas.

Permisos administrativos

Permisos necesarios para la administración del ciclo de vida de las aplicaciones de Redshift/IAM Identity Center

Debe crear una identidad de IAM que un administrador de Redshift utilice para configurar Redshift para usarlo con IAM Identity Center. Lo más habitual es crear un rol de IAM con permisos y asignarlo a otras identidades según sea necesario. Debe tener los permisos indicados para realizar las siguientes acciones.

Creación de la aplicación de Redshift/IAM Identity Center

- `sso:PutApplicationAssignmentConfiguration`: se utiliza para la seguridad.
- `sso:CreateApplication` – Se utiliza para crear una aplicación de IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod`: otorga acceso de autenticación de Redshift.
- `sso:PutApplicationGrant` – Se utiliza para cambiar la información del emisor de tokens de confianza.
- `sso:PutApplicationAccessScope`: se utiliza para configurar la aplicación Redshift IAM Identity Center. Esto incluye para AWS Lake Formation y para permisos de acceso de Amazon S3.
- `redshift:CreateRedshiftIdcApplication`: se utiliza para crear la aplicación Redshift IDC.

Descripción de la aplicación de Redshift/IAM Identity Center

- `sso:GetApplicationGrant` – Se utiliza para enumerar la información del emisor de tokens de confianza.
- `sso:ListApplicationAccessScopes`: para que en la configuración de la aplicación de Redshift IAM Identity Center se enumeren las integraciones posteriores, como las de AWS Lake Formation y los permisos de acceso de S3.
- `redshift:DescribeRedshiftIdcApplications`: se utiliza para describir las aplicaciones existentes de IAM Identity Center.

Cambio de la aplicación de Redshift/IAM Identity Center

- `redshift:ModifyRedshiftIdcApplication`: se utiliza para cambiar una aplicación Redshift existente.
- `sso:UpdateApplication`: se utiliza para actualizar una aplicación IAM Identity Center.
- `sso:GetApplicationGrant`: obtiene la información del emisor de tokens de confianza.
- `sso:ListApplicationAccessScopes`: se utiliza para configurar la aplicación Redshift IAM Identity Center.
- `sso:DeleteApplicationGrant` – Elimina la información del emisor de tokens de confianza.
- `sso:PutApplicationGrant` – Se utiliza para cambiar la información del emisor de tokens de confianza.
- `sso:PutApplicationAccessScope`: se utiliza para configurar la aplicación Redshift IAM Identity Center. Esto incluye para AWS Lake Formation y para permisos de acceso de Amazon S3.
- `sso:DeleteApplicationAccessScope`: para eliminar la configuración de la aplicación de Redshift IAM Identity Center. Esto incluye para AWS Lake Formation y para permisos de acceso de Amazon S3.

Eliminación de la aplicación de Redshift/IAM Identity Center

- `sso:DeleteApplication`: se utiliza para eliminar una aplicación IAM Identity Center.
- `redshift:DeleteRedshiftIdcApplication`: ofrece la posibilidad de eliminar una aplicación Redshift IDC existente.

Permisos necesarios para la administración del ciclo de vida de las aplicaciones de Redshift/editor de consultas v2

Debe crear una identidad de IAM que un administrador de Redshift utilice para configurar Redshift para usarlo con IAM Identity Center. Lo más habitual es crear un rol de IAM con permisos y asignarlo a otras identidades según sea necesario. Debe tener los permisos indicados para realizar las siguientes acciones.

Creación de la aplicación del editor de consultas v2

- `redshift:CreateQev2IdcApplication`: se utiliza para crear la aplicación de QEV2.
- `sso:CreateApplication`: da la capacidad de crear una aplicación de IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod`: otorga acceso de autenticación de Redshift.

- `sso:PutApplicationGrant` – Se utiliza para cambiar la información del emisor de tokens de confianza.
- `sso:PutApplicationAccessScope`: se utiliza para configurar la aplicación Redshift IAM Identity Center. Esto incluye el editor de consultas v2.
- `sso:PutApplicationAssignmentConfiguration`: se utiliza para la seguridad.

Descripción de la aplicación del editor de consultas v2

- `redshift:DescribeQev2IdcApplications`: se utiliza para describir la aplicación de QEV2 de IAM Identity Center.

Cambio de la aplicación del editor de consultas v2

- `redshift:ModifyQev2IdcApplication`: se utiliza para cambiar la aplicación de QEV2 de IAM Identity Center.
- `sso:UpdateApplication`: se utiliza para cambiar la aplicación de QEV2 de IAM Identity Center.

Eliminación de la aplicación del editor de consultas v2

- `redshift:DeleteQev2IdcApplication`: se utiliza para eliminar la aplicación de QEV2.
- `sso:DeleteApplication`: se utiliza para eliminar la aplicación de QEV2.

> **Note**
>
> En el SDK de Amazon Redshift, las siguientes API no están disponibles:
>
> - CreateQev2IdcApplication
> - DescribeQev2IdcApplications
> - ModifyQev2IdcApplication
> - DeleteQev2IdcApplication
>
> Estas acciones se utilizan específicamente para realizar la integración de IAM Identity Center con Redshift QEV2 en la consola de AWS. Para obtener más información, consulte Acciones definidas por Amazon Redshift.

Permisos necesarios para que el administrador de base de datos conecte nuevos recursos en la consola

Estos permisos son necesarios para conectar nuevos clústeres aprovisionados o grupos de trabajo de Amazon Redshift sin servidor durante el proceso de creación. Si tiene estos permisos, aparece una selección en la consola para elegir conectarse a la aplicación administrada por IAM Identity Center para Redshift.

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Configuración de Redshift como una aplicación administrada por AWS con IAM Identity Center

Para que IAM Identity Center pueda administrar las identidades de un clúster aprovisionado de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor, el administrador de Redshift debe completar los pasos para que Redshift sea una aplicación administrada por IAM Identity Center:

1. Seleccione Integración de IAM Identity Center en el menú de la consola de Amazon Redshift o Amazon Redshift sin servidor y, a continuación, Conectarse a IAM Identity Center. A partir de ahí, debe realizar una serie de selecciones para rellenar las propiedades para la integración de IAM Identity Center.
2. Elija un nombre para mostrar y un nombre exclusivo para la aplicación gestionada por IDC de Redshift.
3. Especifique el espacio de nombres de su organización. En general suele ser una versión abreviada del nombre de la organización y se añade como prefijo a los usuarios y roles administrados por IDC en la base de datos de Redshift.
4. Seleccione el rol de IAM que desee utilizar. Este rol de IAM debe estar separado de los roles que se utilizan para Redshift. Además, recomendamos que no se utilice para otros fines. Los permisos de política específicos necesarios son los siguientes:

- `sso:DescribeApplication`: se requiere para crear una entrada de proveedor de identidades (IdP) en el catálogo.
- `sso:DescribeInstance`: se utiliza para crear manualmente roles o usuarios federados de IdP.

5. Configure las conexiones de los clientes y los emisores de tokens de confianza. La configuración de emisores de tokens de confianza facilita la propagación de identidades de confianza al definir una relación con un proveedor de identidades externo. La propagación de identidades permite a un usuario, por ejemplo, iniciar sesión en una aplicación y acceder a datos específicos en otra aplicación. Esto permite a los usuarios recopilar datos de ubicaciones distintas de forma más fluida. En este paso, debe establecer los atributos para cada emisor de tokens de confianza en la consola. Los atributos incluyen el nombre y la notificación de audiencia (o aud claim), que puede que tenga que obtener de los atributos de configuración de la herramienta o el servicio. Es posible que también tenga que proporcionar el nombre de la aplicación que aparece en el JSON Web Token (JWT) de la herramienta de terceros.

   > **Note**
   >
   > La `aud claim` requerida para cada herramienta o servicio de terceros puede variar en función del tipo de token, que puede ser un token de acceso emitido por un proveedor de identidades, o de otro tipo, como un token de ID. Cada proveedor puede ser diferente. Al implementar la propagación de identidades de confianza y la integración con Redshift, se debe proporcionar el valor aud correcto para el tipo de token que la herramienta de terceros envía a AWS. Consulte las recomendaciones de su proveedor de herramientas o servicios.

   Para obtener información detallada sobre la propagación de identidades de confianza, consulte How trusted identity propagation works. Consulte también la documentación beta del IAM Identity Center que se adjunta a esta documentación.

Cuando el administrador de Redshift finalice los pasos y guarde la configuración, las propiedades del IAM Identity Center aparecerán en la consola de Redshift. También puede consultar la vista del sistema SVV_IDENTITY_PROVIDERS para comprobar las propiedades de la aplicación que incluyen el nombre de la aplicación y el espacio de nombres. El espacio de nombres se utiliza como prefijo para los objetos de base de datos de Redshift que están asociados a la aplicación. Al realizar estas

tareas, Redshift se convierte en una aplicación habilitada por IAM Identity Center. Las propiedades de la consola incluyen el estado de la integración. Cuando se completa la integración, muestra Habilitado. Tras este proceso, se puede habilitar la integración del IAM Identity Center en cada clúster nuevo.

Tras la configuración, puede incluir usuarios y grupos del IAM Identity Center en Redshift seleccionando la pestaña Usuarios o Grupos y Asignar.

Habilitación de la integración de IAM Identity Center para un nuevo clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor

El administrador de la base de datos configura los nuevos recursos de Redshift para que funcionen junto con el IAM Identity Center y así facilitar el inicio de sesión y el acceso a los datos. Esto se realiza como parte de los pasos para crear un clúster aprovisionado o un grupo de trabajo sin servidor. Cualquier persona con permisos para crear recursos de Redshift puede realizar estas tareas de integración del IAM Identity Center. Al crear un clúster aprovisionado, primero debe elegir Crear clúster en la consola de Amazon Redshift. Los siguientes pasos muestran cómo habilitar la administración del IAM Identity Center para una base de datos. (No incluye todos los pasos para crear un clúster).

1. Seleccione Habilitar para **<**nombre de su clúster**>** en la sección para la integración del IAM Identity Center en los pasos de creación del clúster.
2. Hay un paso en el proceso en el que se habilita la integración. Para ello, seleccione Habilitar la integración del IAM Identity Center en la consola.
3. Para el nuevo clúster o grupo de trabajo, cree roles de base de datos en Redshift con los comandos SQL. A continuación, se muestra el comando:

   ```
   CREATE ROLE <idcnamespace:rolename>;
   ```

   El espacio de nombres y el nombre del rol son los siguientes:

   - Prefijo del espacio de nombres de IAM Identity Center: es el espacio de nombres que se ha definido al configurar la conexión entre IAM Identity Center y Redshift.
   - Nombre del rol: este rol de base de datos de Redshift debe coincidir con el nombre del grupo en IAM Identity Center.

   Redshift se conecta con el IAM Identity Center y obtiene la información necesaria para crear y asignar el rol de la base de datos al grupo del IAM Identity Center.

Tenga en cuenta que, cuando se crea un nuevo almacenamiento de datos, el rol de IAM especificado para la integración con IDC se adjunta automáticamente al clúster aprovisionado o al grupo de trabajo de Amazon Redshift sin servidor. Cuando termine de introducir los metadatos del clúster necesarios y de crear el recurso, podrá comprobar el estado de la integración del IAM Identity Center en las propiedades. Si los nombres de grupo del IAM Identity Center tienen espacios, es obligatorio utilizar comillas en SQL al crear el rol correspondiente.

Tras habilitar la base de datos de Redshift y crear roles, ya podrá conectarse a la base de datos con el editor de consultas v2 de Amazon Redshift o Amazon QuickSight. Encontrará información detallada al respecto en las secciones siguientes.

Configuración de la **`RedshiftIdcApplication`** predeterminada mediante la API

Su administrador de identidades se encarga de la configuración. En la API, se crea y rellena una `RedshiftIdcApplication`, que representa la aplicación de Redshift en el IAM Identity Center.

1. Para empezar, puede crear usuarios y añadirlos a grupos del IAM Identity Center. Puede hacerlo en la consola de AWS del IAM Identity Center (IDC).
2. Llame a `create-redshift-idc-application` para crear una aplicación de IDC que se pueda usar con Redshift. La aplicación se crea rellenando los valores necesarios. El nombre para mostrar es el nombre que se mostrará en el panel de IDC. El ARN del rol de IAM es un ARN que tiene permisos para acceder al IAM Identity Center y que Redshift también puede asumir.

   ```
   aws redshift create-redshift-idc-application
   --idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
   --identity-namespace 'MyIdcIdentityNamespace'
   --idc-display-name 'TEST-NEW-APPLICATION'
   --iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
   --redshift-idc-application-name 'myredshiftidcapplication'
   ```

   En el siguiente ejemplo, se muestra un ejemplo de respuesta de `RedshiftIdcApplication` a la llamada a `create-redshift-idc-application`.

   ```
   "RedshiftIdcApplication": {
                   "IdcInstanceArn": "arn:aws:sso:::instance/ssoins-1234a01a1b12345d",
                   "RedshiftIdcApplicationName": "test-application-1",
                   "RedshiftIdcApplicationArn": "arn:aws:redshift:us-
   east-1:012345678901:redshiftidcapplication:12aaa111-3ab2-3ab1-8e90-b2d72aea588b",
                   "IdentityNamespace": "AWSIDC",
   ```

```
                "IdcDisplayName": "Redshift-Idc-Application",
                "IamRoleArn": "arn:aws:redshift:us-east-1:012345678901:role/
TestRedshiftRole",
                "IdcManagedApplicationArn": "arn:aws:sso::012345678901:application/
ssoins-1234a01a1b12345d/apl-12345678910",
                "IdcOnboardStatus": "arn:aws:redshift:us-
east-1:123461817589:redshiftidcapplication",
                "RedshiftIdcApplicationArn": "Completed",
                "AuthorizedTokenIssuerList": [
                      "TrustedTokenIssuerArn": ...,
                      "AuthorizedAudiencesList": [...]...
                ]}
```

3. Puede utilizar `create-application-assignment` para asignar grupos específicos o usuarios individuales a la aplicación administrada en el IAM Identity Center. De este modo, puede especificar los grupos que desea administrar a través del IAM Identity Center. Si el administrador de la base de datos crea roles de base de datos en Redshift, los nombres de grupo en el IAM Identity Center se asignan a los nombres de los roles de Redshift. Los roles controlan los permisos en la base de datos. Para obtener más información, consulte Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center.
4. Tras habilitar la aplicación, llame a `create-cluster` e incluya el ARN de la aplicación administrada por Redshift desde el IAM Identity Center. De este modo, se asocia el clúster a la aplicación administrada en el IAM Identity Center.

Asociación de una aplicación del IAM Identity Center a un clúster o grupo de trabajo existentes

Si ya tiene un clúster o grupo de trabajo que le gustaría habilitar para la integración del IAM Identity Center, puede hacerlo ejecutando un comando SQL. Puede ejecutar el siguiente comando para habilitar la integración. Es necesario que un administrador de bases de datos ejecute la consulta y que la conexión entre Redshift y el IAM Identity Center ya esté configurada. Al configurar `ENABLE`, permite que el IAM Identity Center administre las identidades del clúster o grupo de trabajo.

```
ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-
id-1>:role/<role-name>' | [DISABLE | ENABLE]
```

Puede eliminar un proveedor de identidades existente. En el siguiente ejemplo, se muestra cómo CASCADE elimina los usuarios y roles asociados al proveedor de identidades.

```
DROP IDENTITY PROVIDER
```

```
<provider_name> [ CASCADE ]
```

Configuración de permisos de usuario

Un administrador configura los permisos para varios recursos en función de los atributos de identidad de los usuarios y la pertenencia a grupos dentro de su proveedor de identidades o directamente en el IAM Identity Center. Por ejemplo, el administrador del proveedor de identidades puede añadir un ingeniero de bases de datos a un grupo adecuado a su rol. El nombre de este grupo se asigna a un nombre de rol de base de datos de Redshift. El rol proporciona o restringe el acceso a tablas o vistas específicas en Redshift.

Personas con el rol de administrador para conectar aplicaciones

A continuación se indican las personas clave para conectar las aplicaciones de análisis a la aplicación administrada por IAM Identity Center para Redshift:

- Administrador de aplicaciones: crea una aplicación y configura los servicios con los que permitirá el intercambio de tokens de identidad. Este administrador también especifica qué usuarios o grupos tienen acceso a la aplicación.
- Administrador de datos: configura el acceso detallado a los datos. Los usuarios y grupos del IAM Identity Center pueden asignarse a permisos específicos.

Conexión a Amazon Redshift con IAM Identity Center mediante Amazon QuickSight

A continuación, se muestra cómo utilizar Amazon QuickSight para autenticarse con Redshift cuando está conectado y el acceso se administra a través del IAM Identity Center: Autorización de conexiones desde Amazon QuickSight a clústeres de Amazon Redshift. Estos pasos también se aplican a Amazon Redshift sin servidor.

Conexión a Amazon Redshift con IAM Identity Center mediante el editor de consultas v2 de Amazon Redshift

Al completar los pasos para configurar una conexión del IAM Identity Center con Redshift, el usuario puede acceder a la base de datos y a los objetos correspondientes de la base de datos a través de su identidad basada en el IAM Identity Center y con el prefijo de espacio de nombres. Para obtener más información sobre la conexión a bases de datos de Redshift con el editor de consultas v2, consulte Trabajo con el editor de consultas v2.

Consulta de datos mediante AWS Lake Formation

El uso de AWS Lake Formation facilita la administración y la protección centralizadas de su lago de datos y proporciona acceso a los datos. La configuración de la propagación de identidades a Lake Formation a través del IAM Identity Center y Redshift permite que un administrador pueda permitir un acceso detallado a un lago de datos de Amazon S3, en función de los grupos de proveedores de identidades (IdP) de la organización. Estos grupos se administran a través del IAM Identity Center. En esta sección se explica cómo configurar un par de casos prácticos mediante consultas de un lago de datos y consultas de un recurso compartido de datos, que demuestran cómo aprovechar el IAM Identity Center con Redshift para conectarse a los recursos gobernados por Lake Formation.

Uso de una conexión de Redshift y el IAM Identity Center para consultar un lago de datos

Estos pasos explican un caso práctico en el que se utiliza el IAM Identity Center conectado a Redshift para consultar un lago de datos gobernado por Lake Formation.

Requisitos previos

Este procedimiento tiene varios pasos de requisitos previos:

1. El IAM Identity Center debe configurarse para admitir la autenticación y la administración de identidades con Redshift. Puede activar el IAM Identity Center desde la consola y seleccionar un origen de proveedor de identidades (IdP). Después, debe sincronizar un conjunto de usuarios de IdP con el IAM Identity Center. También debe configurar una conexión entre el IAM Identity Center y Redshift, siguiendo los pasos detallados anteriormente en este documento.
2. Cree un nuevo clúster de Amazon Redshift y habilite la administración de identidades a través del IAM Identity Center en los pasos de configuración.
3. Cree una aplicación administrada por IAM Identity Center para Lake Formation y configúrela. Esto se realiza tras configurar la conexión entre IAM Identity Center y Redshift. A continuación se indican los pasos a seguir:
   a. En la AWS CLI, utilice el comando `modify-redshift-idc-application` para habilitar la integración del servicio Lake Formation con la aplicación administrada por IAM Identity Center para Redshift. Esta llamada incluye el parámetro `service-integrations`, que se establece en un valor de cadena de configuración que da autorización a Lake Formation.
   b. Configure Lake Formation con el comando `create-lake-formation-identity-center-configuration`. Al hacerlo, se crea una aplicación de IAM Identity Center para Lake Formation, que es visible en el portal del IAM Identity Center. El administrador debe establecer el argumento `--cli-input-json`, cuyo valor es la ruta hacia un archivo JSON que usa el

formato estándar para todas las llamadas a la API de la CLI de AWS. Debe incluir los siguientes valores:

- `CatalogId`: ID del catálogo de Lake Formation.
- `InstanceArn`: el ARN de la instancia del IAM Identity Center.

Una vez que el administrador complete la configuración previa, el administrador de la base de datos puede crear un esquema externo con el fin de consultar el lago de datos.

1. El administrador crea el esquema externo: el administrador de la base de datos de Redshift se conecta a la base de datos y crea un esquema externo mediante la siguiente instrucción SQL:

   ```
   CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
    'my_lf_integrated_db' catalog_id '12345678901234';
   ```

   Tenga en cuenta que, en este caso, no es necesario especificar un rol de IAM, ya que el acceso se gestiona a través del IAM Identity Center.

2. El administrador concede permisos: el administrador concede el uso a un grupo del IAM Identity Center, que concede permisos sobre los recursos de Redshift. Para ello, se ejecuta una instrucción SQL como la siguiente:

   ```
   GRANT USAGE ON SCHEMA "my_external_schema" to "IDCCO:sales";
   ```

   Posteriormente, el administrador concede permisos de Lake Formation sobre los objetos, según los requisitos de la organización, mediante la CLI de AWS:

   ```
   aws lakeformation grant-permissions ...
   ```

3. Los usuarios ejecutan consultas: en este punto, un usuario del IAM Identity Center que forme parte del grupo de ventas puede iniciar sesión mediante el editor de consultas v2 en la base de datos de Redshift. A continuación, puede ejecutar una consulta que acceda a una tabla del esquema externo, como en el ejemplo siguiente:

   ```
   SELECT * from my_external_schema.table1;
   ```

Uso de una conexión de Redshift y el IAM Identity Center para conectarse a un recurso compartido de datos

Puede acceder a un recurso compartido de datos desde un almacenamiento de datos de Redshift diferente cuando el acceso se administre a través del IAM Identity Center. Para ello, ejecute una consulta para configurar una base de datos externa. Antes de completar estos pasos, se supone que tiene una conexión configurada entre Redshift y el IAM Identity Center y que ha creado la aplicación de AWS Lake Formation, tal y como se detalla en el procedimiento anterior.

1. Creación de la base de datos externa: el administrador crea una base de datos externa para compartir datos y hace referencia a ella a través de su ARN. En el siguiente ejemplo se muestra cómo hacerlo:

   ```
   CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-
   east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
   ```

   En este caso práctico, en el que se utiliza el IAM Identity Center con Redshift para la administración de identidades, no se incluye el rol de IAM.

2. El administrador configura los permisos: tras crear una base de datos, el administrador otorga su uso a un grupo del IAM Identity Center. Esto otorga permisos sobre los recursos de Redshift:

   ```
   GRANT USAGE ON DATABASE "my_external_db" to "IDCCO:sales";
   ```

   El administrador también otorga permisos de Lake Formation sobre los objetos mediante la CLI de AWS:

   ```
   aws lakeformation grant-permissions ...
   ```

3. Los usuarios ejecutan consultas: un usuario del grupo de ventas puede consultar una tabla de la base de datos en función de los permisos asignados:

   ```
   select * from redshift_external_db.public.employees;
   ```

Para obtener más información sobre la concesión de permisos en un lago de datos y la concesión de permisos en los recursos compartidos de datos, consulte Granting permissions to users and groups. Para obtener más información sobre cómo conceder el uso a un esquema o a una base de datos, consulte GRANT.

Integración de su aplicación o herramienta con OAuth mediante un emisor de tokens de confianza

Si es un proveedor de herramientas, puede añadir funciones para conectarse a Redshift mediante la conexión del IAM Identity Center.

Complemento para el uso de Redshift con el IAM Identity Center

Este complemento, que se utiliza para la autenticación con el IAM Identity Center, proporciona propiedades de conexión adicionales para facilitar la autenticación:

Nombre del complemento	Descripción	Valor
`IdpTokenAuthPlugin`	Es un complemento de autenticación que acepta un token del IAM Identity Center (IDC) o un OIDC JWT de cualquier proveedor de identidades web vinculado al IDC.	`com.amazon.redshift.plugin.IdpTokenAuthPlugin`

El nombre del complemento correspondiente para ODBC y Python es IdpTokenAuthPlugin. Además, ODBC y Python no utilizan el nombre de clase completo para los complementos. Solo lo usa JDBC. En la herramienta, utilice la propiedad `plugin_name` para introducir el valor del nombre. En las herramientas basadas en Python, esta propiedad se denomina `credentials_provider`.

El complemento tiene asociadas las siguientes opciones de conexión:

- IDC_Region: es la región de AWS en la que se encuentra la instancia del IAM Identity Center (IDC).
- Identity_Namespace: es el espacio de nombres de identidad que se utilizará al autenticarse con el complemento IdpTokenAuthPlugin. Ayuda a Redshift a determinar qué instancia del IAM Identity Center utilizar.

Estos valores se introducen en las propiedades de conexión de la herramienta que se desarrolla y se utiliza para conectarse. Para obtener más información sobre las opciones de JDBC, consulte

Opciones de configuración del controlador JDBC versión 2.1. Para obtener más información sobre las opciones de ODBC, consulte Configuración de las opciones del controlador ODBC.

Limitaciones

Se aplican estas limitaciones:

- La autenticación de herramientas basadas en JDBC, ODBC y Python no se admite con Redshift conectado al IAM Identity Center. Tendría que personalizar el controlador de la herramienta. Solo admite conexiones desde Amazon QuickSight y el editor de consultas v2.
- La configuración de seguridad y privacidad del navegador de Internet, especialmente la que controla la configuración segura de las cookies, como la característica Protección total de cookies de Firefox, puede provocar el bloqueo de los intentos de conexión desde el editor de consultas v2 a la base de datos de Redshift. Para solucionar el problema, puede agregar la URL del sitio de la consola del editor de consultas v2 a la lista de excepciones de protección contra el rastreo del navegador. Para hacerlo en Firefox, haga clic en el escudo de la barra de direcciones del navegador y cambie el botón para desactivar la protección contra el rastreo del editor de consultas v2. En Chrome, si utiliza el modo incógnito, haga clic en el icono del ojo de la barra de direcciones para permitir el uso de cookies de terceros para el editor de consultas v2.

Uso de roles vinculados a servicios para Amazon Redshift

Amazon Redshift utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está conectado de forma directa a Amazon Redshift. Los roles vinculados a servicio están predefinidos por Amazon Redshift e incluyen todos los permisos que el servicio requiere para llamar a servicios de AWS en nombre de su clúster de Amazon Redshift.

Un rol vinculado a un servicio simplifica la configuración de Amazon Redshift porque ya no tendrá que agregar los permisos necesarios de forma manual. El rol está vinculado a los casos de uso de Amazon Redshift y tiene permisos predefinidos. Solo Amazon Redshift puede asumir el rol y solo el rol vinculado a un servicio puede usar la política de permisos predefinida. Amazon Redshift crea un rol vinculado a un servicio en su cuenta la primera vez que crea un clúster. Puede eliminar el rol vinculado al servicio solo después de eliminar todos los clústeres de Amazon Redshift de su cuenta. De esta forma, se protegen los recursos de Amazon Redshift, ya que evita que se puedan eliminar accidentalmente los permisos necesarios para obtener acceso a los recursos.

Amazon Redshift admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicio). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon Redshift

Amazon Redshift utiliza el rol vinculado al servicio denominado AWSServiceRoleForRedshift que permite que Amazon Redshift llame a los servicios de AWS en su nombre.
Este rol vinculado a un servicio se adjunta a la siguiente política administrada: `AmazonRedshiftServiceLinkedRolePolicy`. Para obtener actualizaciones de esta política, consulte Políticas administradas por AWS (predefinidas) para Amazon Redshift.

El rol vinculado a un servicio AWSServiceRoleForRedshift solo confía en que **`redshift.amazonaws.com`** asuma el rol.

La política de permisos del rol vinculado al servicio de AWSServiceRoleForRedshift permite que Amazon Redshift realice las siguientes operaciones en todos los recursos relacionados:

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeAddress`
- `ec2:AssociateAddress`
- `ec2:DisassociateAddress`
- `ec2:CreateNetworkInterface`
- `ec2:DeleteNetworkInterface`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:DescribeVpcEndpoints`

- ec2:ModifyVpcEndpoint
- ec2:DescribeVpcAttribute
- ec2:DescribeSecurityGroups
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroupRules
- ec2:DescribeAvailabilityZones
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:AssignIpv6Addresses
- ec2:UnassignIpv6Addresses

Permisos para recursos de red

Los siguientes permisos permiten acciones en Amazon EC2 para crear y administrar reglas de grupo de seguridad. Estos grupos y reglas de seguridad están asociados específicamente a la etiqueta de recurso aws:RequestTag/Redshift de Amazon Redshift. Esto limita el alcance de los permisos a recursos de Amazon Redshift específicos.

- ec2:CreateSecurityGroup
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:RevokeSecurityGroupEgress
- ec2:RevokeSecurityGroupIngress
- ec2:ModifySecurityGroupRules
- ec2:DeleteSecurityGroup

Acciones para el registro de auditoría

Las acciones enumeradas con el prefijo logs se refieren al registro de auditoría y a las características relacionadas. En concreto, la creación y la administración de grupos de registro y flujos de registro.

- logs:CreateLogGroup

- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

El siguiente JSON muestra las acciones y el alcance de los recursos, a Amazon Redshift, para el registro de auditoría.

```
[
    {
        "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogGroup",
            "logs:PutRetentionPolicy"
        ],
        "Resource": [
            "arn:aws:logs:*:*:log-group:/aws/redshift/*"
        ]
    },
    {
        "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:DescribeLogStreams",
            "logs:GetLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
        ]
    }
]
```

Para obtener más información sobre los roles vinculados a servicios y su finalidad en AWS, consulte Uso de roles vinculados a servicios. Para obtener más información sobre acciones específicas y otros recursos de IAM para Amazon Redshift, consulte Acciones, recursos y claves de condición para Amazon Redshift.

Acciones para administrar las credenciales de administrador con AWS Secrets Manager

Las acciones que aparecen con el prefijo `secretsmanager` están relacionadas con el uso de Amazon Redshift para administrar las credenciales de administrador. Estas acciones permiten que Amazon Redshift use AWS Secrets Manager para crear y administrar los secretos de sus credenciales de administrador.

El siguiente JSON muestra las acciones y el alcance de los recursos a Amazon Redshift para administrar las credenciales de administrador con AWS Secrets Manager.

```
[
    {
        "Effect": "Allow",
        "Action": [
            "secretsmanager:DescribeSecret",
            "secretsmanager:DeleteSecret",
            "secretsmanager:PutSecretValue",
            "secretsmanager:UpdateSecret",
            "secretsmanager:UpdateSecretVersionStage",
            "secretsmanager:RotateSecret"
        ],
        "Resource": [
            "arn:aws:secretsmanager:*:*:secret:redshift!*"
        ],
        "Condition": {
            "StringEquals": {
                "secretsmanager:ResourceTag/aws:secretsmanager:owningService":
 "redshift"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetRandomPassword"
        ],
        "Resource": "*"
    }
]
```

Para permitir a una entidad de IAM crear roles vinculados a servicios AWSServiceRoleForRedshift

```
{
```

```
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

Para permitir a una entidad de IAM eliminar roles vinculados a servicios AWSServiceRoleForRedshift

Agregue la siguiente instrucción de política a los permisos para esa entidad de IAM:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
    "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

Si lo desea, también puede usar una política administrada por AWS para proporcionar acceso completo a Amazon Redshift.

Creación de un rol vinculado a un servicio para Amazon Redshift

No es necesario crear de forma manual el rol vinculado al servicio AWSServiceRoleForRedshift. Amazon Redshift crea el rol vinculado al servicio por usted. Si el rol vinculado al servicio AWSServiceRoleForRedshift se ha eliminado de la cuenta, Amazon Redshift crea el rol cuando se lanza un nuevo clúster de Amazon Redshift.

> **Important**
>
> Si utilizaba el servicio Amazon Redshift antes del 18 de septiembre de 2017, fecha en que comenzó a admitir los roles vinculados a servicios, entonces Amazon Redshift creó el rol AWSServiceRoleForRedshift en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Edición de un rol vinculado a un servicio para Amazon Redshift

Amazon Redshift no permite editar el rol vinculado al servicio AWSServiceRoleForRedshift. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. No obstante, puede editar la descripción del rol con la consola de IAM, la AWS Command Line Interface (AWS CLI) o la API de IAM. Para obtener más información, consulte Modificación de un rol en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Amazon Redshift

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa.

Antes de poder eliminar un rol vinculado a un servicio de una cuenta, necesita apagar y eliminar todos los clústeres de la cuenta. Para obtener más información, consulte Cierre y eliminación de clústeres.

Puede utilizar la consola de IAM, la AWS CLI o la API de IAM para eliminar un rol vinculado a un servicio. Para obtener más información, consulte Eliminación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Uso de la autenticación de IAM para generar credenciales de usuario de base de datos

Puede generar credenciales temporales de base de datos basadas en los permisos concedidos a través de una política de permisos de AWS Identity and Access Management (IAM) para administrar el acceso que los usuarios tienen a su base de datos de Amazon Redshift.

Normalmente, los usuarios de bases de datos de Amazon Redshift inician sesión en la base de datos proporcionando un nombre de usuario y una contraseña de la base de datos. No obstante, no es necesario mantener los nombres de usuario y las contraseñas en la base de datos de Amazon Redshift. Como alternativa, puede configurar el sistema para permitir que los usuarios creen credenciales de usuario e inicien sesión en la base de datos en función de sus credenciales de IAM.

Para obtener más información, consulte Federación y proveedores de identidades en la Guía del usuario de IAM.

Temas

- Información general
- Creación de credenciales de IAM temporales
- Opciones para proporcionar credenciales de IAM

Información general

Amazon Redshift proporciona la operación de la API GetClusterCredentials para generar credenciales temporales de usuario de la base de datos. Puede configurar su cliente SQL con controladores JDBC u ODBC de Amazon Redshift que administren el proceso de llamar a la operación `GetClusterCredentials`. Para ello, recuperan las credenciales de usuario de la base de datos y establecen una conexión entre su cliente SQL y la base de datos de Amazon Redshift. También puede usar la aplicación de base de datos para llamar mediante programación a la operación `GetClusterCredentials`, recuperar las credenciales de usuario de base de datos y conectarse a la base de datos.

Si ya administra identidades de usuario fuera de AWS, puede utilizar un proveedor de identidades (IdP) conforme con el lenguaje de marcado para confirmaciones de seguridad (SAML) 2.0 para administrar el acceso a los recursos de Amazon Redshift. Puede utilizar su IdP para permitir a los usuarios federados tener acceso a un rol de IAM. Con ese rol de IAM, puede generar credenciales de base de datos temporales e iniciar sesión en las bases de datos de Amazon Redshift.

Su cliente SQL necesita permiso para llamar a la operación `GetClusterCredentials` en su nombre. Estos permisos se administran creando un rol de IAM y asociando una política de permisos de IAM que conceda o restrinja el acceso a la operación `GetClusterCredentials` y acciones relacionadas. Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

La política también concede o restringe el acceso a recursos específicos, como clústeres, bases de datos, nombres de usuario de base de datos y nombres de grupos de usuarios de Amazon Redshift.

> **Note**
>
> Le recomendamos que utilice los controladores JDBC u ODBC de Amazon Redshift para administrar el proceso de llamar a la operación `GetClusterCredentials` e iniciar sesión en la base de datos. Para simplificar, asumimos que en este tema utiliza un cliente SQL con los controladores JDBC u ODBC.

Para obtener detalles concretos y ejemplos del uso de la operación `GetClusterCredentials` o del comando paralelo de la CLI `get-cluster-credentials`, vea GetClusterCredentials y get-cluster-credentials.

Para administrar la autenticación y la autorización de forma centralizada, Amazon Redshift admite la autenticación de base de datos con IAM, lo que permite la autenticación de usuarios a través de la federación de empresas. En lugar de crear un usuario, puede utilizar las identidades existentes de AWS Directory Service, el directorio de usuarios de su empresa o un proveedor de identidades web. A estas identidades se las conoce como usuarios federados. AWS asigna un rol a un usuario federado cuando se solicita acceso a través de un IdP.

Para proporcionar acceso federado a un usuario o una aplicación cliente de la organización para llamar a las operaciones de la API de Amazon Redshift, también puede utilizar el controlador JDBC u ODBC compatible con SAML 2.0 para solicitar la autenticación del IdP de la organización. En este caso, los usuarios de la organización no tienen acceso directo a Amazon Redshift.

Creación de credenciales de IAM temporales

En esta sección, puede encontrar cómo configurar el sistema para generar credenciales temporales de usuario de base de datos basadas en IAM e iniciar sesión en la base de datos con las nuevas credenciales.

En líneas generales, el proceso es el siguiente:

1. Paso 1: Crear un rol de IAM para el acceso de inicio de sesión único de IAM

   (Opcional) Puede autenticar a los usuarios para que obtengan acceso a una base de datos de Amazon Redshift integrando la autenticación de IAM y un proveedor de identidad (IdP) de terceros.

2. Paso 2: Configurar aserciones SAML para su IdP

   (Opcional) Para usar la autenticación de IAM mediante un IdP, necesita definir una regla de notificación en la aplicación de su IdP que asigne los usuarios o grupos de su organización a un rol de IAM. Opcionalmente, puede incluir elementos de atributo para definir parámetros `GetClusterCredentials`.

3. Paso 3: Crear un rol de IAM con permisos para llamar a GetClusterCredentials

La aplicación de cliente de SQL asume el usuario cuando llama a la operación `GetClusterCredentials`. Si ha creado un rol de IAM para el acceso al proveedor de identidad, puede agregar el permiso necesario a ese rol.

4. Paso 4: Crear un usuario de base de datos y grupos de usuarios de base de datos

   (Opcional) De forma predeterminada, `GetClusterCredentials` devuelve credenciales crear un nuevo usuario si el nombre de usuario no existe. También puede elegir especificar grupos de usuarios a los que se unan los usuarios cuando inicien sesión. De forma predeterminada, los usuarios de la base de datos se unen al grupo PUBLIC.

5. Paso 5: Configurar una conexión JDBC u ODBC para usar credenciales de IAM

   Para conectarse a la base de datos de Amazon Redshift, tiene que configurar el cliente SQL para que use un controlador JDBC u ODBC de Amazon Redshift.

Paso 1: Crear un rol de IAM para el acceso de inicio de sesión único de IAM

Si no utiliza un proveedor de identidad para el acceso de inicio de sesión único, puede omitir este paso.

Si ya administra las identidades de los usuarios fuera de AWS, puede autenticar a los usuarios para que tengan acceso a una base de datos de Amazon Redshift integrando la autenticación de IAM y un proveedor de identidad (IdP) SAML-2.0 de terceros.

Para obtener más información, consulte Federación y proveedores de identidades en la Guía del usuario de IAM.

Antes de poder utilizar la autenticación de IdP de Amazon Redshift, cree un proveedor de identidad SAML de AWS. El IdP se crea en la consola de IAM para informar a AWS del IdP y de su configuración. Esto establece una relación de confianza entre la cuenta de AWS y el IdP. Si desea ver los pasos necesarios para crear un rol, consulte Creación de un rol para una federación SAML 2.0 (consola) en la Guía del usuario de IAM.

Paso 2: Configurar aserciones SAML para su IdP

Después de crear el rol de IAM, necesita definir una regla de reclamación en la aplicación de su IdP que asigne los usuarios o grupos de su organización al rol de IAM. Para obtener más información, consulte Configuración de aserciones SAML para la respuesta de autenticación en la Guía del usuario de IAM.

Si elige utilizar los parámetros `GetClusterCredentials` opcionales `DbUser`, `AutoCreate`, y `DbGroups`, tiene dos opciones. Puede establecer los valores de los parámetros con su conexión JDBC u ODBC, o bien puede establecer los valores agregando elementos de atributo SAML a su IdP. Para obtener más información acerca de los parámetros `DbUser`, `AutoCreate` y `DbGroups`, consulte Paso 5: Configurar una conexión JDBC u ODBC para usar credenciales de IAM.

> **Note**
>
> Si utiliza una variable de política de IAM `${redshift:DbUser}`, como se describe en Políticas de recursos de GetClusterCredentials, el valor de `DbUser` se sustituye por el valor obtenido por el contexto de la solicitud de la operación de la API. Los controladores de Amazon Redshift utilizan el valor de la variable `DbUser` proporcionado por la URL de conexión en lugar del valor proporcionado como atributo SAML.
> Para ayudar a proteger esta configuración, recomendamos que utilice una condición en una política de IAM para validar el valor de `DbUser` con el `RoleSessionName`. Puede encontrar ejemplos de cómo establecer una condición utilizando una política de IAM en Política de ejemplo para usar GetClusterCredentials.

Para configurar el IdP para que establezca los parámetros `DbUser`, `AutoCreate` y `DbGroups`, incluya los siguientes elementos de `Attribute`:

- Un elemento `Attribute` con el atributo `Name` establecido en "https://redshift.amazon.com/SAML/Attributes/DbUser"

  Establezca el elemento `AttributeValue` en el nombre del usuario que se va a conectar a la base de datos de Amazon Redshift.

  El valor del elemento `AttributeValue` debe estar en mayúsculas, empezar por una letra, contener solo caracteres alfanuméricos, guion bajo ('_'), signo más ('+'), punto ('.'), arroba ('@') o guion ('-') y tener menos de 128 caracteres. Normalmente, el nombre de usuario es un ID de usuario (por ejemplo, bobsmith) o una dirección de correo electrónico (por ejemplo, bobsmith@example.com). El valor no puede incluir un espacio (por ejemplo, un nombre de visualización de un usuario como Bob Smith).

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
    <AttributeValue>user-name</AttributeValue>
</Attribute>
```

- Un elemento Attribute con el atributo Name establecido en "https://redshift.amazon.com/SAML/Attributes/AutoCreate"

  Establezca el elemento AttributeValue en true para crear un nuevo usuario de base de datos si no existe ninguno. Establezca el elemento AttributeValue en false para especificar que el usuario de la base de datos debe existir en la base de datos de Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
    <AttributeValue>true</AttributeValue>
</Attribute>
```

- Un elemento `Attribute` con el atributo `Name` establecido en "https://redshift.amazon.com/SAML/Attributes/DbGroups"

  Este elemento contiene uno o más elementos `AttributeValue`. Establezca cada elemento `AttributeValue` en un nombre de grupo de bases de datos al que `DbUser` debe unirse durante la sesión cuando se conecta a la base de datos de Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
    <AttributeValue>group1</AttributeValue>
    <AttributeValue>group2</AttributeValue>
    <AttributeValue>group3</AttributeValue>
</Attribute>
```

Paso 3: Crear un rol de IAM con permisos para llamar a GetClusterCredentials

El cliente SQL necesita autorización para llamar a la operación `GetClusterCredentials` en su nombre. Para proporcionar esta autorización, cree un usuario o rol y asocie una política que conceda los permisos necesarios.

Para crear un rol de IAM con permisos para llamar a GetClusterCredentials

1. Mediante el servicio IAM, cree un usuario o rol. También puede utilizar un usuario o rol existente. Por ejemplo, si ha creado un rol de IAM para el acceso al proveedor de identidad, puede asociar las políticas de IAM necesarias a ese rol.
2. Asocie una política de permisos con permiso para llamar a la operación `redshift:GetClusterCredentials`. En función de los parámetros opcionales que especifique, también puede permitir o restringir acciones y recursos adicionales en la política:

- Para permitir que el cliente SQL recupere el ID de clúster, la región de AWS y el puerto, debe incluir el permiso para llamar a la operación `redshift:DescribeClusters` con el recurso del clúster de Redshift.
- Si utiliza la opción `AutoCreate`, incluya el permiso para llamar a `redshift:CreateClusterUser` con el recurso `dbuser`. El siguiente formato de nombre de recurso de Amazon (ARN) especifica el `dbuser` de Amazon Redshift. Reemplace *`region`*, *`account-id`* y *`cluster-name`* por los valores correspondientes a su región, cuenta y clúster de AWS. Para *`dbuser-name`*, especifique el nombre de usuario que se utilizará para iniciar sesión en la base de datos del clúster.

  ```
  arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
  ```

- (Opcional) Agregue un ARN que especifique el recurso `dbname` de Amazon Redshift en el siguiente formato. Reemplace *`region`*, *`account-id`* y *`cluster-name`* por los valores correspondientes a su región, cuenta y clúster de AWS. En *`database-name`*, especifique el nombre de una base de datos en la que el usuario va a iniciar sesión.

  ```
  arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
  ```

- Si utiliza la opción `DbGroups`, incluya el permiso para llamar a la operación `redshift:JoinGroup` con el recurso `dbgroup` de Amazon Redshift en el siguiente formato. Reemplace *`region`*, *`account-id`* y *`cluster-name`* por los valores correspondientes a su región, cuenta y clúster de AWS. En *`dbgroup-name`*, especifique el nombre del grupo de usuarios al que se unirá el usuario cuando inicie sesión.

  ```
  arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
  ```

Para obtener más información y ejemplos, consulte Políticas de recursos de GetClusterCredentials.

En el siguiente ejemplo, se muestra una política que permite al rol de IAM llamar a la operación `GetClusterCredentials`. La especificación del recurso `dbuser` de Amazon Redshift concede al rol acceso al nombre de usuario de base de datos `temp_creds_user` en el clúster denominado `examplecluster`.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

Puede utilizar el carácter comodín (*) para sustituir todo o una parte del nombre del clúster, el nombre de usuario y los nombres de grupos de usuarios de base de datos. El siguiente ejemplo permite el acceso a cualquier usuario que empiece por `temp_` a cualquier clúster en la cuenta especificada.

> **Important**
>
> En la instrucción del siguiente ejemplo, se especifica un carácter comodín (*) como parte del valor del recurso, de modo que la política admita cualquier recurso que comience por los caracteres especificados. Utilizar un carácter comodín en las políticas de IAM puede resultar demasiado permisivo. Como práctica recomendada, es conveniente utilizar la política más restrictiva posible en la aplicación empresarial.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

El siguiente ejemplo muestra una política que permite al rol de IAM llamar a la operación `GetClusterCredentials` con la opción para crear automáticamente un nuevo usuario y especificar los grupos a los que se une el usuario al iniciar sesión. La cláusula `"Resource": "*"` concede al rol acceso a cualquier recurso, incluidos clústeres, usuarios de bases de datos o grupos de usuarios.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": {
    "Effect": "Allow",
    "Action": [
             "redshift:GetClusterCredentials",
             "redshift:CreateClusterUser",
  "redshift:JoinGroup"
            ],
    "Resource": "*"
  }
}
```

Para obtener más información, consulte Sintaxis de ARN de Amazon Redshift.

Paso 4: Crear un usuario de base de datos y grupos de usuarios de base de datos

De manera opcional, puede crear un usuario de base de datos que utilice para iniciar sesión en la base de datos del clúster. Si crea credenciales de usuario temporales para un usuario existente, puede deshabilitar la contraseña del usuario para obligar al usuario a que inicie sesión con la contraseña temporal. También puede usar la opción Autocreate de `GetClusterCredentials` para crear automáticamente un nuevo usuario de base de datos.

Puede utilizar los permisos que quiera para crear los grupos de usuarios de base de datos a los que el usuario de base de datos de IAM se va a unir al iniciar sesión. Cuando llama a la operación `GetClusterCredentials`, puede especificar una lista de nombres de grupos de usuarios a los que se une el usuario cuando inicia sesión. Esta pertenencia a grupos solo es válida para las sesiones creadas utilizando las credenciales generadas con la solicitud especificada.

Para crear un usuario y grupos de usuarios de base de datos

1. Inicie sesión en la base de datos de Amazon Redshift y cree un usuario de base de datos mediante CREATE USER o modifique un usuario existente mediante ALTER USER.
2. Si lo desea, especifique la opción PASSWORD DISABLE para impedir que el usuario utilice una contraseña. Cuando se deshabilita la contraseña de un usuario, el usuario solo puede iniciar sesión con credenciales temporales. Si la contraseña no está deshabilitada, el usuario puede iniciar sesión con la contraseña o con las credenciales temporales. No puede deshabilitar la contraseña de un super usuario.

   Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	De
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Utilice credenciales a largo plazo para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • En el caso de la AWS CLI, consulte Configuración de la AWS CLI para usar AWS IAM Identity Center en la Guía del usuario de AWS Command Line Interface. • En el caso de los AWS SDK, las herramientas y las API de AWS, consulte Autenticación de IAM Identity Center en la Guía de referencia de AWS SDK y herramientas.
IAM	Utilice credenciales a largo plazo para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de Uso de credenciales temporales con recursos de AWS de la Guía del Usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	De
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para ver los SDK y las herramientas de AWS, consulte Autenticar mediante credenciales a largo plazo en la Guía de referencia de SDK y herramientas de AWS. • Para las API de AWS, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

El siguiente ejemplo crea un usuario con la contraseña deshabilitada.

```
create user temp_creds_user password disable;
```

El siguiente ejemplo deshabilita la contraseña de un usuario existente.

```
alter user temp_creds_user password disable;
```

3. Cree grupos de usuarios de base de datos mediante CREATE GROUP.
4. Utilice el comando GRANT para definir privilegios de acceso para los grupos.

Paso 5: Configurar una conexión JDBC u ODBC para usar credenciales de IAM

Puede configurar su cliente SQL con un controlador JDBC u ODBC de Amazon Redshift. Este controlador administra el proceso de creación de credenciales de usuario de la base de datos y establecimiento de una conexión entre el cliente SQL y la base de datos de Amazon Redshift.

Si usa un proveedor de identidad para la autenticación, especifique el nombre de un complemento de proveedor de credenciales. Los controladores JDBC y ODBC de Amazon Redshift incluyen complementos para los siguientes proveedores de identidad basados en SAML:

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

  Para ver los pasos para configurar Microsoft Azure AD como proveedor de identidades, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD.

Para configurar una conexión JDBC para usar las credenciales de IAM

1. Descargue el controlador JDBC de Amazon Redshift más reciente de la página Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.
2. Cree una URL de JDBC con las opciones de credenciales de IAM en uno de los siguientes formatos. Para usar la autenticación de IAM, agregue `iam:` a la URL de JDBC de Amazon Redshift detrás de `jdbc:redshift:`, como se muestra en el siguiente ejemplo.

   ```
   jdbc:redshift:iam://
   ```

   Agregue `cluster-name`, `region` y `account-id`. El controlador JDBC usa la información de su cuenta de IAM y el nombre del clúster para recuperar el ID del clúster y la región de AWS. Para ello, el usuario o rol debe tener permiso para llamar a la operación `redshift:DescribeClusters` con el clúster especificado. Si el usuario o el rol no tiene permiso para llamar a la operación `redshift:DescribeClusters`, incluya el ID del clúster, la región de AWS y el puerto como se muestra en el siguiente ejemplo. El número de puerto es opcional.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com:5439/dev
```

3. Agregue opciones de JDBC para proporcionar las credenciales de IAM. Para proporcionar las credenciales de IAM se usan diferentes combinaciones de opciones de JDBC. Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

   La siguiente URL especifica AccessKeyID y SecretAccessKey para un usuario.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
   bPxRfiCYEXAMPLEKEY
   ```

   En el siguiente ejemplo, se especifica un perfil con nombre que contiene las credenciales de IAM.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
   ```

4. Agregue las opciones JDBC que utiliza el controlador JDBC para llamar a la operación de la API `GetClusterCredentials`. No incluya estas opciones si llama a la operación de la API `GetClusterCredentials` mediante programación.

   El siguiente ejemplo incluye las opciones `GetClusterCredentials` de JDBC.

   ```
   jdbc:redshift:iam://examplecluster:us-west-2/dev?
   plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
   ```

Para configurar una conexión ODBC para usar las credenciales de IAM

En el procedimiento siguiente, sólo puede encontrar pasos para configurar la autenticación de IAM. Para ver el procedimiento para usar la autenticación estándar, que usa un nombre de usuario y una contraseña de la base de datos, consulte Configuración de una conexión ODBC.

1. Instale y configure el controlador ODBC de Amazon Redshift más reciente para su sistema operativo. Para obtener más información, consulte la página Configuración de una conexión ODBC.

> **Important**
>
> La versión del controlador ODBC de Amazon Redshift debe ser 1.3.6.1000 o posterior.

2. Siga los pasos correspondientes a su sistema operativo para configurar las opciones de conexión.

   Para obtener más información, consulte una de las siguientes:

   - Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows
   - Uso de un administrador de controladores ODBC para configurar el controlador en los sistemas operativos Linux y macOS X

3. En los sistemas operativos Microsoft Windows, acceda a la ventana “Amazon Redshift ODBC Driver DSN Setup” (Configuración de DSN del controlador ODBC de Amazon Redshift).

   a. En Connection Settings (Configuración de conexión), escriba la siguiente información:

      - Data Source Name
      - Server (Servidor) (opcional)
      - Port (Puerto) (opcional)
      - Base de datos

      Si el usuario o el rol tiene permiso para llamar a la operación `redshift:DescribeClusters`, solo son necesarios Nombre del origen de datos y Base de datos. Amazon Redshift utiliza ClusterId y Region (Región) para obtener el servidor y el puerto llamando a la operación `DescribeCluster`.

      Si el usuario o el rol no tiene permiso para llamar a la operación `redshift:DescribeClusters`, proporcione especifique Servidor y Puerto.

   b. En Autenticación, elija un valor para Tipo de autenticación.

      Para cada tipo de autenticación, introduzca los valores que se enumeran a continuación:

      Perfil de AWS

         Introduzca la información siguiente:

         - ID del clúster

- Region
- Nombre del perfil

  Ingrese el nombre de un perfil en un archivo de configuración de AWS que contenga valores para las opciones de conexión de ODBC. Para obtener más información, consulte Uso de un perfil de configuración.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

  Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

Credenciales de IAM

Introduzca la información siguiente:

- ID del clúster
- Region
- AccessKeyID (ID de clave de acceso) y SecretAccessKey (Clave de acceso secreta)

  El ID de clave de acceso y la clave de acceso secreta del rol de IAM configurado para la autenticación de la base de datos de IAM.
- SessionToken

  SessionToken (Token de sesión) es obligatorio para las funciones de IAM con credenciales temporales. Para obtener más información, consulte Credenciales de seguridad temporales.

Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser (obligatorio)
- User AutoCreate (Creación automática de usuarios) (opcional)
- DbGroups (Grupos de base de datos) (opcional)

Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

Proveedor de identidad: AD FS

Para la autenticación integrada de Windows con AD FS, deje User (Usuario) y Password (Contraseña) vacíos.

Proporcione los detalles del IdP:

- IdP Host (Host del proveedor de identidades)

  El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales (/).

- IdP Port (Puerto del proveedor de identidades) (opcional)

  El puerto usado por el proveedor de identidad. El valor predeterminado es 443.

- Preferred Role (Función preferida)

  El nombre de recurso de Amazon (ARN) de un rol de IAM obtenido de los elementos `AttributeValue` de varios valores del atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte Configuración de aserciones SAML para el IdP.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

Proveedor de identidades: PingFederate

En User (Usuario) y Password (Contraseña), introduzca el nombre de usuario y la contraseña del IdP.

Proporcione los detalles del IdP:

- IdP Host (Host del proveedor de identidades)

  El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales (/).

- IdP Port (Puerto del proveedor de identidades) (opcional)

  El puerto usado por el proveedor de identidad. El valor predeterminado es 443.

- Preferred Role (Función preferida)

  El nombre de recurso de Amazon (ARN) de un rol de IAM obtenido de los elementos `AttributeValue` de varios valores del atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte Configuración de aserciones SAML para el IdP.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

Proveedor de identidades: Okta

En User (Usuario) y Password (Contraseña), introduzca el nombre de usuario y la contraseña del IdP.

Proporcione los detalles del IdP:

- IdP Host (Host del proveedor de identidades)

  El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales (/).

- IdP Port (Puerto del proveedor de identidades)

Este valor no es utilizado por Okta.

- Preferred Role (Función preferida)

  Un nombre de recurso de Amazon (ARN) de un rol de IAM obtenido de los elementos `AttributeValue` del atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte Configuración de aserciones SAML para el IdP.

- Okta App ID (ID de aplicación Okta)

  Un ID de una aplicación Okta. El valor de App ID se incluye detrás de "amazon_aws" en el enlace incrustado de la aplicación Okta. Póngase en contacto con el administrador de su IdP para obtener este valor.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

Proveedor de identidades: Azure AD

En User (Usuario) y Password (Contraseña), introduzca el nombre de usuario y la contraseña del IdP.

En Cluster ID (ID de clúster) y Region (Región), ingrese el ID de clúster y la región de AWS del clúster de Amazon Redshift.

En Database (Base de datos), ingrese la base de datos que creó para el clúster de Amazon Redshift.

Proporcione los detalles del IdP:

- Arrendatario de IdP

  El inquilino utilizado para Azure AD.

- Secreto de cliente de Azure

  El secreto del cliente de la aplicación para empresas de Amazon Redshift en Azure.

- ID de cliente de Azure

  El ID del cliente (ID de la aplicación) de la aplicación para empresas de Amazon Redshift en Azure.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

Opciones para proporcionar credenciales de IAM

Para proporcionar credenciales de IAM para una conexión JDBC u ODBC, elija una de las siguientes opciones.

- Perfil de AWS

  Como alternativa a proporcionar valores de credenciales en forma de opciones de JDBC u ODBC, puede incluir los valores en un perfil con nombre. Para obtener más información, consulte Uso de un perfil de configuración.

- Credenciales de IAM

  Proporcione valores para AccessKeyID, SecretAccessKey y, opcionalmente, SessionToken en forma de opciones de JDBC u ODBC. SessionToken es obligatorio únicamente para un rol de IAM con credenciales temporales. Para obtener más información, consulte Opciones de JDBC y ODBC para proporcionar credenciales de IAM.

- Federación de proveedores de identidades

  Cuando utilice la federación de proveedores de identidades para permitir que los usuarios de un proveedor de identidades se autentiquen en Amazon Redshift, especifique el nombre de un

complemento del proveedor de credenciales. Para obtener más información, consulte Uso de un complemento de proveedor de credenciales.

Los controladores JDBC y ODBC de Amazon Redshift incluyen complementos para los siguientes proveedores de credenciales de identidad federada basados en SAML:

- Servicios de identidad federada de Microsoft Active (AD FS)
- PingOne
- Okta
- Microsoft Azure Active Directory (Azure AD)

Puede proporcionar el nombre del complemento y los valores relacionados en forma de opciones de JDBC u ODBC o mediante un perfil. Para obtener más información, consulte Opciones de configuración del controlador JDBC versión 2.1 y Configurar las opciones del controlador ODBC.

Para obtener más información, consulte Configurar una conexión JDBC u ODBC para usar credenciales de IAM.

Uso de un perfil de configuración

Puede proporcionar las opciones de credenciales de IAM y las opciones de `GetClusterCredentials` como configuraciones en perfiles con nombre en su archivo de configuración de AWS. Para proporcionar el nombre del perfil, utilice la opción Profile JDBC. La configuración se almacena en un archivo denominado `config` o en uno denominado `credentials` en la carpeta denominada `.aws` en su directorio principal.

Para un complemento de proveedor de credenciales basado en SAML incluido con un controlador JDBC u ODBC de Amazon Redshift, puede utilizar la configuración descrita anteriormente en Uso de un complemento de proveedor de credenciales. Si no se utiliza `plugin_name`, se ignoran las demás opciones.

En el siguiente ejemplo, se muestra el archivo ~/.aws/credentials con dos perfiles.

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```

```
session_token=AQoDYXdzEPT//////////
wEXAMPLEtc764bNrC9SAPBSM22wDOk4x4HIZ8j4FZTwdQWLWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5VSXDvp75YU
9HFvlRd8Tx6q6fE8YQcHNVXAkiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSIlTJabIQwj2ICCR/oLxBA==
```

Para usar las credenciales para el ejemplo `user2`, especifique `Profile=user2` en la URL de JDBC.

Para obtener más información sobre el uso de perfiles, consulte Opciones de los archivos de configuración y credenciales en la Guía del usuario de AWS Command Line Interface.

Para obtener más información acerca del uso de perfiles para el controlador JDBC, consulte Especificación de perfiles.

Para obtener más información acerca del uso de perfiles para el controlador ODBC, consulte Configuración de la autenticación.

Opciones de JDBC y ODBC para proporcionar credenciales de IAM

En la tabla siguiente se indican las opciones de JDBC y ODBC para proporcionar credenciales de IAM.

Opción	Descripción
`Iam`	Para uso exclusivo en una cadena de conexión de ODBC. Establézcalo en 1 para usar la autenticación de IAM.

`AccessKeyID`
 	
`SecretAccessKey`
 	
`SessionToken`
	El ID de clave de acceso y clave de acceso secreta para el rol o usuario de IAM configurado para autenticación de base de datos de IAM. `SessionToken` es necesario solo para un rol de IAM con credenciales temporales. SessionToken no se usa para un usuario. Para obtener más información, consulte Credenciales de seguridad temporales.

`plugin_name`	El nombre completo de una clase que implementa un proveedor de credenciales. El controlador JDBC de Amazon Redshift incluye complementos de proveedores

Opción	Descripción
	de credenciales basados en SAML. Si proporciona `plugin_name` , también puede proporcionar otras opciones relacionadas. Para obtener más información, consulte Uso de un complemento de proveedor de credenciales.
`Profile`	El nombre de un perfil en un archivo de credenciales o configuración de AWS que contiene valores para las opciones de conexión de JDBC. Para obtener más información, consulte Uso de un perfil de configuración.

Uso de un complemento de proveedor de credenciales

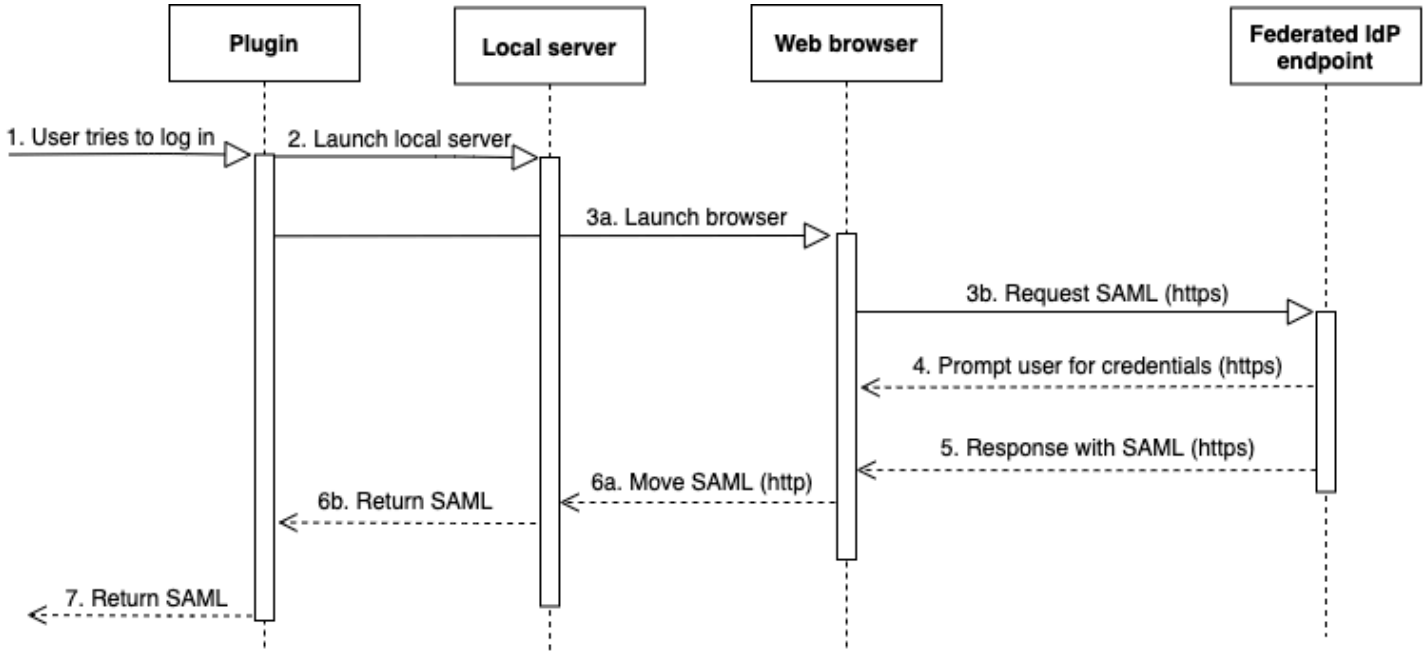
Amazon Redshift utiliza complementos de proveedor de credenciales para la autenticación de inicio de sesión único.

Para admitir la autenticación de inicio de sesión único, Amazon Redshift proporciona el complemento de Azure AD para Microsoft Azure Active Directory. Para obtener información sobre cómo configurar este complemento, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD.

Configuración de la autenticación multifactor
Configuración de la autenticación multifactor

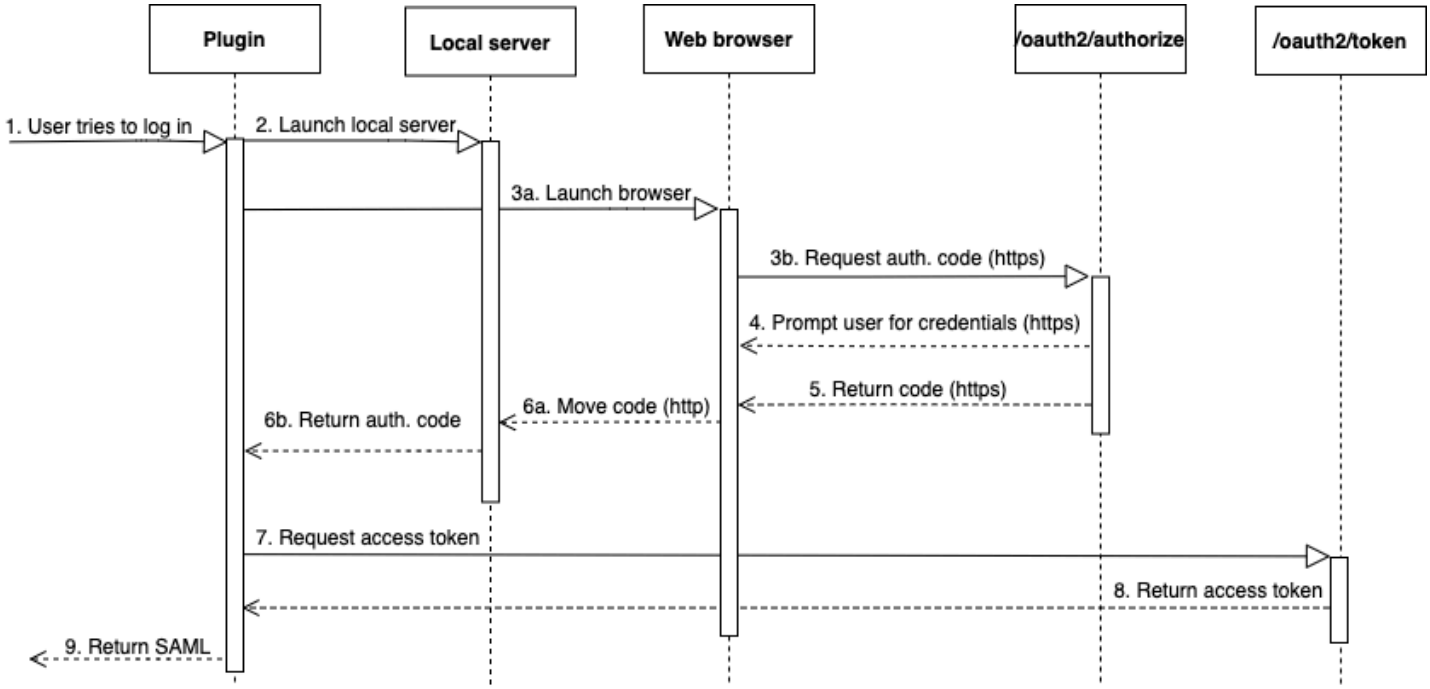
Para admitir la autenticación multifactor (MFA), Amazon Redshift proporciona complementos basados en navegador. Utilice el complemento SAML del navegador para Okta y PingOne, y el complemento de Azure AD del navegador para Microsoft Azure Active Directory.

Con el complemento SAML del navegador, la autenticación SAML sigue este flujo:



1. Un usuario intenta iniciar sesión.
2. El complemento lanza un servidor local para escuchar las conexiones entrantes en el localhost.
3. El complemento lanza un navegador web para solicitar una respuesta SAML a través de HTTPS desde el punto de conexión del proveedor de identidad federada de la URL de inicio de sesión único especificado.
4. El navegador web sigue el enlace y pide al usuario que escriba las credenciales.
5. Una vez que el usuario autentica y otorga su consentimiento, el punto de conexión del proveedor de identidad federadas devuelve una respuesta SAML a través de HTTPS al URI indicado por `redirect_uri`.
6. El navegador web traslada el mensaje de respuesta con la respuesta SAML a la `redirect_uri` indicada.
7. El servidor local acepta la conexión entrante y el complemento recupera la respuesta SAML y la transfiere a Amazon Redshift.

Con el complemento de Azure AD del navegador, la autenticación SAML sigue este flujo:



1. Un usuario intenta iniciar sesión.
2. El complemento lanza un servidor local para escuchar las conexiones entrantes en el localhost.
3. El complemento lanza un explorador web para solicitar un código de autorización desde el punto de conexión `oauth2/authorize` de Azure AD.
4. El navegador web sigue el enlace generado a través de HTTPS y solicita al usuario que escriba las credenciales. El enlace se genera utilizando propiedades de configuración, como tenant y client_id.
5. Una vez que el usuario se autentica y otorga su consentimiento, el punto de conexión `oauth2/authorize` de Azure AD devuelve y envía una respuesta a través de HTTPS con el código de autorización al `redirect_uri` indicado.
6. El navegador web traslada el mensaje de respuesta con la respuesta SAML a la `redirect_uri` indicada.
7. El servidor local acepta la conexión entrante y las solicitudes del complemento, recupera el código de autorización y envía una solicitud POST al punto de conexión `oauth2/token` de Azure AD.
8. El punto de conexión `oauth2/token` de Azure AD devuelve una respuesta con un token de acceso al `redirect_uri` indicado.
9. El complemento recupera la respuesta SAML y la transfiere a Amazon Redshift.

Consulte las siguientes secciones:

- Active Directory Federation Services (AD FS)

  Para obtener más información, consulte Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con AD FS.
- PingOne (Ping)

  Ping solo puede usarse con el adaptador de IdP PingOne mediante la autenticación de formularios.

  Para obtener más información, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Ping Identity.
- Okta

  Okta solo es compatible con la aplicación suministrada por Okta que se utiliza con la AWS Management Console.

  Para obtener más información, consulte Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con Okta.
- Microsoft Azure Active Directory

  Para obtener más información, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD.

Configuración de las opciones del complemento
Configuración de las opciones del complemento

Para usar un complemento de proveedor de credenciales basado en SAML, especifique las siguientes opciones utilizando las opciones de JDBC u ODBC o en un perfil con nombre. Si no se especifica `plugin_name`, se omiten las demás opciones.

Opción	Descripción
`plugin_name`	Para JDBC, el nombre de la clase que implementa un proveedor de credenciales. Especifique uno de los siguientes valores: • Para Active Directory Federation Services `com.amazon.redshift.plugin.AdfsCredentialsProvider` • Para Okta

Opción	Descripción

	`com.amazon.redshift.plugin.OktaCredentialsProvider`
	• Para PingFederate
	`com.amazon.redshift.plugin.PingCredentialsProvider`
	• Para Microsoft Azure Active Directory
	`com.amazon.redshift.plugin.AzureCredentialsProvider`
	• Para SAML MFA
	`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`
	• Para el inicio de sesión único de Microsoft Azure Active Directory con MFA
	`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`
	
	Para ODBC, especifique uno de los siguientes valores:
	• Para Active Directory Federation Services: `adfs`
	• Para Okta: `okta`
	• Para PingFederate: `ping`
	• Para Microsoft Azure Active Directory: `azure`
	• Para SAML MFA: `browser saml`
	• Para el inicio de sesión único de Microsoft Azure Active Directory con MFA: `browser azure ad`

`idp_host`	El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales ('/'). Para un proveedor de identidad de Okta, el valor de `idp_host` debe terminar por `.okta.com` .
`idp_port`	El puerto usado por el proveedor de identidad. El valor predeterminado es 443. Este puerto se omite para Okta.

Opción	Descripción
`preferred_role`	El nombre de recurso de Amazon (ARN) de los elementos `AttributeValue` para el atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte Configuración de aserciones SAML para el IdP.
`user`	Un nombre de usuario corporativo, incluido el dominio cuando proceda. Por ejemplo, en Active Directory, el nombre de dominio debe tener el formato dominio\nombre_usuario.
password	La contraseña del usuario corporativo. Le recomendamos que no utilice esta opción. En lugar de ello, use el cliente SQL para proporcionar la contraseña.
`app_id`	Un ID de una aplicación Okta. Solo se usa con Okta. El valor de `app_id` se incluye detrás de `amazon_aws` en el enlace incrustado de la aplicación Okta. Para obtener este valor, póngase en contacto con el administrador de su IdP. A continuación se muestra un ejemplo de un enlace incrustado de aplicación: `https://example.okta.com/home/amazon_aws/0oa2hylwrpM8UGehd1t7/272`
`idp_tenant`	Un inquilino utilizado para Azure AD. Se utiliza solo con Azure.
`client_id`	Un ID de cliente para la aplicación para empresas de Amazon Redshift en Azure AD. Se utiliza solo con Azure.

Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD

Puede usar Microsoft Azure AD como proveedor de identidades (IdP) para obtener acceso al clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin. Para obtener más información acerca de cómo configurar AWS como proveedor de servicios para el IdP, consulte Configuración de una relación de confianza para usuario autenticado y agregación de notificaciones en el proveedor de identidades SAML 2.0 en la Guía del usuario de IAM.

> **Note**
>
> Para usar Azure AD con JDBC, el controlador JDBC de Amazon Redshift debe ser la versión 1.2.37.1061 o una posterior. Para usar Azure AD con ODBC, el controlador ODBC de Amazon Redshift debe ser la versión 1.4.10.1000 o una posterior.

Vea el siguiente video para obtener información acerca de cómo federar el acceso de Amazon Redshift con el inicio de sesión único de Microsoft Azure AD: Federating Amazon Redshift access with Microsoft Azure AD single sign-on.

Para configurar Azure AD y su cuenta de AWS para establecer una relación de confianza entre ellas

1. Cree o utilice un clúster de Amazon Redshift existente para que los usuarios de Azure AD se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte Creating a Cluster (Creación de un clúster).
2. Configure un Azure Active Directory, los grupos y los usuarios utilizados para AWS en el portal de Microsoft Azure.
3. Agregue Amazon Redshift como una aplicación para empresas en el portal de Microsoft Azure para utilizar el inicio de sesión único en la consola de AWS y el inicio de sesión federado en Amazon Redshift. Elija Enterprise application (Aplicación de Enterprise).
4. Elija +New application (+Nueva aplicación). Aparecerá la página Add an application (Agregar una aplicación).
5. Buscar **`AWS`** en el campo de búsqueda.
6. Elija Amazon Web Services (AWS) y elija Add (Agregar). Esto crea la aplicación de AWS.
7. En Manage (Administrar), elija Single sign-on (Inicio de sesión único).
8. Elija SAML. Se abrirá la página Amazon Web Services (AWS) | Inicio de sesión basado en SAML.
9. Elija Yes (Sí) para continuar con la página Set up Single Sign-On with SAML (Configurar inicio de sesión único con SAML). Esta página muestra la lista de atributos preconfigurados relacionados con el inicio de sesión único.
10. En Basic SAML Configuration (Configuración básica de SAML), elija el icono de edición y, a continuación, Save (Guardar).

11. Cuando esté configurando para más de una aplicación, proporcione un valor de identificador. Por ejemplo, escriba ***https://signin.aws.amazon.com/saml#2***. Tenga en cuenta que a partir de la segunda aplicación, utilice este formato con un signo # para especificar un valor SPN único.
12. En la sección User Attributes and Claims (Atributos y reclamaciones de usuario), elija el icono de edición.

    De forma predeterminada, las reclamaciones Identificador único de usuario (UID), Role, RoleSessionName y SessionDuration están preconfiguradas.
13. Elija + Add new claim (+Agregar nueva reclamación) para agregar una reclamación para los usuarios de base de datos.

    En Nombre, ingrese **`DbUser`**.

    En Namespace (Espacio de nombres), escriba **`https://redshift.amazon.com/SAML/Attributes`**.

    En Source (Origen), elija Attribute (Atributo).

    En Source attribute (Atributo de origen), elija user.userprincipalname. A continuación, elija Guardar.
14. Elija + Add new claim (+Agregar nueva reclamación) para agregar una reclamación para AutoCreate.

    En Nombre, ingrese **`AutoCreate`**.

    En Namespace (Espacio de nombres), escriba **`https://redshift.amazon.com/SAML/Attributes`**.

    En Source (Origen), elija Attribute (Atributo).

    En Source attribute (Atributo de origen), elija "true". A continuación, elija Guardar.

    Aquí, *`123456789012`* es su cuenta de AWS, *`AzureSSO`* es un rol de IAM que ha creado y *`AzureADProvider`* es el proveedor de IAM.

Nombre de la reclamación	Valor
Identificador de usuario único (ID de nombre)	user.userprincipalname

Nombre de la reclamación	Valor
https://aws.amazon.com/SAML/Attributes/SessionDuration	"900"
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam::*123456789012* :role/*AzureSSO*,arn:aws:iam::*123456789012* :saml-provider/*AzureADProvider*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbGroups	user.assignedroles
https://redshift.amazon.com/SAML/Attributes/DbUser	user.userprincipalname

15. En Registro de aplicaciones > ***your-application-name*** > Autenticación, agregue Aplicación móvil y de escritorio. Especifique la URL como http://localhost/redshift/.
16. En la sección SAML Signing Certificate (Certificado de firma SAML), elija Download (Descargar) para descargar y guardar el archivo XML de metadatos de federación para usarlo cuando cree un proveedor de identidad SAML de IAM. Este archivo se utiliza para crear la identidad federada de inicio de sesión único.
17. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Azure Enterprise Application. Para obtener información detallada sobre los pasos, consulte Creación y administración de un proveedor de identidad de IAM (Consola) en la Guía del usuario de IAM.
18. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de un rol para SAML en la Guía del usuario de IAM.

19. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de políticas de IAM (Consola) en la Guía del usuario de IAM.

    Modifique la siguiente política (en formato JSON) para su entorno:

    - Sustituya la región de AWS de su clúster por *us-west-1*.
    - Sustituya su cuenta de AWS por *123456789012*.
    - Sustituya el identificador de clúster (o * para todos los clústeres) por *cluster-identifier*.
    - Sustituya la base de datos (o * para todas las bases de datos) por *dev*.
    - Sustituya el identificador único de su rol de IAM por *AROAJ2UCCR6DPCEXAMPLE*.
    - Sustituya el dominio de correo electrónico de su arrendatario o empresa por *example.com*.
    - Sustituya el grupo de base de datos al que planea asignar el usuario por *my_dbgroup*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:GetClusterCredentials",
            "Resource": [
                "arn:aws:redshift:us-west-1:123456789012:dbname:cluster-
identifier/dev",
                "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/
${redshift:DbUser}",
                "arn:aws:redshift:us-west-1:123456789012:cluster:cluster-
identifier"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:userid": "AROAJ2UCCR6DPCEXAMPLE:
${redshift:DbUser}@example.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "redshift:CreateClusterUser",
```

```
            "Resource": "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-
identifier/${redshift:DbUser}"
        },
        {
            "Effect": "Allow",
            "Action": "redshift:JoinGroup",
            "Resource": "arn:aws:redshift:us-west-1:123456789012:dbgroup:cluster-
identifier/my_dbgroup"
        },
        {
            "Effect": "Allow",
            "Action": [
                "redshift:DescribeClusters",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

Esta política concede permisos de la siguiente manera:

- La primera sección concede permiso a la operación `GetClusterCredentials` de la API para obtener credenciales temporales para el clúster especificado. En este ejemplo, el recurso es *`cluster-identifier`* con la base de datos *`dev`*, en la cuenta *`123456789012`* y en la región AWS *`us-west-1`*. La cláusula `${redshift:DbUser}` permite que sólo los usuarios que coincidan con el valor `DbUser` especificado en Azure AD se conecten.
- La cláusula de condición obliga a que solo ciertos usuarios obtengan credenciales temporales. Se trata de usuarios con el rol especificado por el ID único de rol *`AROAJ2UCCR6DPCEXAMPLE`* en la cuenta de IAM identificada por una dirección de email en el dominio de correo electrónico de su empresa. Para obtener más información acerca de los ID únicos, consulte ID únicos en la Guía del usuario de IAM.

  La configuración con el IdP (en este caso, Azure AD) determina cómo se escribe la cláusula de condición. Si el correo electrónico de su empleado es `johndoe@example.com`, primero establezca `${redshift:DbUser}` en el supercampo que coincida con el nombre de usuario del empleado `johndoe`. A continuación, para que esta condición funcione, configure el campo `RoleSessionName` de SAML de AWS en el supercampo que concuerde con el email del empleado `johndoe@example.com`. Cuando tome este enfoque, tenga en cuenta lo siguiente:

- Si establece `${redshift:DbUser}` para que sea el correo electrónico del empleado, quite el `@example.com` en el archivo JSON de muestra para que coincida con el `RoleSessionName`.
- Si establece `RoleSessionId` para que solo sea el nombre de usuario del empleado, quite el `@example.com` en el ejemplo para que coincida con el `RoleSessionName`.
- En el JSON de ejemplo, `${redshift:DbUser}` y `RoleSessionName` se establecen en el correo electrónico del empleado. En este ejemplo, JSON utiliza el nombre de usuario de la base de datos de Amazon Redshift con `@example.com` para que el usuario inicie sesión y acceda al clúster.

- La segunda sección concede permiso para crear un nombre `dbuser` en el clúster especificado. En este JSON de muestra, restringe la creación a `${redshift:DbUser}`.
- La tercera sección concede permisos para especificar a qué `dbgroup` puede unirse un usuario. En este JSON de muestra, un usuario puede unirse al grupo `my_dbgroup` en el clúster especificado.
- La cuarta sección otorga permiso a las acciones que el usuario puede realizar en todos los recursos. En este JSON de ejemplo, se permite a los usuarios llamar a `redshift:DescribeClusters` para obtener información del clúster, como el punto de conexión del clúster, la región de AWS y el puerto. También permite a los usuarios llamar a `iam:ListRoles` para comprobar qué roles puede asumir un usuario.

Para configurar JDBC para la autenticación en Microsoft Azure AD

- Configure el cliente de la base de datos para conectarse al clúster a través de JDBC mediante el inicio de sesión único de Azure AD.

  Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de Azure AD o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.

  Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

a. Inicie SQL Workbench/J. En la página Select Connection Profile (Seleccionar perfil de conexión) agregue un Profile group (Grupo de perfiles) denominado **`AzureAuth`**.

b. En Connection Profile (Perfil de conexión), escriba **`Azure`**.

c. Elija Manage Drivers (Administrar controladores), y elija Amazon Redshift. Elija el icono Open folder (Abrir carpeta) junto a Library (Biblioteca) y a continuación, elija el archivo JDBC .jar adecuado.

d. En la página Select connection profile (Seleccionar perfil de conexión) agregue información al perfil de conexión de la siguiente manera:

- En User (Usuario), escriba su nombre de usuario de Microsoft Azure. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse.
- En Password (Contraseña), escriba la contraseña de Microsoft Azure.
- En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
- En URL, escriba **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`*.

e. Elija Extended properties (Propiedades extendidas) para agregar información adicional a las propiedades de conexión, como se describe a continuación.

Para la configuración de inicio de sesión único de Azure AD, agregue información adicional como se indica a continuación:

- En plugin_name, escriba **`com.amazon.redshift.plugin.AzureCredentialsProvider`**. Este valor especifica al controlador que debe utilizar el inicio de sesión único de Azure AD como método de autenticación.
- En idp_tenant, escriba ***`your-idp-tenant`***. Se utiliza solo para Microsoft Azure AD. Este es el nombre del arrendatario de su empresa configurado en Azure AD. Este valor puede ser el nombre del arrendatario o el ID único del inquilino con guiones.
- En client_secret, escriba ***`your-azure-redshift-application-client-secret`***. Se utiliza solo para Microsoft Azure AD. Este es el secreto de cliente de la aplicación de Amazon Redshift que creó cuando configuró el inicio de sesión único de Azure. Esto solo es aplicable al complemento com.amazon.redshift.plugin.AzureCredentialsProvider.

- En client_id, escriba ***your-azure-redshift-application-client-id***. Se utiliza solo para Microsoft Azure AD. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift que creó cuando configuró el inicio de sesión único de Azure.

Para la configuración de inicio de sesión único de Azure AD con MFA, agregue información adicional a las propiedades de conexión de la siguiente manera:

- En plugin_name, escriba **`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`**. Este valor le indica al controlador que debe utilizar el inicio de sesión único de Azure AD con MFA como método de autenticación.
- En idp_tenant, escriba ***your-idp-tenant***. Se utiliza solo para Microsoft Azure AD. Este es el nombre del arrendatario de su empresa configurado en Azure AD. Este valor puede ser el nombre del arrendatario o el ID único del inquilino con guiones.
- En client_id, escriba ***your-azure-redshift-application-client-id***. Esta opción se utiliza solo para Microsoft Azure AD. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift que creó al configurar el inicio de sesión único de Azure AD con MFA.
- En listen_port, escriba ***your-listen-port***. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890.
- En idp_response_timeout, escriba ***the-number-of-seconds***. Este es el número de segundos que se deben esperar antes de que el servidor IdP devuelva una respuesta. El número mínimo de segundos debe ser 10. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión.

Para configurar ODBC para la autenticación en Microsoft Azure AD

- Configure el cliente de base de datos para que se conecte al clúster a través de ODBC mediante el inicio de sesión único de Azure AD.

  Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y MacOS. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

También instale y configure el controlador ODBC de Amazon Redshift más reciente para su sistema operativo según se indica a continuación:

- Para Windows, vea Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.
- Para macOS, consulte Instalación del controlador ODBC de Amazon Redshift en macOS X.
- Para Linux, vea Instalación del controlador ODBC de Amazon Redshift en Linux.

En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba ***your-DSN***. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- En Auth type (Tipo de autenticación) para la configuración de inicio de sesión único de Azure AD, seleccione **`Identity Provider: Azure AD`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Azure.
- En Auth type (Tipo de autenticación) para la configuración de inicio de sesión único de Azure AD con MFA, seleccione **`Identity Provider: Browser Azure AD`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticarse mediante el inicio de sesión único de Azure con MFA.
- En Cluster ID (ID de clúster), escriba ***your-cluster-identifier***.
- En Region (Región), escriba ***your-cluster-region***.
- En Database (Base de datos), escriba ***your-database-name***.
- En User (Usuario), escriba ***your-azure-username***. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Utilice esto solo para Auth Type (Tipo de autorización) es Identity Provider: Azure AD (Proveedor de identidades: Azure AD).
- En Password (Contraseña), escriba ***your-azure-password***. Utilice esto solo para Auth Type (Tipo de autorización) es Identity Provider: Azure AD (Proveedor de identidades: Azure AD).
- En IdP Tenant (Arrendatario de IdP), escriba ***your-idp-tenant***. Este es el nombre del arrendatario de su empresa configurado en su IdP (Azure). Este valor puede ser el nombre del arrendatario o el ID único del inquilino con guiones.

- En Azure Client Secret (Secreto de cliente de Azure), escriba ***your-azure-redshift-application-client-secret***. Este es el secreto de cliente de la aplicación de Amazon Redshift que creó cuando configuró el inicio de sesión único de Azure.
- En Azure Client ID (ID de cliente de Azure), escriba ***your-azure-redshift-application-client-id***. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift que creó cuando configuró el inicio de sesión único de Azure.
- En Puerto de escucha, escriba ***your-listen-port***. Este es el puerto de escucha predeterminado en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento Browser Azure AD.
- En Response Timeout (Tiempo de espera de respuesta), escriba ***the-number-of-seconds***. Este es el número de segundos que se deben esperar antes de que el servidor IdP devuelva una respuesta. El número mínimo de segundos debe ser 10. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión. Esta opción solo se aplica al complemento Browser Azure AD.

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

> **Note**
>
> Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba ***your-cluster-identifier***. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba ***your-cluster-region***. Esta es la región de AWS del clúster de Amazon Redshift creado.
- En database, escriba ***your-database-name***. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **`en-us`**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **`1`**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En nombre_complemento para la configuración de inicio de sesión único de Azure AD, introduzca**`AzureAD`**. Esto especifica al controlador que debe utilizar el inicio de sesión único de Azure como método de autenticación.

- En nombre_complemento para la configuración de inicio de sesión único de Azure AD con MFA, introduzca **`BrowserAzureAD`**. Esto especifica al controlador que debe utilizar el inicio de sesión único de Azure con MFA como método de autenticación.
- En uid, escriba ***`your-azure-username`***. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Utilice esto solo para plugin_name es AzureAD.
- En pwd, escriba ***`your-azure-password`***. Utilice esto solo para plugin_name es AzureAD.
- En idp_tenant, escriba ***`your-idp-tenant`***. Este es el nombre del arrendatario de su empresa configurado en su IdP (Azure). Este valor puede ser el nombre del arrendatario o el ID único del inquilino con guiones.
- En client_secret, escriba ***`your-azure-redshift-application-client-secret`***. Este es el secreto de cliente de la aplicación de Amazon Redshift que creó cuando configuró el inicio de sesión único de Azure.
- En client_id, escriba ***`your-azure-redshift-application-client-id`***. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift que creó cuando configuró el inicio de sesión único de Azure.
- En listen_port, escriba ***`your-listen-port`***. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto se aplica al complemento Browser Azure AD.
- En idp_response_timeout, escriba ***`the-number-of-seconds`***. Este es el periodo de tiempo especificado en segundos que esperar la respuesta de Azure. Esta opción se aplica al complemento Browser Azure AD.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Para solucionar problemas con el complemento Azure AD de navegador

1. Para utilizar el complemento Azure AD de navegador, debe establecer la URL de respuesta especificada en la solicitud para que coincida con la URL de respuesta configurada para la aplicación.

Vaya a la página Configurar el inicio de sesión único con SAML en el portal de Microsoft Azure. A continuación, compruebe que la URL de respuesta está establecida en http://localhost/redshift/.

2. Si aparece un error de inquilino de IdP, compruebe que el nombre de Inquilino de IdP coincide con el nombre de dominio que utilizó inicialmente para configurar Active Directory en Microsoft Azure.

   En Windows, vaya a la sección Connection Settings (Configuración de conexión) de la página Amazon Redshift ODBC DSN Setup (Configuración de DSN de ODBC de Amazon Redshift). A continuación, compruebe que el nombre de inquilino de su empresa configurado en su IdP (Azure) coincide con el nombre de dominio que utilizó inicialmente para configurar Active Directory en Microsoft Azure.

   En macOS y Linux, busque el archivo odbc.ini. A continuación, compruebe que el nombre de inquilino de su empresa configurado en su IdP (Azure) coincide con el nombre de dominio que utilizó inicialmente para configurar Active Directory en Microsoft Azure.

3. Si aparece un error que indica que la URL de respuesta especificada en la solicitud no coincide con las URL de respuesta configuradas para la aplicación, verifique que los URI de redirección son los mismos que la URL de respuesta.

   Vaya a la página Registro de aplicaciones de su aplicación en el portal de Microsoft Azure. A continuación, compruebe que los URI de redirección coinciden con la URL de respuesta.

4. Si obtiene la respuesta inesperada de error no autorizado, verifique que haya completado la configuración de Aplicaciones móviles y de escritorio.

   Vaya a la página Registro de aplicaciones de su aplicación en el portal de Microsoft Azure. A continuación, vaya a Autenticación y compruebe que ha configurado Aplicaciones móviles y de escritorio para utilizar http://localhost/redshift/ como URI de redirección.

Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con AD FS

Puede utilizar AD FS como proveedor de identidad (IdP) para acceder al clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin. Para obtener más información acerca de cómo configurar AWS como proveedor de servicios para AD FS, consulte Configuración de una relación de confianza para usuario autenticado y agregación de reclamaciones en el proveedor de identidades SAML 2.0 en la Guía del usuario de IAM.

Para configurar AD FS y su cuenta de AWS para establecer una relación de confianza entre ellas

1. Cree o utilice un clúster de Amazon Redshift existente para que los usuarios de AD FS se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte Creating a Cluster (Creación de un clúster).
2. Configure AD FS para controlar el acceso de Amazon Redshift en la consola de administración de Microsoft Management:

    1. Elija ADFS 2.0, y, a continuación, elija Add Relying Party Trust (Agregar confianza de parte de confianza). En la página Add Relying Party Trust Wizard (Asistente para agregar confianza de parte), elija Start (Inicio).
    2. En la página Select Data Source (Seleccionar origen de datos), elija Import data about the relying party published online or on a local network (Importar los datos sobre el usuario de confianza publicado en línea o en una red local).
    3. En Federation metadata address (host name or URL) (Dirección de metadatos de federación [nombre de host o URL]), escriba **`https://signin.aws.amazon.com/saml-metadata.xml`**. El archivo XML de metadatos es un documento de metadatos SAML estándar que describe a AWS como parte de confianza.
    4. En la página Specify Display Name (Especificar nombre para mostrar), escriba un valor para Display name (Nombre para mostrar).
    5. En la página Choose Issuance Authorization Rules (Elegir reglas de autorización de emisión), elija una regla de autorización de emisión para permitir o denegar a todos los autores que accedan a esta parte de confianza.
    6. En la página Ready to Add Trust (Listo para agregar confianza), revise la configuración.
    7. En la página Finish (Finalizar), elija Open the Edit Claim Rules dialog for this relying party trust when the wizard closes (Abrir el cuadro de diálogo Editar reglas de reclamación para esta relación de confianza para usuarios autenticado al cerrarse el asistente).
    8. En el menú contextual (clic con el botón derecho), elija Relying Party Trusts (Relaciones de confianza para usuario autenticado).
    9. Para el usuario autenticado, abra el menú contextual (haga clic con el botón derecho) y elija Edita Claim Rules (Editar reglas de reclamación). En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla).

10. En Claim rule template (Plantilla de regla de reclamación), elija Transform an Incoming Claim (Transformar una reclamación entrante) y, a continuación, en la página Edit Rule – NameId (Editar regla – NameId), haga lo siguiente:
    - En Claim rule name (Nombre de regla de reclamación), escriba NameId.
    - En Incoming claim name (Nombre de reclamación entrante), elija Windows Account Name (Nombre de cuenta de Windows).
    - En Outgoing claim name (Nombre de reclamación saliente), elija Name ID (ID de nombre).
    - En Outgoing name ID format (Formato de ID de nombre saliente), elija Persistent Identifier (Identificador persistente).
    - Elija Pass through all claim values (Acceso directo a todos los valores de reclamación).
11. En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla). En la página Select Rule Template (Seleccionar plantilla de regla), en Claim rule template (Plantilla de regla de reclamación), elija Send LDAP Attributes as Claims (Enviar atributos LDAP como reclamaciones).
12. En la página Configure Rule (Configurar regla), haga lo siguiente:
    - En Claim rule name (Nombre de regla de reclamación), escriba RoleSessionName.
    - En Attribute store (Almacén de atributos), elija Active Directory.
    - En LDAP Attribute (Atributo LDAP), elija Email Addresses (Direcciones de correo electrónico).
    - En Outgoing Claim Type (Tipo de reclamación saliente), elija https://aws.amazon.com/SAML/Attributes/RoleSessionName.
13. En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla). En la página Select Rule Template (Seleccionar plantilla de regla), para Claim rule template (Plantilla de regla de reclamación), elija Send Claims Using a Custom Rule (Enviar reclamaciones utilizando una regla personalizada).
14. En la página Edit Rule – Get AD Groups (Editar regla –Obtener grupos de AD), en Claim rule name (Nombre de regla de reclamación), escriba Get AD Groups (Obtener grupos de AD).
15. En Custom rule (Regla personalizada), escriba lo siguiente.

```
c:[Type ==
                                    "http://schemas.microsoft.com/ws/2008/06/
identity/claims/windowsaccountname",
                                    Issuer == "AD AUTHORITY"] => add(store =
 "Active Directory",
```

```
                                        types = ("http://temp/variable"), query =
 ";tokenGroups;{0}",
                                        param = c.Value);
```

16. En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla). En la página Select Rule Template (Seleccionar plantilla de regla), para Claim rule template (Plantilla de regla de reclamación), elija Send Claims Using a Custom Rule (Enviar reclamaciones utilizando una regla personalizada).
17. En la página Edit Rule – Roles (Editar regla – Roles), en Claim rule name (Nombre de regla de reclamación), escriba Roles.
18. En Custom rule (Regla personalizada), escriba lo siguiente.

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-"] =>
 issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-", "arn:aws:iam::123456789012:saml-provider/
ADFS,arn:aws:iam::123456789012:role/ADFS-"));
```

Tenga en cuenta los ARN del proveedor SAML y el rol que se van a asumir. En este ejemplo, `arn:aws:iam:123456789012:saml-provider/ADFS` es el ARN del proveedor SAML y `arn:aws:iam:123456789012:role/ADFS-` es el ARN del rol.

3. Asegúrese de haber descargado el archivo `federationmetadata.xml`. Compruebe que el contenido del documento no tenga caracteres no válidos. Este es el archivo de metadatos que utiliza al configurar la relación de confianza con AWS.
4. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Azure Enterprise Application. Para obtener información detallada sobre los pasos, consulte Creación y administración de un proveedor de identidad de IAM (Consola) en la Guía del usuario de IAM.
5. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de un rol para SAML en la Guía del usuario de IAM.
6. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de políticas de IAM (Consola) en la Guía del usuario de IAM. Para ver un ejemplo de Azure AD, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD.

Para configurar JDBC para la autenticación en AD FS

- Configure el cliente de la base de datos para conectarse al clúster a través de JDBC mediante el inicio de sesión único de AD FS.

  Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de AD FS o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.

  Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

  a. Inicie SQL Workbench/J. En la página Select Connection Profile (Seleccionar perfil de conexión), agregue un Profile Group (Grupo de perfil); por ejemplo, **ADFS**.

  b. En Connection Profile (Perfil de conexión), escriba el nombre de perfil de su conexión; por ejemplo **ADFS**.

  c. Elija Manage Drivers (Administrar controladores), y elija Amazon Redshift. Elija el icono Open folder (Abrir carpeta) junto a Library (Biblioteca) y a continuación, elija el archivo JDBC .jar adecuado.

  d. En la página Select connection profile (Seleccionar perfil de conexión) agregue información al perfil de conexión de la siguiente manera:

     - En User (Usuario), escriba su nombre de usuario de AD FS. Este es el nombre de usuario de la cuenta de que está utilizando para el inicio de sesión único que tiene permisos en el clúster en el que está intentando autenticarse.
     - En Password (Contraseña), escriba su contraseña de AD FS.
     - En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
     - En URL, escriba **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.

  e. Elija Extended Properties (Propiedades extendidas). En plugin_name, escriba **com.amazon.redshift.plugin.AdfsCredentialsProvider**. Este valor especifica

al controlador que debe utilizar el inicio de sesión único de Azure AD como método de autenticación.

Para configurar ODBC para la autenticación en AD FS

- Configure el cliente de la base de datos para conectarse al clúster a través de ODBC mediante el inicio de sesión único de AD FS.

  Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y MacOS. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

  También instale y configure el controlador ODBC de Amazon Redshift más reciente para su sistema operativo según se indica a continuación:

  - Para Windows, vea Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.
  - Para macOS, consulte Instalación del controlador ODBC de Amazon Redshift en macOS X.
  - Para Linux, vea Instalación del controlador ODBC de Amazon Redshift en Linux.

  En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

  - En Data Source Name (Nombre de origen de datos), escriba ***your-DSN***. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
  - Para Auth type (Tipo de autenticación), elija Identity Provider: SAML (Proveedor de identidades: SAML). Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de AD FS.
  - En Cluster ID (ID de clúster), escriba ***your-cluster-identifier***.
  - En Region (Región), escriba ***your-cluster-region***.
  - En Database (Base de datos), escriba ***your-database-name***.
  - En User (Usuario), escriba ***your-adfs-username***. Este es el nombre de usuario de la cuenta de AD FS que está utilizando para el inicio de sesión único que tiene permiso para

el clúster con el que está intentando autenticarse. Utilice esto solo para Auth type (Tipo de autorización) es Identity Provider: SAML (Proveedor de identidades: SAML).

- En Password (Contraseña), escriba ***your-adfs-password***. Utilice esto solo para Auth type (Tipo de autorización) es Identity Provider: SAML (Proveedor de identidades: SAML).

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

> **Note**
>
> Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba ***your-cluster-identifier***. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba ***your-cluster-region***. Esta es la región de AWS del clúster de Amazon Redshift creado.
- En database, escriba ***your-database-name***. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **`en-us`**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **`1`**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En plugin_name, realice una de las operaciones siguientes:
  - Para la configuración de inicio de sesión único de AD FS con MFA, introduzca **`BrowserSAML`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar en AD FS.
  - Para la configuración de inicio de sesión único de AD FS, introduzca **`ADFS`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Azure AD.
- En uid, escriba ***your-adfs-username***. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Utilice esto solo para plugin_name es ADFS.
- En pwd, escriba ***your-adfs-password***. Utilice esto solo para plugin_name es ADFS.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Ping Identity

Puede utilizar Ping Identity como proveedor de identidades (IdP) para acceder a su clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin mediante el portal de PingOne. Para obtener más información acerca de cómo configurar AWS como proveedor de servicios para Ping Identity, consulte Configuración de una relación de confianza para usuario autenticado y agregación de reclamaciones en el proveedor de identidades SAML 2.0 en la Guía del usuario de IAM.

Para establecer una relación de confianza entre Ping Identity y su cuenta de AWS

1. Cree o use un clúster de Amazon Redshift existente para que los usuarios de Ping Identity se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte Creating a Cluster (Creación de un clúster).
2. Agregue Amazon Redshift como una nueva aplicación SAML en el portal de PingOne. Para obtener información detallada sobre los pasos, consulte la documentación de Ping Identity.
    1. Vaya a My Applications (Mis aplicaciones).
    2. En Add Application (Agregar aplicación), elija New SAML Application (Nueva aplicación SAML).
    3. En Application name (Nombre de la application), escriba **`Amazon Redshift`**.
    4. En Protocol Version (Versión de protocolo), elija SAML v2.0.
    5. En Category (Categoría), elija ***`your-application-category`***.
    6. En Assertion Consumer Service (ACS), escriba ***`your-redshift-local-host-url`***. Éste es el host local y el puerto al que redirige la aserción SAML.
    7. En Entity ID (ID de entidad), escriba `urn:amazon:webservices`.

8. En Signing (Firma), elija Sign Assertion (Aserción de firma).
9. En la sección SSO Attribute Mapping (Mapeo de atributos de SSO), cree las reclamaciones como se muestra en la tabla siguiente.

Atributo de aplicación	Atributo de puente de identidad de valor literal
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam::*123456789012* :role/*Ping*,arn:aws:iam::*123456789012* :saml-provider/*PingProvider*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbUser	email
https://redshift.amazon.com/SAML/Attributes/DbGroups	Los grupos en los atributos “DbGroups ” contienen el prefijo @directory. Para eliminar esto, en Identity bridge (Puente de identidad), ingrese memberOf. En Function (Función), elija ExtractByRegularExpression. En Expression (Expresión), escriba (.*)[\@](?:.*).

3. En Group Access (Acceso de grupo), configure el acceso de grupo siguiente en caso necesario:
   - https://aws.amazon.com/SAML/Attributes/Role
   - https://aws.amazon.com/SAML/Attributes/RoleSessionName
   - https://redshift.amazon.com/SAML/Attributes/AutoCreate
   - https://redshift.amazon.com/SAML/Attributes/DbUser
4. Revise la configuración y realice cambios, si es necesario.
5. Utilice la Initiate Single Sign-On (SSO) URL ((URL iniciar inicio de sesión único (SSO)) como URL de inicio de sesión para el complemento Browser SAML.

6. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Ping Identity. Para obtener información detallada sobre los pasos, consulte Creación y administración de un proveedor de identidad de IAM (Consola) en la Guía del usuario de IAM.
7. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de un rol para SAML en la Guía del usuario de IAM.
8. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de políticas de IAM (Consola) en la Guía del usuario de IAM. Para ver un ejemplo de Azure AD, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD.

Para configurar JDBC para autenticación en Ping Identity

- Configure el cliente de base de datos para que se conecte al clúster a través de JDBC mediante el inicio de sesión único de Ping Identity.

  Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de Ping Identity o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.

  Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

  a. Inicie SQL Workbench/J. En la página Select Connection Profile (Seleccionar perfil de conexión), agregue un Profile Group (Grupo de perfil); por ejemplo, **`Ping`**.
  b. En Connection Profile (Perfil de conexión), escriba ***`your-connection-profile-name`***; por ejemplo **`Ping`**.
  c. Elija Manage Drivers (Administrar controladores), y elija Amazon Redshift. Elija el icono Open folder (Abrir carpeta) junto a Library (Biblioteca) y a continuación, elija el archivo JDBC .jar adecuado.

d. En la página Select connection profile (Seleccionar perfil de conexión) agregue información al perfil de conexión de la siguiente manera:

   - En User (Usuario), especifique el nombre de usuario de PingOne. Este es el nombre de usuario de la cuenta de PingOne que está utilizando con el inicio de sesión único que tiene permisos para el clúster en el que está intentando autenticarse.
   - En Password (Contraseña), escriba la contraseña de PingOne.
   - En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
   - En URL, escriba **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.

e. Elija Extended Properties (Propiedades extendidas) y realice una de las acciones siguientes:

   - En login_url, escriba ***your-ping-sso-login-url***. Este valor especifica la dirección URL que va a utilizar el inicio de sesión único como autenticación al iniciar sesión.
   - Para Ping Identity, en nombre_complemento, escriba **com.amazon.redshift.plugin.PingCredentialsProvider**. Este valor especifica al controlador que debe utilizar el inicio de sesión único de Ping Identity como método de autenticación.
   - Para el inicio de sesión único en Ping Identity, en nombre_complemento, escriba **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**. Este valor especifica al controlador que debe utilizar el inicio de sesión único de PingOne para Ping Identity como método de autenticación.

Para configurar ODBC para la autenticación en Ping Identity

- Configure el cliente de la base de datos para que se conecte al clúster a través de ODBC utilizando el inicio de sesión único de PingOne para Ping Identity.

  Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y MacOS. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

  También instale y configure el controlador ODBC de Amazon Redshift más reciente para su sistema operativo según se indica a continuación:

- Para Windows, vea Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.
- Para macOS, consulte Instalación del controlador ODBC de Amazon Redshift en macOS X.
- Para Linux, vea Instalación del controlador ODBC de Amazon Redshift en Linux.

En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba ***your-DSN***. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- En Auth Type (Tipo de autenticación), realice una de las operaciones siguientes:
  - Para la configuración de Ping Identity, elija Proveedor de identidad: Ping Federate. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante inicio de sesión único Ping Identity.
  - Para la configuración de Ping Identity con inicio de sesión único, elija Identity Provider: Browser SAML (Proveedor de identidades: Browser SAML). Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante Ping Identity con inicio de sesión único.
- En Cluster ID (ID de clúster), escriba ***your-cluster-identifier***.
- En Region (Región), escriba ***your-cluster-region***.
- En Database (Base de datos), escriba ***your-database-name***.
- En User (Usuario), escriba ***your-ping-username***. Este es el nombre de usuario de la cuenta de PingOne que está utilizando con el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Utilice esto solo para el Auth type (Tipo de autenticación) es Identity Provider: PingFederate (Proveedor de identidad: PingFederate).
- En Password (Contraseña), escriba ***your-ping-password***. Utilice esto solo para el Auth type (Tipo de autenticación) es Identity Provider: PingFederate (Proveedor de identidad: PingFederate).
- En Puerto de escucha, escriba ***your-listen-port***. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento SAML del navegador.

- En Response Timeout (Tiempo de espera de respuesta), escriba ***the-number-of-seconds***. Este es el número de segundos que se deben esperar antes de que el servidor IdP devuelva una respuesta. El número mínimo de segundos debe ser 10. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión. Esto solo se aplica al complemento SAML del navegador.
- En Login URL (URL de inicio de sesión), escriba ***your-login-url***. Esto solo se aplica al complemento SAML del navegador.

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

> **Note**
>
> Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba ***your-cluster-identifier***. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba ***your-cluster-region***. Esta es la región de AWS del clúster de Amazon Redshift creado.
- En database, escriba ***your-database-name***. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **`en-us`**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **`1`**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En plugin_name, realice una de las operaciones siguientes:
  - Para la configuración de Ping Identity, escriba **`BrowserSAML`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar con Ping Identity.
  - Para la configuración de Ping Identity con inicio de sesión único, introduzca **`Ping`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante Ping Identity con inicio de sesión único.
- En uid, escriba ***your-ping-username***. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Utilice esto solo para plugin_name es Ping.
- En pwd, escriba ***your-ping-password***. Utilice esto solo para plugin_name es Ping.

- En login_url, escriba ***your-login-url***. Esta es la URL de inicio de inicio de sesión único que devuelve la respuesta SAML. Esto solo se aplica al complemento SAML del navegador.
- En idp_response_timeout, escriba ***the-number-of-seconds***. Este es el periodo de tiempo especificado en segundos que se va a esperar a que PingOne Identity responda. Esto solo se aplica al complemento SAML del navegador.
- En listen_port, escriba ***your-listen-port***. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento SAML del navegador.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con Okta

Puede utilizar Okta como proveedor de identidades (IdP) para acceder a su clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin. Para obtener más información acerca de cómo configurar AWS como proveedor de servicios para Okta, consulte Configuración de una relación de confianza para usuario autenticado y agregación de reclamaciones en el proveedor de identidades SAML 2.0 en la Guía del usuario de IAM.

Para configurar Okta y su cuenta de AWS para establecer una relación de confianza entre ellas

1. Cree o utilice un clúster de Amazon Redshift existente para que los usuarios de Okta se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte Creating a Cluster (Creación de un clúster).
2. Agregue Amazon Redshift como una nueva aplicación en el portal de Okta. Para ver los pasos detallados, consulte la documentación de Okta.

   - Elija Add Application (Agregar aplicación).
   - En Add Application (Agregar aplicación), elija Create New App (Crear nueva aplicación).

- En la página Create a New Add Application Integration (Crear una nueva integración Agregar aplicación), en Platform (Plataforma), elija Web.
- En Sign on method (Método de inicio de sesión), elija SAML v2.0.
- En la página General Settings (Configuración general), en App name (Nombre de la aplicación), escriba ***your-redshift-saml-sso-name***. Se trata del nombre de la aplicación.
- En la página Configuración de SAML, en URL de inicio de sesión único, escriba ***your-redshift-local-host-url***. Este es el alojamiento local y el puerto al que redirige la aserción SAML; por ejemplo, `http://localhost:7890/redshift/`.

3. Utilice el valor de Single sign on URL (URL de inicio de sesión único) como Recipient URL (URL de destinatario) y Destination URL (URL de destino).
4. En Signing (Firma), elija Sign Assertion (Aserción de firma).
5. En Audience URI (SP Entity ID) (URI de audiencia [ID entidad SP]), ingrese **`urn:amazon:webservices`** para las reclamaciones, como se muestra en la siguiente tabla.
6. En la sección Advanced Settings (Configuración avanzada), en SAML Issuer ID (ID de emisor SAML), ingrese ***your-Identity-Provider-Issuer-ID***, que puede encontrar en la sección View Setup Instructions (Ver instrucciones de configuración).
7. En la sección Attribute Statements (Declaraciones de atributos), cree las reclamaciones como se muestra en la tabla siguiente.

Nombre de la reclamación	Valor
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam::*123456789012* :role/*Okta*,arn:aws:iam::*123456789012* :saml-provider/*Okta*
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbUser	user.email

8. En la sección App Embed Link (Enlace de inserción de aplicaciones), busque la URL que quiere usar como URL de inicio de sesión con el complemento Browser SAML.

9. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Okta. Para obtener información detallada sobre los pasos, consulte Creación y administración de un proveedor de identidad de IAM (Consola) en la Guía del usuario de IAM.
10. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de un rol para SAML en la Guía del usuario de IAM.
11. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para obtener información detallada sobre los pasos, consulte Creación de políticas de IAM (Consola) en la Guía del usuario de IAM. Para ver un ejemplo de Azure AD, consulte Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD.

Para configurar JDBC para la autenticación en Okta

- Configure el cliente de la base de datos para conectarse al clúster a través de JDBC mediante el inicio de sesión único de Okta.

  Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de Okta o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte Configuración de una conexión del controlador JDBC versión 2.1 para Amazon Redshift.

  Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

  ```
  jdbc:redshift:iam://cluster-identifier:us-west-1/dev
  ```

  Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

  a. Inicie SQL Workbench/J. En la página Select Connection Profile (Seleccionar perfil de conexión), agregue un Profile Group (Grupo de perfil); por ejemplo, **`Okta`**.
  b. En Connection Profile (Perfil de conexión), escriba ***`your-connection-profile-name`***; por ejemplo **`Okta`**.
  c. Elija Manage Drivers (Administrar controladores), y elija Amazon Redshift. Elija el icono Open folder (Abrir carpeta) junto a Library (Biblioteca) y a continuación, elija el archivo JDBC .jar adecuado.

d. En la página Select connection profile (Seleccionar perfil de conexión) agregue información al perfil de conexión de la siguiente manera:

   - Para User (Usuario), escriba su nombre de usuario de Okta. Este es el nombre de usuario de la cuenta de Okta que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse.
   - En Password (Contraseña), escriba su contraseña de Okta.
   - En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
   - En URL, escriba **`jdbc:redshift:iam://`*`your-cluster-identifier`*`:`*`your-cluster-region`*`/`*`your-database-name`*.

e. Elija Extended Properties (Propiedades extendidas) y realice una de las acciones siguientes:

   - En login_url, escriba ***`your-okta-sso-login-url`***. Este valor especifica la dirección URL que va a utilizar el inicio de sesión único como autenticación al iniciar sesión en Okta.
   - Para el inicio de sesión único de Okta, en nombre_complemento, introduzca **`com.amazon.redshift.plugin.OktaCredentialsProvider`**. Este valor especifica al controlador que debe utilizar el inicio de sesión único de Okta como método de autenticación.
   - Para el inicio de sesión único de Okta con MFA, en nombre_complemento, introduzca **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**. Este valor le indica al controlador que debe utilizar el inicio de sesión único de Okta con MFA como método de autenticación.

Para configurar ODBC para la autenticación en Okta

- Configure el cliente de la base de datos para conectarse al clúster a través de ODBC mediante el inicio de sesión único de Okta.

  Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y MacOS. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

También instale y configure el controlador ODBC de Amazon Redshift más reciente para su sistema operativo según se indica a continuación:

- Para Windows, vea Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.
- Para macOS, consulte Instalación del controlador ODBC de Amazon Redshift en macOS X.
- Para Linux, vea Instalación del controlador ODBC de Amazon Redshift en Linux.

En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba ***your-DSN***. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- En Auth Type (Tipo de autenticación), realice una de las operaciones siguientes:
  - Para la configuración del inicio de sesión único de Okta, elija **`Identity Provider: Okta`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Okta.
  - Para la configuración del inicio de sesión único de Okta con MFA, elija **`Identity Provider: Browser SAML`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticarse mediante el inicio de sesión único de Okta con MFA.
- En Cluster ID (ID de clúster), escriba ***your-cluster-identifier***.
- En Region (Región), escriba ***your-cluster-region***.
- En Database (Base de datos), escriba ***your-database-name***.
- En User (Usuario), escriba ***your-okta-username***. Este es el nombre de usuario de la cuenta de Okta que está utilizando para el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Utilice esto solo si Auth type (Tipo de autorización) es Identity Provider: Okta (Proveedor de identidades: Okta).
- En Password (Contraseña), escriba ***your-okta-password***. Utilice esto solo si Auth type (Tipo de autorización) es Identity Provider: Okta (Proveedor de identidades: Okta).

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

> **Note**
>
> Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba ***your-cluster-identifier***. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba ***your-cluster-region***. Esta es la región de AWS del clúster de Amazon Redshift creado.
- En database, escriba ***your-database-name***. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **en-us**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **1**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En plugin_name, realice una de las operaciones siguientes:
  - Para la configuración de inicio de sesión único de Okta con MFA, introduzca **BrowserSAML**. Este es el método de autenticación que utiliza el controlador ODBC para autenticarse mediante el inicio de sesión único de Okta con MFA.
  - Para la configuración del inicio de sesión único de Okta, introduzca **Okta**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Okta.
- En uid, escriba ***your-okta-username***. Este es el nombre de usuario de la cuenta de Okta que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Use esto solo para plugin_name es Okta.
- En pwd, escriba ***your-okta-password***. Use esto solo para plugin_name es Okta.
- En login_url, escriba ***your-login-url***. Esta es la URL de inicio de inicio de sesión único que devuelve la respuesta SAML. Esto solo se aplica al complemento SAML del navegador.
- En idp_response_timeout, escriba ***the-number-of-seconds***. Este es el periodo de tiempo especificado en segundos que se va a esperar a que PingOne responda. Esto solo se aplica al complemento SAML del navegador.
- En listen_port, escriba ***your-listen-port***. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento SAML del navegador.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos

Para usar el controlador JDBC u ODBC de Amazon Redshift para crear credenciales de usuario de base de datos, proporcione el nombre de usuario de base de datos como una opción de JDBC u ODBC. Si lo desea, puede hacer que el controlador cree un nuevo usuario de base de datos si no existe ninguno y puede especificar una lista de grupos de usuarios de base de datos a los que se une el usuario cuando inicia sesión.

Si usa un proveedor de identidad (IdP), póngase en contacto con el administrador de su IdP para determinar los valores correctos para estas opciones. El administrador de su IdP también puede configurar su IdP para proporcionar estas opciones, en cuyo caso no necesita proporcionarlas como opciones de JDBC u ODBC. Para obtener más información, consulte Configuración de aserciones SAML para el IdP.

> **Note**
>
> Si utiliza una variable de política de IAM `${redshift:DbUser}`, como se describe en Políticas de recursos de GetClusterCredentials, el valor de `DbUser` se sustituye por el valor obtenido por el contexto de la solicitud de la operación de la API. Los controladores de Amazon Redshift utilizan el valor de la variable `DbUser` proporcionado por la URL de conexión en lugar del valor proporcionado como atributo SAML.
> Para ayudar a proteger esta configuración, recomendamos que utilice una condición en una política de IAM para validar el valor de `DbUser` con el `RoleSessionName`. Puede encontrar ejemplos de cómo establecer una condición utilizando una política de IAM en Política de ejemplo para usar GetClusterCredentials.

En la tabla siguiente se indican las opciones para crear credenciales de usuario de base de datos.

Opción	Descripción
DbUser	El nombre de un usuario de base de datos. Si un usuario llamado DbUser existe en la base de datos, las credenciales temporales del usuario tienen los mismos permisos que el usuario existente. Si DbUser no existe en la base de datos y AutoCreate está establecido en true, se crea un nuevo usuario llamado DbUser. Si lo desea, deshabilite la contraseña de un usuario existente. Para obtener más información, consulte ALTER_USER.
AutoCreate	Establezca esta opción en `true` para crear un usuario de base de datos con el nombre especificado para DbUser si no existe ninguno. El valor predeterminado es false.
`DbGroups`	Una lista delimitada por comas de los nombres de uno o varios grupos de usuarios de base de datos a los que se une el usuario de base de datos durante la sesión actual. De forma predeterminada, el nuevo usuario se agrega solamente a PUBLIC.

Generación de credenciales de base de datos para una identidad de IAM mediante la CLI o la API de Amazon Redshift

Para generar credenciales temporales de usuario de base de datos mediante programación, Amazon Redshift proporciona el comando get-cluster-credentials para la AWS Command Line Interface (AWS CLI) y la operación de la API GetClusterCredentials. También puede configurar su cliente SQL con controladores JDBC u ODBC de Amazon Redshift que administren el proceso de llamar a la operación `GetClusterCredentials`, recuperar las credenciales de usuario de base de datos y establecer una conexión entre su cliente SQL y la base de datos de Amazon Redshift. Para obtener más información, consulte Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos.

> **Note**
>
> Recomendamos el uso de controladores JDBC u ODBC de Amazon Redshift para generar credenciales de usuario de base de datos.

En esta sección, encontrará los pasos para llamar mediante programación a la operación `GetClusterCredentials` o el comando get-cluster-credentials, recuperar las credenciales de usuario de base de datos y conectarse a la base de datos.

Para generar y usar credenciales temporales de base de datos

1. Cree o modifique un usuario o rol con los permisos necesarios. Para obtener más información sobre los permisos de IAM, consulte Crear un rol de IAM con permisos para llamar a GetClusterCredentials.
2. Como el usuario o el rol que autorizó en el paso anterior, ejecute el comando de la CLI get-cluster-credentials o llame a la operación de la API `GetClusterCredentials` y proporcione los siguientes valores:

   - Identificador del clúster: nombre del clúster que contiene la base de datos.
   - Nombre de usuario de base de datos: nombre de un usuario de base de datos nuevo o existente.
     - Si el usuario no existe en la base de datos y AutoCreate está establecido en true, se crea un nuevo usuario con la contraseña deshabilitada.
     - Si el usuario no existe y AutoCreate está establecido en false, la solicitud produce un error.
     - En este ejemplo, el nombre de usuario de base de datos es `temp_creds_user`.
   - Creación automática (opcional): crea un usuario nuevo si el nombre de usuario de base de datos no existe.
   - Nombre de base de datos (opcional): nombre de la base de datos en la que el usuario tiene autorización para iniciar sesión. Si no se especifica el nombre de la base de datos, el usuario puede iniciar sesión en cualquier base de datos del clúster.
   - Grupos de bases de datos (opcional): lista de grupos de usuarios de bases de datos existentes. Tras iniciar sesión correctamente, el usuario de base de datos se agrega a los grupos de usuarios especificados. Si no se especifica ningún grupo, el usuario sólo tiene permisos PUBLIC. Los nombres de los grupos de usuarios deben coincidir con los ARN de los recursos de dbgroup especificados en la política de IAM asociada al usuario o rol.
   - Fecha de vencimiento (opcional): fecha de vencimiento, en segundos, de las credenciales temporales. Puede especificar un valor comprendido entre 900 segundos (15 minutos) y 3 600 segundos (60 minutos). El valor predeterminado es de 900 segundos.
3. Amazon Redshift verifica que el usuario tenga permiso para llamar a la operación `GetClusterCredentials` con los recursos especificados.

4. Amazon Redshift devuelve una contraseña temporal y el nombre de usuario de la base de datos.

   En el siguiente ejemplo, se utiliza la CLI de Amazon Redshift para generar credenciales temporales de base de datos para un usuario existente denominado `temp_creds_user`.

   ```
   aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
    temp_creds_user --db-name exampledb --duration-seconds 3600
   ```

   El resultado es el siguiente.

   ```
   {
     "DbUser": "IAM:temp_creds_user",
     "Expiration": "2016-12-08T21:12:53Z",
     "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
   gqX2Eeaq6P3DgTzgPg=="
   }
   ```

   En el siguiente ejemplo, se utiliza la CLI de Amazon Redshift para crear automáticamente credenciales temporales de base de datos para un usuario nuevo y agregar el usuario al grupo `example_group`.

   ```
   aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
    temp_creds_user --auto-create --db-name exampledb --db-groups example_group --
   duration-seconds 3600
   ```

   El resultado es el siguiente.

   ```
   {
     "DbUser": "IAMA:temp_creds_user:example_group",
     "Expiration": "2016-12-08T21:12:53Z",
     "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpDHwXVPyJYBDm/
   gqX2Eeaq6P3DgTzgPg=="
   }
   ```

5. Establezca una conexión de autenticación de capa de conexión segura (SSL) con el clúster de Amazon Redshift y envíe una solicitud de inicio de sesión con el nombre de usuario y la contraseña de la respuesta de `GetClusterCredentials`. Incluya el prefijo `IAM:` o `IAMA:` con el nombre de usuario; por ejemplo `IAM:temp_creds_user` o `IAMA:temp_creds_user`.

> **Important**
>
> Configure el cliente SQL para que requiera SSL. En caso contrario, si el cliente SQL intenta conectarse automáticamente con SSL, puede cambiar a una conexión distinta de SSL en caso de que se produzca algún error. En tal caso, el primer intento de conexión podría producir un error porque las credenciales han caducado o no son válidas, y el segundo intento de conexión podría producir un error porque la conexión no es SSL. Si eso ocurre, el primer mensaje de error podría pasarse por alto. Para obtener más información acerca de la conexión al clúster mediante SSL, consulte Configuración de las opciones de seguridad para las conexiones.

6. Si la conexión no usa SSL, el intento de conexión produce un error.
7. El clúster envía una solicitud `authentication` al cliente SQL.
8. El cliente SQL envía entonces la contraseña temporal al clúster.
9. Si la contraseña es válida y no ha caducado, el clúster realiza la conexión.

Autorización a Amazon Redshift para obtener acceso a otros servicios de AWS en su nombre

Algunas características de Amazon Redshift requieren que este servicio acceda a otros servicios de AWS en su nombre. Por ejemplo, los comandos COPY y UNLOAD pueden cargar o descargar datos en el clúster de Amazon Redshift mediante un bucket de Amazon S3. El comando CREATE EXTERNAL FUNCTION puede invocar una función de AWS Lambda mediante una función escalar de Lambda definida por el usuario (UDF). Amazon Redshift Spectrum puede usar un catálogo de datos en Amazon Athena oAWS Glue. Para que los clústeres de Amazon Redshift actúen en su nombre, debe proporcionarles credenciales de seguridad. El método preferido para proporcionar credenciales de seguridad consiste en especificar un rol de AWS Identity and Access Management (IAM). Para COPY y UNLOAD, puede proporcionar credenciales temporales.

Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	De
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • En el caso de la AWS CLI, consulte Configuración de la AWS CLI para usar AWS IAM Identity Center en la Guía del usuario de AWS Command Line Interface. • En el caso de los AWS SDK, las herramientas y las API de AWS, consulte Autenticación de IAM Identity Center en la Guía de referencia de AWS SDK y herramientas.
IAM	Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de Uso de credenciales temporales con recursos de AWS de la Guía del Usuario de IAM.
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para ver los SDK y las herramientas de AWS,

¿Qué usuario necesita acceso programático?	Para	De
		consulte Autenticar mediante credenciales a largo plazo en la Guía de referencia de SDK y herramientas de AWS. • Para las API de AWS, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

A continuación, se explica cómo crear un rol de IAM con los permisos adecuados para tener acceso a otros servicios de AWS. También necesitará asociar el rol al clúster y especificar el nombre de recurso de Amazon (ARN) del rol cuando ejecute el comando de Amazon Redshift. Para obtener más información, consulte Autorización de las operaciones COPY, UNLOAD, CREATE EXTERNAL FUNCTION y CREATE EXTERNAL SCHEMA mediante roles de IAM.

Además, un superusuario puede conceder el privilegio ASSUMEROLE a usuarios y grupos específicos para proporcionar acceso a un rol para las operaciones COPY y UNLOAD. Para obtener más información, consulte GRANT en la Guía para desarrolladores de base de datos de Amazon Redshift.

Creación de un rol de IAM que permita al clúster de Amazon Redshift obtener acceso a los servicios de AWS

Para crear un rol de IAM que permita al clúster de Amazon Redshift comunicarse con otros servicios de AWS en su nombre, siga estos pasos. Los valores utilizados en esta sección son ejemplos; puede elegir valores en función de sus necesidades.

Para crear un rol de IAM que permita a Amazon Redshift el acceso a los servicios de AWS

1. Abra la consola de IAM.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.

4. Elija AWS service (Servicio de AWS) y, a continuación, elija Redshift.
5. En Select your use case (Seleccione su caso de uso), elija Redshift - Customizable (Redshift - Personalizable) y Next: Permissions (Siguiente: permisos). Aparece la página Attach permissions policy (Adjuntar política de permisos).
6. Para obtener acceso a Amazon S3 mediante COPY, por ejemplo, puede usar **`AmazonS3ReadOnlyAccess`** y agregarlo. Para acceder a Amazon S3 mediante COPY o UNLOAD, le sugerimos que cree políticas administradas que restrinjan el acceso al bucket y al prefijo deseados según corresponda. Para las operaciones de lectura y escritura, recomendamos aplicar los privilegios mínimos y restringirlas únicamente a los buckets y los prefijos de clave de Amazon S3 que Amazon Redshift requiere.

   Para poder obtener acceso para invocar las funciones de Lambda del comando CREATE EXTERNAL FUNCTION, agregue **`AWSLambdaRole`**.

   En Redshift Spectrum, además del acceso a Amazon S3, agregue **`AWSGlueConsoleFullAccess`** o **`AmazonAthenaFullAccess`**.

   Elija Siguiente: etiquetas.
7. Aparece la página Add tags (Agregar etiquetas). Si lo desea, puede agregar etiquetas. Elija Siguiente: Revisar.
8. En Role Name (Nombre de la función), escriba un nombre para la función; por ejemplo, **`RedshiftCopyUnload`**. Seleccione Crear rol.
9. El nuevo rol está disponible para todos los usuarios en clústeres que utilizan el rol. Para restringir el acceso solo para usuarios específicos o para clústeres en regiones específicas, edite la relación de confianza del rol. Para obtener más información, consulte Restricción de acceso a los roles de IAM.
10. Asocie el rol al clúster. Puede asociar un rol de IAM a un clúster cuando crea el clúster o agrega el rol a un clúster existente. Para obtener más información, consulte Asociación de roles de IAM a los clústeres.

> **Note**
>
> Para restringir el acceso a datos específicos, utilice un rol de IAM que otorgue los privilegios mínimos necesarios.

Restricción de acceso a los roles de IAM

De manera predeterminada, los roles de IAM que están disponibles en un clúster de Amazon Redshift están disponibles para todos los usuarios de ese clúster. Tiene la opción de restringir los roles de IAM para usuarios específicos de la base de datos de Amazon Redshift en clústeres o regiones específicos.

Para permitir la utilización de un rol de IAM solo a usuarios específicos de la base de datos, siga estos pasos.

Para identificar a los usuarios específicos de la base de datos con acceso a un rol de IAM

1. Identifique el nombre de recurso de Amazon (ARN) de los usuarios de la base de datos en el clúster de Amazon Redshift. El ARN de un usuario de la base de datos está en el formato: `arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name`.

   Para Amazon Redshift sin servidor utilice el siguiente formato de ARN. `arn:aws:redshift:region:account-id:dbuser:workgroup-name/user-name`
2. Abra la consola de IAM.
3. Seleccione Roles en el panel de navegación.
4. Elija el rol de IAM que desea restringir para usuarios específicos de la base de datos de Amazon Redshift.
5. Seleccione la pestaña Trust Relationships (Relaciones de confianza) y Edit Trust Relationship (Editar relación de confianza). Un rol de IAM nuevo que permita a Amazon Redshift obtener acceso a otros servicios de AWS en su nombre tiene la siguiente relación de confianza:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Agregue una condición a la sección de acción `sts:AssumeRole` de la relación de confianza que limita el campo `sts:ExternalId` a los valores que usted especifique. Incluya un ARN para cada usuario de la base de datos al que desea concederle acceso al rol. El ID externo puede ser cualquier cadena única.

   Por ejemplo, la siguiente relación de confianza especifica que solo los usuarios de la base de datos `user1` y `user2` en el clúster `my-cluster` en la región `us-west-2` tienen permiso para utilizar este rol de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "redshift.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": [
          "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user1",
          "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user2"
        ]
      }
    }
  }]
}
```

7. Elija Actualizar política de confianza.

Restricción de un rol de IAM a una región de AWS

Puede restringir un rol de IAM para que sea accesible solo en una determinada región de AWS. De manera predeterminada, los roles de IAM para Amazon Redshift no se restringen a ninguna región en particular.

Para restringir la utilización de un rol de IAM por región, siga estos pasos.

Para identificar las regiones permitidas para un rol de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/.
2. Seleccione Roles en el panel de navegación.
3. Seleccione el rol que desea modificar con regiones específicas.
4. Seleccione la pestaña Trust Relationships (Relaciones de confianza) y Edit Trust Relationship (Editar relación de confianza). Un rol de IAM nuevo que permita a Amazon Redshift obtener acceso a otros servicios de AWS en su nombre tiene la siguiente relación de confianza:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Modifique la lista `Service` para el `Principal` con la lista de las regiones específicas a las que desea permitir la utilización del rol. Cada región de la lista `Service` debe indicarse con el formato siguiente: `redshift.`*`region`*`.amazonaws.com`.

   Por ejemplo, la siguiente relación de confianza editada permite la utilización del rol de IAM solo en las regiones `us-east-1` y `us-west-2`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.us-east-1.amazonaws.com",
          "redshift.us-west-2.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
```

```
    }
  ]
}
```

6. Seleccione Update Trust Policy (Actualizar política de confianza)

Encadenamiento de roles de IAM en Amazon Redshift

Cuando adjunta un rol a su clúster, este puede asumir ese rol y, de esa manera, obtener acceso a Amazon S3, Amazon Athena, AWS Glue y AWS Lambda en su nombre. Si un rol que está asociado al clúster no tiene acceso a los recursos necesarios, puede encadenar otro rol, que posiblemente pertenezca a otra cuenta. El clúster asumirá de forma temporal el rol encadenado para obtener acceso a los datos. También puede conceder acceso entre cuentas mediante el encadenamiento de roles. Cada uno de los roles de la cadena asume el rol siguiente, hasta que el clúster asume el rol situado al final de la cadena. El número máximo de roles de IAM que puede asociar está sujeto a una cuota. Para obtener más información, consulte la cuota "Roles de IAM del clúster que permiten a Amazon Redshift acceder a otros servicios de AWS" en Cuotas para objetos de Amazon Redshift.

Por ejemplo, imagine que la empresa A desea obtener acceso a los datos de un bucket de Amazon S3 que pertenece a la empresa B. La empresa A crea una función del servicio de AWS para Amazon Redshift denominada `RoleA` y la adjunta a su clúster. La empresa B crea un rol denominado `RoleB` que está autorizado para obtener acceso a los datos del bucket de la empresa B. Para obtener acceso a los datos del bucket de la empresa B, la empresa A ejecuta un comando COPY utilizando un parámetro `iam_role` que encadena `RoleA` y `RoleB`. Durante la operación COPY, `RoleA` asume de forma temporal `RoleB` para obtener acceso al bucket de Amazon S3.

Para encadenar roles, debe establecer una relación de confianza entre ellos. Un rol que asume otro rol (por ejemplo, `RoleA`) debe tener una política de permisos que le permita asumir el rol encadenado siguiente (por ejemplo, `RoleB`). A su vez, el rol que transfiere los permisos (`RoleB`) debe tener una política de confianza que le permita transferir sus permisos al rol encadenado anterior (`RoleA`). Para obtener más información, consulte Uso de roles de IAM en la Guía del usuario de IAM.

El primer rol de la cadena debe ser un rol asociado al clúster. El primer rol y cada uno de los roles posteriores que asuma el rol siguiente en la cadena deben tener una política que incluya una instrucción específica. Esta instrucción tiene el efecto `Allow` en la acción `sts:AssumeRole` y el nombre de recurso de Amazon (ARN) del rol siguiente en un elemento `Resource`. En nuestro ejemplo, `RoleA` tiene la siguiente política de permisos que le permite asumir `RoleB`, que pertenece a la cuenta de AWS `210987654321`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1487639602000",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::210987654321:role/RoleB"
       }
    ]
}
```

Un rol que se transfiere a otro rol debe establecer una relación de confianza con el rol que lo asume o con la cuenta de AWS a la que pertenece el rol. En nuestro ejemplo, `RoleB` tiene la siguiente política de confianza para establecer una relación de confianza con `RoleA`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

La siguiente política de confianza establece una relación de confianza con el propietario de `RoleA`, la cuenta de AWS `123456789012`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
```

```
      }
    }
  ]
}
```

> **Note**
>
> Para restringir la autorización de encadenamiento de roles a usuarios específicos, defina una condición. Para obtener más información, consulte Restricción de acceso a los roles de IAM.

Los comandos UNLOAD, COPY, CREATE EXTERNAL FUNCTION o CREATE EXTERNAL SCHEMA permiten encadenar roles al incluir una lista de ARN de rol separada por comas en el parámetro `iam_role`. A continuación se muestra la sintaxis para encadenar roles en el parámetro `iam_role`.

```
unload ('select * from venue limit 10')
to 's3://acmedata/redshift/venue_pipe_'
IAM_ROLE 'arn:aws:iam::<aws-account-id-1>:role/<role-name-1>[,arn:aws:iam::<aws-account-id-2>:role/<role-name-2>][,...]';
```

> **Note**
>
> La cadena de roles debe estar encerrada entre comillas simples y no puede contener espacios.

En los siguientes ejemplos, `RoleA` está adjuntado al clúster que pertenece a la cuenta de AWS `123456789012`. `RoleB`, que pertenece a la cuenta `210987654321`, tiene permiso para obtener acceso al bucket denominado `s3://companyb/redshift/`. En el siguiente ejemplo, se encadenan `RoleA` y `RoleB` para DESCARGAR datos en el bucket s3://companyb/redshift/.

```
unload ('select * from venue limit 10')
to 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

En el siguiente ejemplo, se utiliza un comando COPY para cargar los datos que se descargaron en el ejemplo anterior.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

En el siguiente ejemplo, CREATE EXTERNAL SCHEMA utiliza roles encadenados para asumir el rol `RoleB`.

```
create external schema spectrumexample from data catalog
database 'exampledb' region 'us-west-2'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

En el siguiente ejemplo, CREATE EXTERNAL FUNCTION utiliza roles encadenados para asumir el rol `RoleB`.

```
create external function lambda_example(varchar)
returns varchar
volatile
lambda 'exampleLambdaFunction'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Información adicional

También puede consultar Autorización de las operaciones COPY, UNLOAD, CREATE EXTERNAL FUNCTION y CREATE EXTERNAL SCHEMA mediante roles de IAM para obtener más información.

Autorización de las operaciones COPY, UNLOAD, CREATE EXTERNAL FUNCTION y CREATE EXTERNAL SCHEMA mediante roles de IAM

Puede utilizar el comando COPY para cargar (o importar) datos en Amazon Redshift y utilizar el comando UNLOAD para descargar (o exportar) datos desde Amazon Redshift. Puede utilizar el comando CREATE EXTERNAL FUNCTION para crear funciones definidas por el usuario que invoquen funciones desde AWS Lambda.

Con Amazon Redshift Spectrum, el comando CREATE EXTERNAL SCHEMA se utiliza para especificar la ubicación del bucket de Amazon S3 que contiene los datos. Cuando ejecute los comandos COPY, UNLOAD o CREATE EXTERNAL SCHEMA, debe proporcionar credenciales de seguridad. Estas credenciales autorizan a su clúster de Amazon Redshift a leer o escribir datos en su lugar de destino o desde él, como un bucket de Amazon S3.

Cuando ejecuta CREATE EXTERNAL FUNCTION, proporciona credenciales de seguridad mediante el parámetro del rol de IAM. Estas credenciales autorizan a su clúster de Amazon Redshift a invocar funciones de Lambda desde AWS Lambda. El método preferido para proporcionar credenciales de seguridad consiste en especificar un rol de AWS Identity and Access Management (IAM). Para COPY y UNLOAD, puede proporcionar credenciales temporales. Para obtener información sobre la creación de un rol de IAM, consulte Autorización a Amazon Redshift para obtener acceso a otros servicios de AWS en su nombre.

Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	De
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • En el caso de la AWS CLI, consulte Configuración de la AWS CLI para usar AWS IAM Identity Center en la Guía del usuario de AWS Command Line Interface. • En el caso de los AWS SDK, las herramientas y las API de AWS, consulte Autenticación de IAM Identity Center en la Guía de referencia de AWS SDK y herramientas.
IAM	Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS	Siga las instrucciones de Uso de credenciales temporales con recursos de AWS de la Guía del Usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	De
	CLI, los AWS SDK o las API de AWS.	
IAM	(No recomendado) Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para ver los SDK y las herramientas de AWS, consulte Autenticar mediante credenciales a largo plazo en la Guía de referencia de SDK y herramientas de AWS. • Para las API de AWS, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

Los pasos para utilizar un rol de IAM son los siguientes:

- Cree un rol de IAM para usar con el clúster de Amazon Redshift.
- Asocie el rol de IAM al clúster.
- Incluya el ARN del rol de IAM cuando llame al comando COPY, UNLOAD, CREATE EXTERNAL SCHEMA o CREATE EXTERNAL FUNCTION.

En este tema, aprenderá a asociar un rol de IAM con un clúster de Amazon Redshift.

Asociación de roles de IAM a los clústeres

Cuando haya creado un rol de IAM que autorice a Amazon Redshift a acceder a otros servicios de AWS en su nombre, debe asociar ese rol con un clúster de Amazon Redshift. Debe hacerlo para poder utilizar el rol para cargar o descargar datos.

Permisos requeridos para asociar un rol de IAM a un clúster

Para asociar un rol de IAM a un clúster, un usuario de IAM debe disponer del permiso `iam:PassRole` para dicho rol de IAM. Este permiso permite que un administrador pueda restringir los roles de IAM que un usuario puede asociar a clústeres de Amazon Redshift. Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

En el siguiente ejemplo se muestra una política de IAM que se puede asociar a un usuario y que le permite realizar estas acciones:

- obtener los detalles de todos los clústeres de Amazon Redshift que pertenecen a esa cuenta de usuario
- asociar cualquiera de los tres roles de IAM a uno de los dos clústeres de Amazon Redshift

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "redshift:DescribeClusters",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "redshift:ModifyClusterIamRoles",
                "redshift:CreateCluster"
            ],
            "Resource": [
                "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-cluster",
                "arn:aws:redshift:us-east-1:123456789012:cluster:my-second-redshift-
cluster"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::123456789012:role/MyRedshiftRole",
                "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                "arn:aws:iam::123456789012:role/ThirdRedshiftRole"
             ]
        }
    ]
}
```

Una vez que un usuario tenga los permisos adecuados, ese usuario puede asociar un rol de IAM con un clúster de Amazon Redshift. El rol de IAM estará listo entonces para su uso con el comando COPY u UNLOAD u otros comandos de Amazon Redshift.

Para obtener más información acerca de las políticas de IAM, consulte Información general de las políticas de IAM en la Guía del usuario de IAM.

Administración de la asociación de roles de IAM a un clúster

Puede asociar un rol de IAM con un clúster de Amazon Redshift cuando cree el clúster. O puede modificar un clúster existente y agregar o eliminar una o más asociaciones a roles de IAM.

Tenga en cuenta lo siguiente:

- El número máximo de roles de IAM que puede asociar está sujeto a una cuota.
- Puede asociar un rol de IAM a varios clústeres de Amazon Redshift.
- Puede asociar un rol de IAM a un clúster de Amazon Redshift solo si el rol de IAM y el clúster son propiedad de la misma cuenta de AWS.

Uso de la consola para administrar las asociaciones de roles de IAM

Puede administrar las asociaciones de roles de IAM a un clúster con la consola mediante el siguiente procedimiento.

Para administrar las asociaciones a roles de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el clúster que desea actualizar.
3. En Actions (Acciones), seleccione Administrar roles de IAM para mostrar la lista actual de roles de IAM asociados al clúster.
4. En la página Manage IAM roles (Administrar roles de IAM), seleccione los roles de IAM disponibles que desea agregar y luego seleccione Add IAM role (Agregar rol de IAM).
5. Seleccione Done (Aceptar) para guardar los cambios.

Uso de la AWS CLI para administrar las asociaciones de roles de IAM

Puede administrar las asociaciones de roles de IAM a un clúster con la AWS CLI a través de los siguientes métodos.

Asociación de un rol de IAM a un clúster mediante la AWS CLI

Para asociar un rol de IAM a un clúster cuando se crea el clúster, especifique el nombre de recurso de Amazon (ARN) del rol de IAM para el parámetro `--iam-role-arns` del comando `create-cluster`. El número máximo de roles de IAM que puede agregar cuando llama al comando `create-cluster` está sujeto a una cuota.

La asociación y la desvinculación de roles de IAM a clústeres de Amazon Redshift es un proceso asíncrono. Llame al comando `describe-clusters` para obtener el estado de todas las asociaciones de roles de IAM a su clúster.

En el siguiente ejemplo, se asocian dos roles de IAM al clúster recién creado con el nombre `my-redshift-cluster`.

```
aws redshift create-cluster \
    --cluster-identifier "my-redshift-cluster" \
    --node-type "dc1.large" \
    --number-of-nodes 16 \
    --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \
                    "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Para asociar un rol de IAM a un clúster de Amazon Redshift existente, especifique el nombre de recurso de Amazon (ARN) del rol de IAM para el parámetro `--add-iam-roles` del comando `modify-cluster-iam-roles`. El número máximo de roles de IAM que puede agregar cuando llama al comando `modify-cluster-iam-roles` está sujeto a una cuota.

En el siguiente ejemplo, se asocia un rol de IAM a un clúster existente con el nombre `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Desvinculación de un rol de IAM de un clúster mediante la AWS CLI

Para desvincular un rol de IAM de un clúster, especifique el ARN del rol de IAM para el parámetro `--remove-iam-roles` del comando `modify-cluster-iam-roles`. `modify-cluster-iam-roles` El número máximo de roles de IAM que puede eliminar cuando llama al comando `modify-cluster-iam-roles` está sujeto a una cuota.

En el siguiente ejemplo, se quita la asociación de un rol de IAM para la cuenta `123456789012` de AWS de un clúster denominado `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier "my-redshift-cluster" \
    --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Descripción de asociaciones de roles de IAM a un clúster mediante la AWS CLI

Para obtener una lista de todos los roles de IAM que están asociados a un clúster de Amazon Redshift y los estados de la asociación de los roles de IAM, llame al comando `describe-clusters`. El ARN de cada rol de IAM asociado al clúster se devuelve en la lista `IamRoles` como se muestra en el siguiente resultado de ejemplo.

Los roles que se asociaron al clúster muestran un estado de `in-sync`. Los roles que se encuentran en el proceso de asociación al clúster muestran un estado de `adding`. Los roles que se están desvinculando del clúster muestran un estado de `removing`.

```
{
    "Clusters": [
        {
            "ClusterIdentifier": "my-redshift-cluster",
            "NodeType": "dc1.large",
            "NumberOfNodes": 16,
            "IamRoles": [
                {
```

```
                    "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                }
            ],
            ...
        },
        {
            "ClusterIdentifier": "my-second-redshift-cluster",
            "NodeType": "dc1.large",
            "NumberOfNodes": 10,
            "IamRoles": [
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                },
                {
                    "IamRoleArn": "arn:aws:iam::123456789012:role/ThirdRedshiftRole",
                    "IamRoleApplyStatus": "in-sync"
                }
            ],
            ...
        }
    ]
}
```

Para obtener más información acerca de cómo usar AWS CLI, consulte la Guía del usuario de AWS CLI.

Creación de un rol de IAM como predeterminado para Amazon Redshift

Al crear roles de IAM a través de la consola de Redshift, Amazon Redshift crea los roles mediante programación en su Cuenta de AWS y adjunta automáticamente las políticas existentes administradas por AWS a ellos. Este enfoque significa que puede permanecer dentro de la consola de Redshift y no tiene que cambiar a la consola de IAM para crear roles. Para obtener un control

pormenorizado de los permisos de un rol de IAM existente creado en la consola de Amazon Redshift, puede adjuntar una política administrada personalizada al rol de IAM.

Información general de los roles de IAM creados en la consola

Cuando utiliza la consola de Amazon Redshift para crear roles de IAM, Amazon Redshift realiza un seguimiento de todos los roles de IAM creados a través de la consola. Amazon Redshift preselecciona el rol de IAM predeterminado más reciente para crear todos los clústeres nuevos y restaurar clústeres a partir de instantáneas.

Puede crear un rol de IAM a través de la consola que tiene una política con permisos para ejecutar comandos SQL. Estos comandos incluyen COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL o CREATE LIBRARY. De forma opcional, puede obtener un control más pormenorizado del acceso de los usuarios a sus recursos de AWS creando y adjuntando políticas personalizadas al rol de IAM.

Cuando crea un rol de IAM y lo configura como predeterminado para el clúster mediante la consola, no tiene que proporcionar el nombre de recurso de Amazon (ARN) del rol de IAM para realizar la autenticación y la autorización.

Uso de los roles de IAM creados en la consola

El rol de IAM que crea a través de la consola para su clúster tiene la política administrada `AmazonRedshiftAllCommandsFullAccess` adjunta de forma automática. Este rol de IAM permite a Amazon Redshift copiar, descargar, consultar y analizar datos de los recursos de AWS de su cuenta de IAM. La política administrada proporciona acceso a las operaciones COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL y CREATE LIBRARY. La política también concede permisos para ejecutar instrucciones SELECT para servicios relacionados de AWS, como Amazon S3, Amazon CloudWatch Logs, Amazon SageMaker y AWS Glue.

Los comandos CREATE EXTERNAL FUNCTION, CREATE EXTERNAL SCHEMA, CREATE MODEL y CREATE LIBRARY tienen una palabra clave `default`. Para esta palabra clave para estos comandos, Amazon Redshift utiliza el rol de IAM establecido como predeterminado y asociado al clúster cuando se ejecuta el comando. Puede ejecutar el comando DEFAULT_IAM_ROLE, para verificar el rol de IAM predeterminado actual que está adjunto al clúster.

Para controlar los privilegios de acceso del rol de IAM creado y establecido como predeterminado para el clúster de Redshift, utilice el privilegio ASSUMEROLE. Este controlador de acceso se aplica a los usuarios y grupos de la base de datos cuando ejecutan comandos, como los enumerados

anteriormente. Después de conceder el privilegio ASSUMEROLE a un usuario o un grupo para un rol de IAM, el usuario o el grupo puede asumir ese rol cuando se ejecuten estos comandos. Mediante el uso del privilegio ASSUMEROLE, puede conceder acceso a los comandos adecuados según sea necesario.

Con la consola de Amazon Redshift, puede hacer lo siguiente:

- Creación de un rol de IAM como predeterminado
- Eliminación de roles de IAM del clúster
- Asociación de roles de IAM al clúster
- Configurar un rol de IAM como predeterminado
- Hacer que un rol de IAM ya no sea predeterminado para el clúster

Permisos de la política administrada AmazonRedShiftAllCommandsFullAccess

En el siguiente ejemplo, se muestran los permisos de la política administrada `AmazonRedshiftAllCommandsFullAccess` que permite ciertas acciones para el rol de IAM que se configura como predeterminado para su clúster. El rol de IAM con políticas de permisos adjuntas autoriza lo que un usuario o grupo puede y no puede hacer. Con estos permisos, puede ejecutar el comando COPY desde Amazon S3, ejecutar UNLOAD y utilizar el comando CREATE MODEL.

```
{
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketCors",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:PutBucketCors",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload",
                "s3:CreateBucket"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::redshift-downloads",
                "arn:aws:s3:::redshift-downloads/*",
                "arn:aws:s3:::*redshift*",
                "arn:aws:s3:::*redshift*/*"
            ]
}
```

En el siguiente ejemplo, se muestran los permisos de la política administrada `AmazonRedshiftAllCommandsFullAccess` que permite ciertas acciones para el rol de IAM que se configura como predeterminado para el clúster. El rol de IAM con políticas de permisos adjuntas autoriza lo que un usuario o grupo puede y no puede hacer. Con los siguientes permisos, puede ejecutar el comando CREATE EXTERNAL FUNCTION.

```
{
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}
```

En el siguiente ejemplo, se muestran los permisos de la política administrada `AmazonRedshiftAllCommandsFullAccess` que permite ciertas acciones para el rol de IAM que se configura como predeterminado para el clúster. El rol de IAM con políticas de permisos adjuntas autoriza lo que un usuario o grupo puede y no puede hacer. Con los siguientes permisos, puede ejecutar los comandos CREATE EXTERNAL SCHEMA y CREATE EXTERNAL TABLE necesarios para Amazon Redshift Spectrum.

```
{
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:GetTable",
```

```
                "glue:GetTables",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:*:*:table/*redshift*/*",
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*redshift*"
            ]
}
```

En el siguiente ejemplo, se muestran los permisos de la política administrada `AmazonRedshiftAllCommandsFullAccess` que permite ciertas acciones para el rol de IAM configurado como predeterminado para el clúster. El rol de IAM con políticas de permisos adjuntas autoriza lo que un usuario o grupo puede y no puede hacer. Con los siguientes permisos, puede ejecutar el comando CREATE EXTERNAL SCHEMA mediante consultas federadas.

```
{
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:*Redshift*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetRandomPassword",
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "secretsmanager:ResourceTag/Redshift": "true"
                }
            }
},
```

Administración de roles de IAM creados para un clúster mediante la consola

Para crear, modificar y eliminar roles de IAM creados desde la consola de Amazon Redshift, utilice la sección Clusters (Clústeres) de la consola.

Creación de un rol de IAM como predeterminado

En la consola, puede crear el rol de IAM para su clúster que tiene la política administrada `AmazonRedshiftAllCommandsFullAccess` adjunta de forma automática. El nuevo rol de IAM que cree permite a Amazon Redshift copiar, cargar, consultar y analizar datos de los recursos de Amazon de su cuenta de IAM.

Solo puede haber un rol de IAM configurado como predeterminado para un clúster. Si crea otro rol de IAM como el predeterminado del clúster cuando un rol de IAM existente está asignado actualmente como predeterminado, el nuevo rol de IAM sustituye al otro como predeterminado.

Para crear un nuevo clúster y un rol de IAM establecido como predeterminado para el nuevo clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Seleccione Create cluster (Crear clúster) para crearlo.
4. Siga las instrucciones en la página de la consola para introducir las propiedades de la Cluster configuration (Configuración del clúster). Para obtener más información acerca de este paso, consulte Creación de un clúster.
5. (Opcional) Elija Load sample data (Cargar datos de muestra) para cargar los datos de muestra configurados en el clúster de Amazon Redshift para comenzar a utilizar el editor de consultas para consultar datos.

   Si se encuentra detrás de un firewall, el puerto de la base de datos debe ser un puerto abierto que acepta conexiones entrantes.

6. Siga las instrucciones en la página de la consola para ingresar las propiedades de las Database configurations (Configuraciones de la base de datos).
7. En Cluster permissions (Permisos de clúster), desde Manage IAM roles (Administrar roles de IAM), elija Create IAM role (Crear rol de IAM).
8. Especifique un bucket de Amazon S3 para que el rol de IAM tenga acceso, mediante la elección de uno de los siguientes métodos:

   - Elija No additional Amazon S3 bucket (Sin bucket de Amazon S3 adicional), para crear el rol de IAM sin especificar buckets específicos de Amazon S3.
   - Elija Any Amazon S3 bucket (Cualquier bucket de Amazon S3) para permitir a los usuarios que tienen acceso a su clúster de Amazon Redshift acceder también a cualquier bucket de Amazon S3 y a su contenido en su Cuenta de AWS.
   - Elija Specific Amazon S3 buckets (Buckets de Amazon S3 específicos) para especificar uno o varios buckets de Amazon S3 a los que el rol de IAM que se está creando tiene permiso para acceder. A continuación, elija uno o más buckets de Amazon S3 de la tabla.
9. Elija Create IAM role as default (Crear un rol de IAM como predeterminado). Amazon Redshift crea y configura automáticamente el rol de IAM como predeterminado para su clúster.
10. Seleccione Create cluster (Crear clúster) para crearlo. El clúster tardará varios minutos antes de estar listo para su uso.

Eliminación de roles de IAM del clúster

Puede eliminar uno o varios roles de IAM del clúster.

Para eliminar roles de IAM del clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el clúster del que desea eliminar el rol de IAM.
4. En Cluster permissions (Permisos de clúster), elija uno o varios roles de IAM que desea eliminar del clúster.
5. Desde Manage IAM roles (Administrar roles de IAM), elija Remove IAM roles (Eliminar roles de IAM).

Asociación de roles de IAM al clúster

Puede asociar uno o más roles de IAM al clúster.

Para asociar el rol de IAM al clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el clúster al que desea asociar los roles de IAM.
4. En Cluster permissions (Permisos de clúster), elija uno o varios roles de IAM que desea asociar con el clúster.
5. Desde Manage IAM roles (Administrar roles de IAM), elija Remove IAM roles (Asociar roles de IAM).
6. Elija uno o más roles de IAM para asociarlos al clúster.
7. Elija Associate IAM roles (Asociar roles de IAM).

Configurar un rol de IAM como predeterminado

Puede configurar un rol de IAM como predeterminado para el clúster.

Para convertir un rol de IAM en el predeterminado del clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el clúster para el que desea configurar un rol de IAM predeterminado.
4. En Cluster permissions (Permisos de clúster), desde Associated IAM roles (Roles de IAM asociados), elija un rol de IAM que desee convertir en predeterminado para el clúster.
5. En Set default (Configurar predeterminado), elija Make default (Convertir en predeterminado).
6. Cuando se le pregunte, elija Set default (Configurar predeterminado) para confirmar el rol de IAM especificado como predeterminado.

Hacer que un rol de IAM ya no sea predeterminado para el clúster

Puede hacer que un rol de IAM ya no sea predeterminado para el clúster.

Para borrar un rol de IAM como el predeterminado del clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres). Se enumeran los clústeres de su cuenta en la Región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Elija el clúster al que desea asociar los roles de IAM.
4. En Cluster permissions (Permisos de clúster), desde Associated IAM roles (Roles de IAM asociados), elija el rol de IAM predeterminado.
5. En Set default (Configurar predeterminado), elija Clear default (Borrar predeterminado).
6. Cuando se le pregunte, elija Clear default (Borrar predeterminado) para confirmar la eliminación del rol de IAM especificado como predeterminado.

Administración de roles de IAM creados en el clúster mediante la AWS CLI

Puede administrar roles de IAM creados en el clúster mediante la AWS CLI.

Para crear un clúster de Amazon Redshift con un rol de IAM configurado como predeterminado

Para crear un clúster de Amazon Redshift con un rol de IAM configurado como predeterminado para el clúster, utilice el comando `aws redshift create-cluster` de la AWS CLI.

Los siguientes comandos de la AWS CLI crean un clúster de Amazon Redshift y el rol de IAM denominado myrole1. El comando de la AWS CLI también configura myrole1 como predeterminado para el clúster.

```
aws redshift create-cluster \
    --node-type dc2.large \
    --number-of-nodes 2 \
    --master-username adminuser \
    --master-user-password TopSecret1 \
    --cluster-identifier mycluster \
    --iam-roles 'arn:aws:iam::012345678910:role/myrole1'
 'arn:aws:iam::012345678910:role/myrole2' \
```

```
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

El siguiente fragmento es un ejemplo de la respuesta.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "adding"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "adding"
            }
        ]
        ...
    }
}
```

Para agregar uno o más roles de IAM a un clúster de Amazon Redshift

Para agregar uno o más roles de IAM asociados al clúster, utilice el comando `aws redshift modify-cluster-iam-roles` de la AWS CLI.

Los siguientes comandos de la AWS CLI agregan `myrole3` y `myrole4` al clúster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

El siguiente fragmento es un ejemplo de la respuesta.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
```

```
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
                "ApplyStatus": "adding"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",
                "ApplyStatus": "adding"
            }
        ],
        ...
    }
}
```

Para eliminar uno o más roles de IAM desde un clúster de Amazon Redshift

Para eliminar uno o más roles de IAM asociados al clúster, utilice el comando `aws redshift modify-cluster-iam-roles` de la AWS CLI.

El siguiente comando de la AWS CLI elimina `myrole3` y `myrole4` del clúster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
 'arn:aws:iam::012345678910:role/myrole4'
```

El siguiente fragmento es un ejemplo de la respuesta.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
```

```
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
                "ApplyStatus": "removing"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",
                "ApplyStatus": "removing"
            }
        ],
        ...
    }
}
```

Para configurar un rol de IAM asociado como predeterminado para el clúster

Para configurar un rol de IAM asociado como predeterminado para el clúster, utilice el comando `aws redshift modify-cluster-iam-roles` de la AWS CLI.

El siguiente comando de la AWS CLI configura `myrole2` como predeterminado para el clúster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'
```

El siguiente fragmento es un ejemplo de la respuesta.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
```

```
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            }
        ],
        ...
    }
}
```

Para configurar un rol de IAM no asociado como predeterminado para el clúster

Para configurar un rol de IAM no asociado como predeterminado para el clúster, utilice el comando `aws redshift modify-cluster-iam-roles` de la AWS CLI.

El siguiente comando de la AWS CLI agrega `myrole2` al clúster de Amazon Redshift y lo configura como predeterminado para el clúster.

```
aws redshift modify-cluster-iam-roles \
    --cluster-identifier mycluster \
    --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3' \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole3'
```

El siguiente fragmento es un ejemplo de la respuesta.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
        "IamRoles": [
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "in-sync"
            },
```

```
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "in-sync"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
                "ApplyStatus": "adding"
            }
        ],
        ...
    }
}
```

Para restaurar un clúster a partir de una instantánea y configurar un rol de IAM como predeterminado para este

Cuando restaura el clúster desde una instantánea, puede asociar un rol de IAM existente o crear uno nuevo y configurarlo como predeterminado para el clúster.

Para restaurar un clúster de Amazon Redshift desde una instantánea y configurar un rol de IAM como predeterminado para el clúster, utilice el comando `aws redshift restore-from-cluster-snapshot` de la AWS CLI.

El siguiente comando de la AWS CLI restaura el clúster desde una instantánea y configura `myrole2` como predeterminado para el clúster.

```
aws redshift restore-from-cluster-snapshot \
    --cluster-identifier mycluster-clone \
    --snapshot-identifier my-snapshot-id
    --iam-roles 'arn:aws:iam::012345678910:role/myrole1'
 'arn:aws:iam::012345678910:role/myrole2' \
    --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

El siguiente fragmento es un ejemplo de la respuesta.

```
{
    "Cluster": {
        "ClusterIdentifier": "mycluster-clone",
        "NodeType": "dc2.large",
        "MasterUsername": "adminuser",
        "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "IamRoles": [
```

```
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
                "ApplyStatus": "adding"
            },
            {
                "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
                "ApplyStatus": "adding"
            }
        ],
        ...
    }
}
```

Uso de una identidad federada para administrar el acceso de Amazon Redshift a los recursos locales y a las tablas externas de Amazon Redshift Spectrum

El uso de la federación de identidades en AWS con las credenciales proporcionadas por `GetDatabaseCredentials` puede simplificar la autorización y el acceso a los datos locales y externos. Actualmente, para conceder a los usuarios acceso a datos externos que residen en Amazon S3, se crea un rol de IAM con los permisos definidos en una política de permisos. A continuación, los usuarios con el rol asociado pueden acceder a los datos externos. Esto funciona, pero si desea proporcionar reglas detalladas, como hacer que determinadas columnas no estén disponibles para un usuario concreto, puede que tenga que realizar una configuración adicional en el esquema externo. En este tema, mostramos cómo proporcionar acceso a los recursos con la federación de identidades de AWS, en lugar de utilizar un rol de IAM específico. La federación de identidades, con las credenciales proporcionadas por `GetDatabaseCredentials`, puede proporcionar acceso a AWS Glue y a los recursos de Redshift Spectrum mediante reglas de IAM precisas que son más fáciles de especificar y cambiar. Esto facilita aplicar un acceso que se ajuste a las reglas de la empresa.

Los beneficios de usar credenciales federadas son los siguientes:

- No es necesario que administre los roles de IAM asociados al clúster para Redshift Spectrum.
- Los administradores de clústeres pueden crear un esquema externo al que puedan acceder los consumidores con diferentes contextos de IAM. Esto resulta útil, por ejemplo, para filtrar columnas en una tabla, donde diferentes consumidores consultan el mismo esquema externo y obtienen diferentes campos en los registros devueltos.
- Puede consultar Amazon Redshift mediante un usuario con permisos de IAM, en lugar de solo con un rol.

Preparación de una identidad para iniciar sesión con una identidad federada

Antes de iniciar sesión con una identidad federada, debe realizar varios pasos preliminares. En estas instrucciones se asume que tiene un esquema externo de Redshift Spectrum existente que hace referencia a un archivo de datos almacenado en un bucket de Amazon S3 y que el bucket está en la misma cuenta que el clúster de Amazon Redshift o el almacenamiento de datos sin servidor de Amazon Redshift.

1. Cree una identidad de IAM. Puede ser un usuario o un rol de IAM. Utilice cualquier nombre que admita IAM.
2. Adjunte políticas de permisos a la identidad. Especifique cualquiera de las siguientes:

   - `redshift:GetClusterCredentialsWithIAM` (para un clúster aprovisionado de Amazon Redshift)
   - `redshift-serverless:GetCredentials` (para Amazon Redshift Serverless)

   Puede agregar permisos con el editor de políticas, mediante la consola de IAM.

   La identidad de IAM también necesita permisos para acceder a los datos externos. Conceda acceso a Amazon S3 agregando directamente las siguientes políticas administradas de AWS:

   - `AmazonS3ReadOnlyAccess`
   - `AWSGlueConsoleFullAccess`

   La política administrada más reciente es obligatoria si usa AWS Glue para preparar los datos externos. Para obtener más información sobre los pasos para conceder acceso a Amazon Redshift Spectrum, consulte Crear un rol de IAM para Amazon Redshift, que forma parte de la guía de introducción de Amazon Redshift y Redshift Spectrum. Muestra los pasos para agregar políticas de IAM para acceder a Redshift Spectrum.
3. Configure el cliente SQL para conectarse a Amazon Redshift. Utilice el controlador JDBC de Amazon Redshift y agregue las credenciales del usuario a las propiedades de credenciales de la herramienta. Un cliente como SQL Workbench/J funciona bien para esto. Defina las siguientes propiedades ampliadas de conexión de cliente:

   - AccessKeyID: el identificador de la clave de acceso.
   - SecretAccessKey: la clave de acceso secreta. (Tenga en cuenta el riesgo de seguridad de transmitir la clave secreta si no utiliza cifrado).

- SessionToken: un conjunto de credenciales temporales para un rol de IAM.
- groupFederation: se establece en `true` si está configurando la identidad federada para un clúster aprovisionado. No defina este parámetro si utiliza Amazon Redshift Serverless.
- LogLevel: valor de nivel de registro entero. Es opcional.

4. Configure la URL en el punto de conexión de JDBC que se encuentra en la consola de Amazon Redshift o Amazon Redshift Serverless. Sustituya el esquema de URL por jdbc:redshift:iam: y use este formato:

   - Formato para un clúster aprovisionado de Amazon Redshift: `jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

     Ejemplo: `jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`
   - Formato para Amazon Redshift Serverless: `jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

     Ejemplo: `jdbc:redshift:iam://default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev`

   Tras conectarse a la base de datos por primera vez mediante una identidad de IAM, Amazon Redshift crea automáticamente una identidad de Amazon Redshift con el mismo nombre, con el prefijo `IAM:` para un usuario o `IAMR:` para un rol de IAM. Los pasos restantes de este tema muestran ejemplos para un usuario.

   Si un usuario de Redshift no se crea automáticamente, puede crear uno ejecutando una instrucción `CREATE USER`, mediante una cuenta de administrador y especificando el nombre de usuario en el formato `IAM:<user name>`.

5. Como administrador del clúster de Amazon Redshift, conceda al usuario de Redshift los permisos necesarios para acceder al esquema externo.

   ```
   GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
   ```

   Para conceder la capacidad al usuario de Redshift de crear tablas en el esquema externo, debe ser el propietario del esquema. Por ejemplo:

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. Para comprobar la configuración, ejecute una consulta como usuario, mediante el cliente SQL, una vez concedidos los permisos. Este ejemplo de consulta recupera datos de una tabla externa.

```
SELECT * FROM my_schema.my_table;
```

Introducción a la propagación de identidades y autorizaciones a Redshift Spectrum

Para pasar una identidad federada a las tablas externas de consulta, debe establecer `SESSION` como valor del parámetro de consulta `IAM_ROLE` de `CREATE EXTERNAL SCHEMA`. Los siguientes pasos muestran cómo configurar y aprovechar `SESSION` para autorizar consultas en el esquema externo.

1. Cree tablas locales y tablas externas. Las tablas externas catalogadas con AWS Glue funcionan para esto.
2. Conéctese a Amazon Redshift con la identidad de IAM. Como se mencionó en la sección anterior, cuando la identidad se conecta a Amazon Redshift, se crea un usuario de base de datos de Redshift. El usuario se crea si no existía anteriormente. Si el usuario es nuevo, el administrador debe concederle permisos para realizar tareas en Amazon Redshift, como consultar y crear tablas.
3. Conéctese a Redshift con la cuenta de administrador. Ejecute el comando para crear un esquema externo con el valor `SESSION`.

```
create external schema spectrum_schema from data catalog
database '<my_external_database>'
region '<my_region>'
iam_role 'SESSION'
catalog_id '<my_catalog_id>';
```

Tenga en cuenta que `catalog_id` está configurado en este caso. Se trata de una nueva configuración que se agrega con la característica, ya que `SESSION` sustituye a un rol específico.

En este ejemplo, los valores de la consulta imitan la forma en que aparecen los valores reales.

```
create external schema spectrum_schema from data catalog
```

```
database 'spectrum_db'
region 'us-east-1'
iam_role 'SESSION'
catalog_id '123456789012'
```

El valor `catalog_id` en este caso es el ID de la cuenta de AWS.

4. Ejecute consultas para acceder a los datos externos mediante la identidad de IAM con la que se conectó en el paso 2. Por ejemplo:

```
select * from spectrum_schema.table1;
```

En este caso, `table1` puede ser, por ejemplo, datos con formato JSON en un archivo, en un bucket de Amazon S3.

5. Si ya tiene un esquema externo que usa un rol de IAM adjunto a un clúster y apunta a la base de datos o esquema externo, puede sustituir el esquema existente y usar una identidad federada como se detalla en estos pasos o crear uno nuevo.

`SESSION` indica que las credenciales de identidad federadas se utilizan para consultar el esquema externo. Cuando utilice el parámetro de consulta `SESSION`, asegúrese de configurar el `catalog_id`. Es obligatorio porque apunta al catálogo de datos utilizado para el esquema. Anteriormente, `catalog_id` se recuperaba del valor asignado a `iam_role`. Al configurar la propagación de identidades y autorizaciones de esta manera, por ejemplo, a Redshift Spectrum, mediante el uso de credenciales federadas para consultar un esquema externo, no se requiere la autorización mediante un rol de IAM.

Notas de uso

Un error de conexión común es el siguiente: Error de IAM al recuperar las credenciales temporales: no se puede desmarcar la respuesta de excepción con los descifradores proporcionados. Este error es resultado de tener un controlador JDBC antiguo. La versión mínima del controlador requerida para la identidad federada es la 2.1.0.9. Puede obtener el controlador JDBC desde Descargar el controlador JDBC de Amazon Redshift, versión 2.1.

Recursos adicionales de

Estos enlaces proporcionan información adicional para administrar el acceso a datos externos.

- Puede seguir accediendo a los datos de Redshift Spectrum mediante un rol de IAM. Para obtener más información, consulte Autorización a Amazon Redshift para obtener acceso a otros servicios de AWS en su nombre.
- Cuando administra el acceso a tablas externas con AWS Lake Formation, puede consultarlas mediante Redshift Spectrum con identidades de IAM federadas. Ya no es necesario que administre los roles de IAM asociados al clúster para que Redshift Spectrum consulte los datos asociados a AWS Lake Formation. Para obtener más información, consulte Uso de AWS Lake Formation con Amazon Redshift Spectrum.

Administración de las contraseñas de administrador de Amazon Redshift mediante AWS Secrets Manager

Amazon Redshift se puede integrar con AWS Secrets Manager para generar y administrar sus credenciales de administrador dentro de un secreto cifrado. Con AWS Secrets Manager, puede sustituir sus contraseñas de administrador por una llamada a la API para recuperar el secreto mediante programación cuando sea necesario. Usar secretos en lugar de credenciales con codificación rígida reduce el riesgo de que dichas credenciales queden expuestas o se vean comprometidas. Para obtener más información sobre AWS Secrets Manager, consulte la Guía del usuario de AWS Secrets Manager.

Puede especificar que Amazon Redshift administre la contraseña de administrador con AWS Secrets Manager cuando realice una de las siguientes operaciones:

- Crear un clúster aprovisionado o un espacio de nombres sin servidor.
- Restaurar un clúster o un espacio de nombres sin servidor a partir de una instantánea.

Al especificar que Amazon Redshift administre la contraseña de administrador en AWS Secrets Manager, Amazon Redshift genera la contraseña y la almacena en Secrets Manager. Puede acceder al secreto directamente en AWS Secrets Manager para recuperar las credenciales del usuario administrador. Si lo desea, también puede especificar una clave administrada por el cliente para cifrar el secreto si necesita acceder a él desde otra cuenta de AWS. También puede usar la clave de KMS que proporciona AWS Secrets Manager.

Amazon Redshift administra la configuración del secreto y lo rota cada 30 días de forma predeterminada. Puede rotar el secreto manualmente en cualquier momento. Si elimina un clúster

aprovisionado o un espacio de nombres sin servidor que administra un secreto en AWS Secrets Manager, también se eliminarán el secreto y sus metadatos asociados.

Para conectarse a un clúster o espacio de nombres sin servidor con las credenciales administradas de forma secreta, puede recuperar el secreto de AWS Secrets Manager desde la consola de Secrets Manager o la llamada a la API `GetSecretValue` de Secrets Manager. Para obtener más información, consulte Recuperar secretos de AWS Secrets Manager y Conexión a una base de datos SQL con credenciales en un secreto de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Permisos necesarios para la integración de AWS Secrets Manager

Los usuarios deben tener los permisos necesarios para realizar las operaciones relacionadas con la integración de AWS Secrets Manager. Cree políticas de IAM que concedan permisos para realizar operaciones de la API concretas en los recursos especificados que necesiten. A continuación, asocie esas políticas a los roles o conjuntos de permisos de IAM que necesiten esos permisos. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

El usuario que especifica que Amazon Redshift administre la contraseña de administrador en AWS Secrets Manager debe tener permisos para realizar las siguientes operaciones:

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`
- `secretsmanager:UpdateSecret`
- `secretsmanager:DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

Si el usuario quiere introducir una clave de KMS en el parámetro `MasterPasswordSecretKmsKeyId` de los clústeres aprovisionados o en el parámetro `AdminPasswordSecretKmsKeyId` de los espacios de nombres sin servidor, necesitará los siguientes permisos además de los permisos enumerados anteriormente.

- `kms:Decrypt`
- `kms:GenerateDataKey`

- `kms:CreateGrant`
- `kms:RetireGrant`

Rotación del secreto de la contraseña de administrador

De forma predeterminada, Amazon Redshift rota automáticamente el secreto cada 30 días para garantizar que sus credenciales no permanezcan iguales durante períodos prolongados. Cuando Amazon Redshift rota el secreto de una contraseña de administrador, AWS Secrets Manager actualiza el secreto existente para incluir una nueva contraseña de administrador. Amazon Redshift cambia la contraseña de administrador del clúster para que coincida con la contraseña del secreto actualizado.

Puede rotar un secreto inmediatamente con AWS Secrets Manager en lugar de esperar a que se programe una rotación. Para obtener más información acerca de la rotación de secretos, consulte Rotar secretos de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Recuperación del nombre de recurso de Amazon (ARN) del secreto en Amazon Redshift

Puede ver el nombre de recurso de Amazon (ARN) de cualquier secreto que administre AWS Secrets Manager desde la consola de Amazon Redshift. Una vez que tenga el ARN del secreto, podrá ver los detalles de su secreto y los datos cifrados de su secreto con AWS Secrets Manager. Para obtener más información sobre cómo recuperar secretos con el ARN, consulte Recuperar secretos en la Guía del usuario de AWS Secrets Manager.

Visualización de los detalles de un secreto para un clúster aprovisionado por Amazon Redshift

Para ver el nombre de recurso de Amazon (ARN) del secreto del clúster desde la consola de Amazon Redshift, siga este procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift.
2. En el panel de Información general acerca del clúster, elija el clúster cuyo secreto desea ver.
3. Elija la pestaña Propiedades.
4. Puede ver el ARN del secreto en ARN de credenciales de administrador. Este ARN es el identificador del secreto, que puede utilizar en AWS Secrets Manager para ver los detalles del secreto.

Visualización de los detalles de un secreto para un espacio de nombres de Amazon Redshift sin servidor

Para ver el nombre de recurso de Amazon (ARN) del secreto del espacio de nombres sin servidor desde la consola de Amazon Redshift, siga este procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift.
2. En el panel Clústeres aprovisionados, elija Ir a la solución sin servidor en la parte superior derecha de la página.
3. En Panel de la solución sin servidor, desplácese hasta el panel Espacios de nombres / Grupos de trabajo y elija el espacio de nombres cuyo secreto desea ver.
4. En el panel Información general, consulte el ARN del secreto en ARN de credenciales de administrador. Este ARN es el identificador del secreto, que puede utilizar en AWS Secrets Manager para ver los detalles del secreto.

Creación de un secreto para las credenciales de conexión a la base de datos

Puede crear un secreto de Secrets Manager para almacenar las credenciales utilizadas para conectarse a un clúster aprovisionado de Amazon Redshift o a un espacio de nombres y grupo de trabajo de Redshift sin servidor.

Creación de un secreto que se utiliza para conectarse a una base de datos en un clúster aprovisionado

1. Abra la consola de Secrets Manager (https://console.aws.amazon.com/secretsmanager/).
2. Elija Almacenar un secreto nuevo.
3. Elija Credenciales para el clúster de Amazon Redshift.

   Introduzca la información de:

   - Nombre de usuario
   - Password
   - Clave de cifrado

   Elija un clúster para el que desee crear las credenciales secretas.

4. Elija Continuar para pasar a la siguiente pantalla.
5. Añada una clave de etiqueta que comience con la cadena “Redshift”.
6. Siga introduciendo la información sobre su secreto en las diversas pantallas y luego seleccione Guardar los cambios.

Confirme que aparezca un mensaje que indique que el secreto se ha guardado correctamente. También puede ver el secreto en la consola de Secrets Manager. Puede utilizar este secreto para conectarse a una base de datos de un clúster de la consola de Amazon Redshift y del editor de consultas de Amazon Redshift v2 mediante el método de conexión de AWS Secrets Manager. El secreto también debe tener una clave de etiqueta que empiece por la cadena “Redshift” para que el secreto aparezca en la aplicación web del editor de consultas v2.

Creación de un secreto que se utiliza para conectarse a una base de datos en un grupo de trabajo Redshift sin servidor

1. Abra la consola de Redshift sin servidor.
2. Navegue hasta Configuración de espacio de nombres.
3. Elija un espacio de nombres para el que desee crear las credenciales secretas.
4. Abra Acciones, Editar credenciales de administrador.
5. En Contraseña de administrador, seleccione Administrar credenciales de administrador en AWS Secrets Manager.
6. Elija Guardar cambios para guardar los cambios.

Confirme que aparezca un mensaje que indique que la contraseña se ha cambiado correctamente. También puede ver el secreto en la consola de Secrets Manager. Puede usar este secreto para conectarse a una base de datos de un grupo de trabajo en la consola de Redshift sin servidor y el editor de consultas de Amazon Redshift v2 mediante el método de conexión de AWS Secrets Manager. El secreto también debe tener una clave de etiqueta que empiece por la cadena “Redshift” para que el secreto aparezca en la aplicación web del editor de consultas v2.

Consideraciones sobre el uso de AWS Secrets Manager con Amazon Redshift

Cuando utilice AWS Secrets Manager para administrar las credenciales de administrador del clúster aprovisionado o del espacio de nombres sin servidor, tenga en cuenta lo siguiente:

- Si pausa un clúster cuyas credenciales de administrador las administra AWS Secrets Manager, el secreto del clúster no se eliminará y se le seguirá cobrando por él. Los secretos solo se eliminan cuando se elimina el clúster.
- Si el clúster está pausado cuando Amazon Redshift intenta rotar el secreto que tiene asociado, la rotación fallará. En este caso, Amazon Redshift detiene la rotación automática y no intentará rotarlo de nuevo, incluso después de reanudar el clúster. Debe reiniciar el programa de rotación automática mediante la llamada a la API `secretsmanager:RotateSecret` para que AWS Secrets Manager siga rotando automáticamente el secreto.
- Si su espacio de nombres sin servidor no tiene ningún grupo de trabajo asociado cuando Amazon Redshift intente rotar el secreto que tiene asociado, la rotación fallará y no volverá a intentar rotarlo, incluso después de adjuntar un grupo de trabajo. Debe reiniciar el programa de rotación automática mediante la llamada a la API `secretsmanager:RotateSecret` para que AWS Secrets Manager siga rotando automáticamente el secreto.

Registro y monitoreo en Amazon Redshift

El monitoreo es una parte importante a la hora de mantener la fiabilidad, la disponibilidad y el rendimiento de Amazon Redshift y sus soluciones de AWS. Puede recopilar datos de monitoreo de todas las partes de su solución de AWS para que pueda depurar un error multipunto de una forma más fácil si se produce. AWS proporciona varias herramientas para monitorear sus recursos de Amazon Redshift y responder a posibles incidentes:

Alarmas de Amazon CloudWatch

Con las alarmas de Amazon CloudWatch, puede ver una métrica determinada durante el periodo especificado. Si la métrica supera un límite determinado, se envía una notificación a un tema de Amazon SNS o a una política de AWS Auto Scaling. Las alarmas de CloudWatch no invocan acciones simplemente porque se encuentren en determinado estado. En su lugar, el estado debe haber cambiado y debe mantenerse durante el número de periodos especificado. Para obtener más información, consulte Administración de alarmas. Para ver una lista de métricas, consulte Monitoreo de Amazon Redshift mediante las métricas de CloudWatch.

AWS CloudTrailRegistros de

CloudTrail proporciona un registro de las operaciones de la API adoptadas por un usuario, un rol de IAM o un servicio de AWS en Amazon Redshift. Con la información que recopila CloudTrail, se puede determinar la solicitud que se realizó a Amazon Redshift la dirección IP desde la que se

realizó, quién la realizó, cuándo la realizó y detalles adicionales. Para obtener más información, consulte Registro con CloudTrail.

Registro de auditoría de bases de datos

Amazon Redshift registra información acerca de las conexiones y las actividades del usuario en la base de datos. Estos registros ayudan a monitorear la base de datos con fines de seguridad y solución de problemas; un proceso denominado auditoría de base de datos. Los registros se pueden almacenar en:

- Buckets de Simple Storage Service (Amazon S3): ofrecen acceso con características de seguridad de datos a los usuarios que se encargan de las actividades de supervisión de la base de datos.
- Amazon CloudWatch: puede consultar los datos de registro de auditoría mediante las características integradas en CloudWatch, como las características de visualización y las acciones de configuración.

> **Note**
>
> SYS_CONNECTION_LOG recopila datos de registro de conexión para Amazon Redshift sin servidor. Tenga en cuenta que, cuando recopile datos de registro de auditoría para Amazon Redshift sin servidor, estos no se pueden enviar a archivos de registro, solo a CloudWatch.

Temas

- Registros de Amazon Redshift
- Habilitación de registros
- Envío de registros de auditoría a Amazon CloudWatch
- Administración de archivos de registro en Amazon S3
- Solución de problemas en el registro de auditoría de Amazon Redshift en Simple Storage Service (Amazon S3)
- Registro de llamadas a la API de Amazon Redshift con AWS CloudTrail
- Configuración de la auditoría con la consola
- Configuración del registro mediante la AWS CLI y la API de Amazon Redshift

Registros de Amazon Redshift

Amazon Redshift registra información en los siguientes archivos de registro:

- Registro de conexión: registra los intentos de autenticación, las conexiones y las desconexiones.
- Registro de usuario: registra la información sobre los cambios en las definiciones del usuario de la base de datos.
- Registro de la actividad de usuario: registra cada consulta antes de su ejecución en la base de datos.

Los registros de usuario y de conexión son útiles principalmente por fines de seguridad. Puede utilizar el registro de conexión para monitorear la información sobre los usuarios que se conectan a la base de datos y la información de conexión relacionada. Esta información puede ser su dirección IP, cuándo hicieron la solicitud, qué tipo de autenticación utilizaron, etc. Puede utilizar el registro de usuario para monitorear los cambios en las definiciones de los usuarios de la base de datos.

El registro de actividad de usuario es útil principalmente para la solución de problemas. Realiza un seguimiento de la información acerca de las consultas que realizan los usuarios y el sistema en la base de datos.

El registro de conexión y el registro de usuario corresponden a la información que se almacena en las tablas de sistema de la base de datos. Puede utilizar las tablas de sistema para obtener la misma información, pero los archivos de registro proporcionan un mecanismo más sencillo de recuperación y revisión. Los archivos de registro dependen de los permisos de Amazon S3, en lugar de los permisos de la base de datos para realizar consultas en las tablas. Además, al revisar la información de los archivos de registro en lugar de consultar las tablas de sistema, se reduce cualquier impacto de interacción con la base de datos.

> **Note**
>
> Los archivos de registro no son tan actuales como las tablas de registro del sistema que son STL_USERLOG y STL_CONNECTION_LOG. Los registros que son más antiguos que el registro más reciente (sin incluir este) se copian en archivos log.

> **Note**
>
> En el caso de Amazon Redshift sin servidor, SYS_CONNECTION_LOG recopila los datos del registro de conexiones. Cuando recopile datos de registro de auditoría para Amazon Redshift sin servidor, estos no se pueden enviar a archivos de registro, solo a CloudWatch.

Registro de conexión

Registra los intentos de autenticación y las conexiones y desconexiones. En la siguiente tabla se describe la información del registro de conexión. Para obtener más información sobre estos campos, consulte STL_CONNECTION_LOG en la Guía para desarrolladores de bases de datos Amazon Redshift. Para obtener más información sobre los datos de registro de conexiones recopilados para Amazon Redshift sin servidor, consulte SYS_CONNECTION_LOG.

Nombre de la columna	Descripción
evento	Evento de conexión o de autenticación.
recordtime	Hora cuando se produjo el evento.
remotehost	Nombre o dirección IP del host remoto.
remoteport	Número del puerto para el host remoto.
pid	ID del proceso asociado a la instrucción.
dbname	Nombre de la base de datos.
username	Nombre de usuario.
authmethod	Método de autenticación.
duration	Duración de la conexión en microsegundos.
sslversion	Versión de la capa de conexión segura (SSL).
sslcipher	Cifrado SSL.

Nombre de la columna	Descripción
mtu	Unidad de transmisión máxima (MTU).
sslcompression	Tipo de compresión de la SSL.
sslexpansion	Tipo de expansión de la SSL.
iamauthguid	ID de autenticación de AWS Identity and Access Management (IAM) para la solicitud de AWS CloudTrail. Este es el identificador de la llamada a la API GetClusterCredentials para crear las credenciales que se utilizan para una conexión determinada.
application_name	Nombre original o actualizado de la aplicación para una sesión.
os_version	La versión del sistema operativo que se encuentra en el equipo cliente que se conecta a su clúster de Amazon Redshift.
driver_version	La versión del controlador ODBC o JDBC que se conecta a su clúster de Amazon Redshift desde las herramientas de cliente SQL de terceros.
plugin_name	El nombre del complemento utilizado para conectarse a su clúster de Amazon Redshift.
protocol_version	La versión del protocolo interno que utiliza el controlador de Amazon Redshift cuando se establece su conexión con el servidor.
sessionid	El identificador único global de la sesión actual.
compression	Algoritmo de compresión que se utiliza para la conexión.

Registro de usuario

Registra detalles de los siguientes cambios realizados en un usuario de una base de datos:

- Creación de usuario
- Eliminación de usuario

- Modificación de usuario (cambio de nombre)
- Modificación de usuario (modificación de propiedades)

Nombre de la columna	Descripción
userid	ID de usuario afectado por el cambio.
username	Nombre del usuario afectado por el cambio.
oldusername	En el caso de una acción de cambio de nombre, el nombre de usuario original. Para el resto de las acciones, este campo está vacío.
acción	Acción que ocurrió. Valores válidos: • Modificación • Creación • Drop (Eliminar) • Cambio de nombre
usecreatedb	Si es true (1), indica que el usuario ha creado permisos de base de datos.
usesuper	Si es true (1), indica que el usuario es un superusuario.
usecatupd	Si es true (1), indica que el usuario puede actualizar los catálogos de sistema.
valuntil	Fecha de vencimiento de la contraseña.
pid	Identificador del proceso.
xid	ID de transacción.
recordtime	Hora en UTC en que comenzó la consulta.

Consulte la vista del sistema SYS_USERLOG para encontrar información adicional sobre los cambios en los usuarios. Esta vista incluye datos de registro de Amazon Redshift sin servidor.

Registro de actividad de usuario

Registra cada consulta antes de su ejecución en la base de datos.

Nombre de la columna	Descripción
recordtime	Hora cuando se produjo el evento.
db	Nombre de la base de datos.
usuario	Nombre de usuario.
pid	ID del proceso asociado a la instrucción.
userid	ID de usuario.
xid	ID de transacción.
consulta	Prefijo de LOG: seguido del texto de la consulta, incluidas las líneas nuevas.

Habilitación de registros

El registro de auditoría no está habilitado de forma predeterminada en Amazon Redshift. Cuando activa el registro en el clúster, Amazon Redshift exporta registros a Amazon CloudWatch o crea y actualiza registros en Simple Storage Service (Amazon S3) que capturan los datos desde el momento en que se habilita el registro de auditoría hasta el momento actual. Cada actualización de registros es una continuación de los registros anteriores.

El registro de auditoría a CloudWatch o Simple Storage Service (Amazon S3) es un proceso opcional. El registro en las tablas de sistema no es opcional y ocurre automáticamente. Para obtener más información acerca de los registros en las tablas de sistema, consulte Referencia de las tablas de sistema en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Los registros de conexión, usuario y actividad del usuario se habilitan juntos a través de la AWS Management Console, la referencia de la API de Amazon Redshift o la AWS Command Line Interface (AWS CLI). Para el registro de actividad de usuario, también debe habilitar el parámetro `enable_user_activity_logging` de la base de datos. Si habilita solo la función de registro de auditoría y no el parámetro asociado, los registros de auditoría de la base de datos registrarán

únicamente la información de los registros de conexión y de usuario, no la del registro de actividad del usuario. El parámetro de `enable_user_activity_logging` no está habilitado (`false`) de forma predeterminada. Puede configurarlo como `true` para habilitar el registro de actividad del usuario. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift.

Envío de registros de auditoría a Amazon CloudWatch

Al habilitar el registro en CloudWatch, Amazon Redshift exporta datos de registro de conexión de clúster, usuario y actividad de usuario a un grupo de registros de Amazon CloudWatch Logs. Los datos de registro no cambian, en términos de esquema. CloudWatch está diseñado para aplicaciones de supervisión y puede utilizarlo para realizar análisis en tiempo real o configurarlo para que realice acciones. También puede utilizar Amazon CloudWatch Logs para almacenar los registros en un almacenamiento de larga duración.

El uso de CloudWatch para consultar los registros es una alternativa recomendada para almacenar archivos de registro en Amazon S3. No requiere mucha configuración y se puede ajustar a los requisitos de supervisión, especialmente si ya lo utiliza para supervisar otros servicios y aplicaciones.

Grupos de registro y eventos de registro de Amazon CloudWatch

Una vez seleccionados los registros de Amazon Redshift que se exportarán, puede monitorear los eventos de registro en Amazon CloudWatch Logs. A continuación, se crea automáticamente un nuevo grupo de registros para Amazon Redshift Serverless con el siguiente prefijo, en el que `log_type` representa el tipo de registro.

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

Por ejemplo, si elige exportar el registro de conexiones, los datos de registro se almacenan en el siguiente grupo de registros.

```
/aws/redshift/cluster/cluster1/connectionlog
```

Los eventos de registro se exportan a un grupo de registro mediante el flujo de registro. Utilice la consola de Amazon CloudWatch Logs, la AWS CLI o la API de Amazon CloudWatch Logs para buscar información en los eventos de registro para su punto de conexión sin servidor. Para obtener información sobre la búsqueda y el filtrado de datos de registro, consulte Creación de métricas a partir de eventos de registro mediante filtros.

En CloudWatch, puede buscar los datos de registro con una sintaxis de consulta que proporciona grado de detalle y flexibilidad. Para obtener más información, consulte Sintaxis de consulta de información de registros de CloudWatch.

Migración al registro de auditoría de Amazon CloudWatch

En cualquier caso en que envíe registros a Amazon S3 y cambie la configuración, por ejemplo, para enviar registros a CloudWatch, los registros que permanecen en Amazon S3 no se verán afectados. Puede consultar los datos de registro en los buckets de Amazon S3 en los que residen.

Administración de archivos de registro en Amazon S3

El número y el tamaño de los archivos de registro de Amazon Redshift en Amazon S3 dependen en gran medida de la actividad de su clúster. Si tiene un clúster activo que genera un gran número de registros, es posible que Amazon Redshift genere los archivos de registro con mayor frecuencia. Es posible que tenga una serie de archivos de registro para el mismo tipo de actividad, como tener varios registros de conexión en la misma hora.

Cuando Amazon Redshift utiliza Simple Storage Service (Amazon S3) para almacenar registros, usted incurre en cargos por el almacenamiento que utilice en Simple Storage Service (Amazon S3). Antes de configurar el registro en Simple Storage Service (Amazon S3), debe tener pensado durante cuánto tiempo necesita almacenar los archivos de registro. Como parte de esto, determine cuándo se pueden eliminar o archivar los archivos de registro según las necesidades de auditoría. El plan que cree depende en gran medida del tipo de datos que almacene, como datos sujetos a requisitos normativos o de conformidad. Para obtener más información acerca de los precios de Amazon S3, vaya a Precios de Amazon Simple Storage Service (S3).

Limitaciones al habilitar el registro en Amazon S3

El registro de la auditoría tiene las siguientes restricciones:

- Solo puede utilizar el cifrado (AES-256) de las claves administradas por Amazon S3 (SSE-S3).
- Los buckets de Amazon S3 deben tener desactivada la característica de bloqueo de objetos de S3.

Permisos del bucket para el registro de auditoría de Amazon Redshift

Cuando activa el registro en Simple Storage Service (Amazon S3), Amazon Redshift recopila la información de los registros y la carga en los archivos de registro almacenados en Simple Storage Service (Amazon S3). Puede utilizar un bucket existente o uno nuevo. Amazon Redshift requiere los siguientes permisos de IAM para el bucket:

- `s3:GetBucketAcl` El servicio requiere permisos de lectura para el bucket de Amazon S3 de manera que se pueda identificar al propietario del bucket.
- `s3:PutObject` El servicio requiere permisos de colocación de objetos para cargar los registros. Además, el usuario o el rol de IAM que habilitan el registro deben tener el permiso `s3:PutObject` para el bucket de Amazon S3. Cada vez que se cargan registros, el servicio determina si el propietario del bucket actual coincide con el propietario del bucket en el momento que se habilitó el registro. Si estos propietarios no coinciden, recibirá un error.

Si, cuando habilita el registro de auditoría, selecciona la opción para crear un bucket nuevo, se le aplicarán los permisos correctos. Sin embargo, si crea su propio bucket en Amazon S3 o utiliza un bucket existente, asegúrese de agregar una política de bucket que incluya el nombre del bucket. Los registros se envían mediante las credenciales principales del servicio. Para la mayoría de las Regiones de AWS, agrega el nombre principal del servicio Redshift, *`redshift.amazonaws.com`*.

La política de bucket utiliza el siguiente formato. *`ServiceName`* y *`BucketName`* son marcadores de posición de sus propios valores. Especifique también las acciones y los recursos asociados en la política de bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "Service": "ServiceName"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::BucketName",
                "arn:aws:s3:::BucketName/*"
            ]
        }
    ]
}
```

En el siguiente ejemplo, se muestra una política de bucket para la región Este de EE. UU. (Norte de Virginia) y un bucket denominado `AuditLogs`.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::AuditLogs",
                "arn:aws:s3:::AuditLogs/*"
            ]
        }
    ]
}
```

Las regiones que no están habilitadas de forma predeterminada, también conocidas como regiones "registradas", requieren un nombre principal del servicio específico de la región. Para ello, el nombre principal del servicio incluye la región, con el formato `redshift.`*`region`*`.amazonaws.com`. Por ejemplo, *`redshift.ap-east-1.amazonaws.com`* para la región Asia-Pacífico (Hong Kong). Para obtener una lista de las regiones que no están habilitadas de forma predeterminada, consulte Administración de las Regiones de AWS en la Referencia general de AWS.

> **Note**
>
> El nombre de la entidad principal del servicio específico de la región corresponde a la región en la que se encuentra el clúster.

Prácticas recomendadas para los archivos de registro

Cuando Redshift carga archivos de registro en Amazon S3, los archivos grandes se pueden cargar en partes. Si una carga multiparte no se realiza correctamente, es posible que algunas partes de un

archivo permanezcan en el bucket de Amazon S3. Esto puede generar costos de almacenamiento adicionales, por lo que es importante comprender qué ocurre cuando se produce un error con una carga multiparte. Para obtener una explicación detallada sobre la carga multiparte para los registros de auditoría, consulte Carga y copia de objetos con la carga multiparte y Anulación de la carga multiparte.

Para obtener más información sobre la creación de buckets de S3 y la incorporación de políticas de bucket, consulte Creación de un bucket y Edición de permisos de bucket en la Guía del usuario de Amazon Simple Storage Service.

Estructura del bucket para el registro de auditoría de Amazon Redshift

De forma predeterminada, Amazon Redshift organiza los archivos de registro en el bucket de Amazon S3 utilizando la siguiente estructura de bucket y objetos:

```
AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region
```

Un ejemplo es: `AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`.

Si proporciona un prefijo de clave de Amazon S3, colóquelo al comienzo de la clave.

Por ejemplo, si especifica un prefijo de myprefix: `myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

El prefijo de clave de Amazon S3 no puede tener más de 512 caracteres. No puede contener espacios ( ), comillas dobles (“), comillas simples (‘) ni una barra inversa (\). También existe una cantidad de caracteres especiales y de control que no están permitidos. Los códigos hexadecimales para estos caracteres son de la siguiente manera:

- de x00 a x20
- x22
- x27
- x5c
- x7f o mayores

Solución de problemas en el registro de auditoría de Amazon Redshift en Simple Storage Service (Amazon S3)

El registro de auditoría de Amazon Redshift puede interrumpirse por las siguientes razones:

- Amazon Redshift no tiene permiso para cargar registros en el bucket de Amazon S3. Compruebe que el bucket esté configurado con la política de IAM correcta. Para obtener más información, consulte Permisos del bucket para el registro de auditoría de Amazon Redshift.
- Cambió el propietario del bucket. Cuando Amazon Redshift carga los registros, comprueba que el propietario del bucket sea el mismo que cuando se habilitó el registro. Si el propietario del bucket ha cambiado, Amazon Redshift no puede cargar los registros hasta que configure otro bucket para utilizarlo en el registro de auditoría.
- No se ha encontrado el bucket. Si el bucket se elimina en Amazon S3, Amazon Redshift no puede cargar los registros. Debe volver a crear el bucket o configurar Amazon Redshift para cargar los registros en un bucket diferente.

Registro de llamadas a la API de Amazon Redshift con AWS CloudTrail

Amazon Redshift se integra a AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon Redshift. CloudTrail captura todas las llamadas a la API para Amazon Redshift como eventos. Para obtener más información acerca de la integración de Amazon Redshift con AWS CloudTrail, consulte Registro con CloudTrail.

Puede utilizar CloudTrail de forma independiente o junto con el registro de auditoría de base de datos de Amazon Redshift.

Para más información sobre CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Configuración de la auditoría con la consola

Configure Amazon Redshift para exportar datos de registros de auditoría. Los registros se pueden exportar a CloudWatch o como archivos a buckets de Amazon S3.

Habilitación del registro de auditoría con la consola

Pasos de la consola

Para habilitar el registro de auditoría de un clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y elija el clúster que desee actualizar.
3. Elija la pestaña Propiedades. En el panel Database configurations (Configuraciones de bases de datos), elija Edit (Editar) y, a continuación, Edit audit logging (Editar registro de auditoría).
4. En la página Edit audit logging (Editar registro de auditoría), elija Turn on (Activar) y seleccione S3 bucket (Bucket de S3) o CloudWatch. Recomendamos utilizar CloudWatch porque la administración es sencilla y tiene características útiles para la visualización de datos.
5. Elija qué registros desea exportar.
6. Para guardar sus elecciones, elija Save changes (Guardar cambios).

Configuración del registro mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para configurar el registro de auditoría:

- describe-logging-status
- disable-logging
- enable-logging

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para configurar el registro de auditoría:

- DescribeLoggingStatus
- DisableLogging
- EnableLogging

Registro con CloudTrail

Registro de llamadas con AWS CloudTrail

El uso compartido de datos de Amazon Redshift, Amazon Redshift Serverless, la API de datos de Amazon Redshift y el editor de consultas v2 están integrados con AWS CloudTrail. CloudTrail es un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon Redshift. CloudTrail captura todas las llamadas a la API para Amazon Redshift como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Redshift y llamadas de código a las operaciones de Redhisft.

Si crea un registro de seguimiento CloudTrail, puede tener la entrega continua de eventos de CloudTrail en un bucket de Amazon S3, incluidos los eventos de Redshift. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Con la información recopilada por CloudTrail, se pueden determinar ciertos detalles. Estos incluyen la solicitud que se realizó a Redshift, la dirección IP desde la que se realizó, quién la realizó, cuándo la realizó y detalles adicionales.

Puede utilizar CloudTrail de forma independiente o junto con el registro de auditoría de base de datos de Amazon Redshift.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Trabajar con información en CloudTrail

CloudTrail se enciende en su cuenta de AWS cuando la crea. Cuando se produce una actividad, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail en la Guía del usuario de AWS CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Amazon Redshift, cree un registro de seguimiento. CloudTrail utiliza registros de seguimiento para entregar los archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte lo indicado en la Guía del usuario de AWS CloudTrail:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configurar notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Amazon Redshift, Amazon Redshift Serverless, la API de datos, el uso compartido de datos y el editor de consultas v2 las registra CloudTrail. Por ejemplo, las llamadas a las acciones `AuthorizeDatashare`, `CreateNamespace`, `ExecuteStatement` y `CreateConnection` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail en la Guía del usuario de AWS CloudTrail.

Descripción de las entradas de los archivos de registro

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros a un bucket de Amazon S3 que se especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Ejemplo de recurso compartido de datos de Amazon Redshift

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la operación `AuthorizeDataShare`.

```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
                "arn": "arn:aws:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "janedoe"
            },
            "attributes": {
                "creationDate": "2021-08-02T23:40:45Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2021-08-02T23:40:58Z",
    "eventSource": "redshift.amazonaws.com",
    "eventName": "AuthorizeDataShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.227.36.75",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "consumerIdentifier": "555555555555"
    },
    "responseElements": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "allowPubliclyAccessibleConsumers": true,
        "dataShareAssociations": [
            {
                "consumerIdentifier": "555555555555",
                "status": "AUTHORIZED",
```

```
                "createdDate": "Aug 2, 2021 11:40:56 PM",
                "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
            }
        ]
    },
    "requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
    "eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Ejemplo de Amazon Redshift Serverless

Amazon Redshift Serverless está integrado con AWS CloudTrail para proporcionar un registro de las acciones realizadas en Amazon Redshift Serverless. CloudTrail captura todas las llamadas a la API de Amazon Redshift Serverless como eventos. Para obtener más información acerca de las funciones de Amazon Redshift Serverless, consulte Información general sobre las características de Amazon Redshift Serverless.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `CreateNamespace`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:admin",
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
        "accountId": "111111111111",
        "accessKeyId": "AAKEOFPINEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::111111111111:role/admin",
                "accountId": "111111111111",
                "userName": "admin"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2022-03-21T20:51:58Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-21T23:15:40Z",
    "eventSource": "redshift-serverless.amazonaws.com",
    "eventName": "CreateNamespace",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "56.23.155.33",
    "userAgent": "aws-cli/2.4.14 Python/3.8.8 Linux/5.4.181-109.354.amzn2int.x86_64
 exe/x86_64.amzn.2 prompt/off command/redshift-serverless.create-namespace",
    "requestParameters": {
        "adminUserPassword": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "dbName": "dev",
        "namespaceName": "testnamespace"
    },
    "responseElements": {
        "namespace": {
            "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
            "creationDate": "Mar 21, 2022 11:15:40 PM",
            "defaultIamRoleArn": "",
            "iamRoles": [],
            "logExports": [],
            "namespaceArn": "arn:aws:redshift-serverless:us-
east-1:111111111111:namespace/befa5123-16c2-4449-afca-1d27cb40fc99",
            "namespaceId": "8b726a0c-16ca-4799-acca-1d27cb403599",
            "namespaceName": "testnamespace",
            "status": "AVAILABLE"
        }
    },
    "requestID": "ed4bb777-8127-4dae-aea3-bac009999163",
    "eventID": "1dbee944-f889-4beb-b228-7ad0f312464",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
}
```

Ejemplo de la API de datos de Amazon Redshift

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `ExecuteStatement`.


```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `ExecuteStatement` que presenta el `clientToken` que se usa para la idempotencia.


```
{
    "eventVersion":"1.05",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn":"arn:aws:sts::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
        "userName": "janedoe"
    },
    "eventTime":"2020-08-19T17:55:59Z",
    "eventSource":"redshift-data.amazonaws.com",
    "eventName":"ExecuteStatement",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"192.0.2.0",
    "userAgent":"aws-cli/1.18.118 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
    "requestParameters":{
        "clusterIdentifier":"example-cluster-identifier",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "sql":"***OMITTED***",
        "clientToken":"32db2e10-69ac-4534-b3fc-a191052616ce"
    },
    "responseElements":{
        "clusterIdentifier":"example-cluster-identifier",
        "createdAt":"Aug 19, 2020 5:55:58 PM",
        "database":"example-database-name",
        "dbUser":"example_db_user_name",
        "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
    },
    "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
    "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "recipientAccountId":"123456789012"
}
```

Ejemplo de editor de consultas de Amazon Redshift v2

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `CreateConnection`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAKEOFPINEXAMPLE:session",
        "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAKEOFPINEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/MyRole",
                "accountId": "123456789012",
                "userName": "MyRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-09-21T17:19:02Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-21T22:22:05Z",
    "eventSource": "sqlworkbench.amazonaws.com",
    "eventName": "CreateConnection",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "192.2.0.2",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
 Gecko/20100101 Firefox/102.0",
    "requestParameters": {
        "password": "***",
        "databaseName": "***",
        "isServerless": false,
        "name": "***",
        "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
        "authenticationType": "***",
        "clusterId": "redshift-cluster-2",
```

```
        "username": "***",
        "tags": {
            "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
        }
    },
    "responseElements": {
        "result": true,
        "code": "",
        "data": {
            "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
            "name": "***",
            "authenticationType": "***",
            "databaseName": "***",
            "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
            "clusterId": "redshift-cluster-2",
            "dbUser": "***",
            "userSettings": "***",
            "recordDate": "2022-09-21 22:22:05",
            "updatedDate": "2022-09-21 22:22:05",
            "accountId": "123456789012",
            "tags": {
                "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
            },
            "isServerless": false
        }
    },
    "requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
    "eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


ID de cuenta de Amazon Redshift en registros de AWS CloudTrail

Cuando Amazon Redshift llama a otro servicio de AWS en su nombre, la llamada se registra con un ID de cuenta que pertenece a Amazon Redshift. No se registra con su ID de cuenta. Por ejemplo, supongamos que Amazon Redshift llama a las operaciones de AWS Key Management Service (AWS KMS) tales como `CreateGrant`, `Decrypt`, `Encrypt` y `RetireGrant` para administrar el

cifrado en su clúster. En este caso, AWS CloudTrail registra las llamadas con un ID de cuenta de Amazon Redshift.

Amazon Redshift utiliza los ID de cuenta de la siguiente tabla cuando llama a otros servicios de AWS.

Región	Región	ID de cuenta
Región del este de EE. UU. (Norte de Virginia)	us-east-1	368064434614
Región del este de EE. UU. (Ohio)	us-east-2	790247189693
Región del oeste de EE. UU. (Norte de California)	us-west-1	703715109447
Región del Oeste de EE. UU. (Oregón)	us-west-2	473191095985
Región África (Ciudad del Cabo)	af-south-1	420376844563
Región de Asia-Pacífico (Hong Kong)	ap-east-1	651179539253
Región Asia Pacífico (Hyderabad)	ap-south-2	297058826802
Región Asia-Pacífico (Yakarta)	ap-southeast-3	623197973179
Región Asia-Pacífico (Melbourne)	ap-southeast-4	945512339897
Región de Asia-Pacífico (Bombay)	ap-south-1	408097707231
Región Asia-Pacífico (Osaka)	ap-northeast-3	398671365691
Región de Asia-Pacífico (Seúl)	ap-northeast-2	713597048934

Región	Región	ID de cuenta
Región Asia Pacífico (Singapur)	ap-southeast-1	960118270566
Región Asia Pacífico (Sídney)	ap-southeast-2	485979073181
Región Asia Pacífico (Tokio)	ap-northeast-1	615915377779
Región de Canadá (centro)	ca-central-1	764870610256
Región de Oeste de Canadá (Calgary)	ca-west-1	830903446466
Región de Europa (Fráncfort)	eu-central-1	434091160558
Región de Europa (Irlanda)	eu-west-1	246478207311
Región de Europa (Londres)	eu-west-2	885798887673
Región Europa (Milán)	eu-south-1	041313461515
Región Europa (París)	eu-west-3	694668203235
Región Europa (España)	eu-south-2	028811157404
Región de Europa (Estocolmo)	eu-north-1	553461782468
Región Europa (Zúrich)	eu-central-2	668912161003
Región Israel (Tel Aviv)	il-central-1	901883065212
Región Medio Oriente (Baréin)	me-south-1	051362938876
Región Medio Oriente (EAU)	me-central-1	595013617770
Región de América del Sur (São Paulo)	sa-east-1	392442076723

En el siguiente ejemplo, se muestra una entrada del registro de CloudTrail para la operación Decrypt de AWS KMS a la que ha llamado Amazon Redshift.

```
{

    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
        "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/
i-0f53e22dbe5df8a89",
        "accountId": "790247189693",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2017-03-03T16:24:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAI5QPCMKLTL4VHFCYY",
                "arn": "arn:aws:iam::790247189693:role/prod-23264-role-wp",
                "accountId": "790247189693",
                "userName": "prod-23264-role-wp"
            }
        }
    },
    "eventTime": "2017-03-03T17:16:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "52.14.143.61",
    "userAgent": "aws-internal/3",
    "requestParameters": {
        "encryptionContext": {
            "aws:redshift:createtime": "20170303T1710Z",
            "aws:redshift:arn": "arn:aws:redshift:us-east-2:123456789012:cluster:my-dw-
instance-2"
        }
    },
    "responseElements": null,
    "requestID": "30d2fe51-0035-11e7-ab67-17595a8411c8",
    "eventID": "619bad54-1764-4de4-a786-8898b0a7f40c",
    "readOnly": true,
    "resources": [
        {
```

```
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/f8f4f94f-e588-4254-
b7e8-078b99270be7",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012",
    "sharedEventID": "c1daefea-a5c2-4fab-b6f4-d8eaa1e522dc"

}
```

Validación de la conformidad para Amazon Redshift

Los auditores externos evalúan la seguridad y la conformidad de Amazon Redshift en distintos programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de AWS servicios en el ámbito de programas de cumplimiento específicos, consulte los AWS servicios en ámbito por programa de cumplimiento. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros con AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad en cuanto a la conformidad al utilizar Amazon Redshift se determina en función del nivel de confidencialidad que requieren los datos, los objetivos de conformidad de su organización, así como la legislación y la normativa aplicables. Si su uso de Amazon Redshift está sujeto a la conformidad con ciertos estándares, como HIPAA, PCI o FedRAMP, AWS proporciona recursos de ayuda:

- En las Guías de inicio rápido de seguridad y conformidad, se incluyen consideraciones sobre arquitectura y se ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA, que describe cómo las empresas pueden utilizar AWS para crear aplicaciones conforme con HIPAA.
- Recursos de conformidad de AWS, manuales y guías que podrían aplicarse a su sector y ubicación.
- AWS Config, servicio de AWS, puede evaluar en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y las normativas.

- AWS Security Hub, un servicio de AWS, proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad. Security Hub utiliza controles de seguridad para evaluar las configuraciones de los recursos y los estándares de seguridad para ayudarlo a cumplir con varios marcos de conformidad. Para obtener más información sobre el uso de Security Hub para evaluar los recursos de Amazon Redshift, consulte Controles de Amazon Redshift en la Guía del usuario de AWS Security Hub.

En los siguientes documentos de conformidad y seguridad, se aborda el tema de Amazon Redshift y están disponibles bajo demanda a través de AWS Artifact. Para obtener más información, consulte AWS Artifact.

- Catálogo de controles de conformidad de informática en la nube (C5)
- Declaración de aplicabilidad (SoA) de ISO 27001:2013
- Certificación ISO 27001:2013
- Declaración de aplicabilidad (SoA) de ISO 27017:2015
- Certificación ISO 27017:2015
- Declaración de aplicabilidad (SoA) de ISO 27018:2015
- Certificación ISO 27018:2014
- Certificación ISO 9001:2015
- Declaración de conformidad (AOC) PCI DSS y resumen de responsabilidad
- Informe de controles de organizaciones de servicios (SOC) 1
- Informe de controles de organizaciones de servicios (SOC) 2
- Informe de controles de organizaciones de servicios (SOC) 2 para la confidencialidad

Resiliencia en Amazon Redshift

La infraestructura global de AWS está compuesta por regiones y zonas de disponibilidad (AZ) de AWS. Las regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad,

tolerancia a errores y escalabilidad que las infraestructuras de centros de datos tradicionales únicos o múltiples.

Casi todas las regiones de AWS tienen varias zonas de disponibilidad y centros de datos. Puede implementar sus aplicaciones en varias zonas de disponibilidad en la misma región para la tolerancia de errores y la baja latencia.

Para mover un clúster a otra zona de disponibilidad sin pérdida de datos ni cambios en las aplicaciones, puede configurar la reubicación del clúster. Con la reubicación, puede continuar las operaciones cuando hay una interrupción del servicio en el clúster con un impacto mínimo. Cuando la reubicación de clústeres está activada, Amazon Redshift puede elegir reubicar clústeres en algunas situaciones. Para obtener más información sobre la reubicación en Amazon Redshift, consulte Reubicación del clúster.

En escenarios de error en los que se produzca un evento inesperado en una zona de disponibilidad, puede establecer una implementación de varias zonas de disponibilidad (Multi-AZ) para garantizar que su almacenamiento de datos de Amazon Redshift pueda seguir funcionando. Amazon Redshift despliega recursos de computación iguales en dos zonas de disponibilidad a las que se puede acceder a través de un único punto de conexión. En caso de que se produzca un error en toda la zona de disponibilidad, los recursos de computación restantes de la segunda zona de disponibilidad estarán disponibles para seguir procesando las cargas de trabajo. Para obtener más información acerca de las implementaciones Multi-AZ, consulte Configuración de la implementación multi-AZ.

Para obtener más información acerca de las zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Seguridad de la infraestructura de Amazon Redshift

Como se trata de un servicio administrado, Amazon Redshift está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas de AWS para acceder a Amazon Redshift a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.

- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de red

Una nube virtual privada (VPC) basada en el servicio Amazon VPC es su red privada y aislada de manera lógica en la nube de AWS. Puede implementar un clúster de Amazon Redshift en una VPC completando los siguientes pasos:

- Cree una VPC en una región de AWS. Para obtener más información, consulte ¿Qué es Amazon VPC? en la Guía del usuario de Amazon VPC.
- Cree dos o más subredes de VPC privadas. Para obtener más información, consulte VPC y subredes en la Guía del usuario de Amazon VPC.
- Implemente un clúster de Amazon Redshift. Para obtener más información, consulte Grupos de subredes del clúster de Amazon Redshift.

Los clústeres de Amazon Redshift se encuentran bloqueados de forma predeterminada desde el aprovisionamiento. Para permitir el tráfico de red entrante de los clientes de Amazon Redshift, asocie un grupo de seguridad de VPC a un clúster de Amazon Redshift. Para obtener más información, consulte Grupos de subredes del clúster de Amazon Redshift.

Para permitir el tráfico solo hacia o desde rangos de direcciones IP específicos, actualice los grupos de seguridad con su VPC. Un ejemplo consiste en permitir el tráfico solo desde o hacia su red corporativa.

Al configurar las listas de control de acceso a la red asociadas con las subredes con las que está etiquetado el clúster de Amazon Redshift, asegúrese de que los intervalos de CIDR de S3 de la región de AWS se agreguen a la lista de permitidos para las reglas de entrada y de salida. Esto le permite ejecutar operaciones basadas en S3, como Redshift Spectrum, COPY y UNLOAD, sin interrupciones.

El siguiente comando de ejemplo analiza la respuesta JSON de todas las direcciones IPv4 utilizadas en Amazon S3 en la región us-east-1.

```
curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] |
 select(.region=="us-east-1") | select(.service=="S3") | .ip_prefix'

54.231.0.0/17

52.92.16.0/20

52.216.0.0/15
```

Para obtener instrucciones sobre cómo conseguir rangos de IP de S3 para una región en particular, consulte Rangos de direcciones IP de AWS.

Amazon Redshift admite la implementación de clústeres en las VPC de tenencia dedicada. Para obtener más información, consulte Instancias dedicadas en la Guía del usuario de Amazon EC2.

Grupos de seguridad del clúster de Amazon Redshift

Cuando aprovisiona un clúster de Amazon Redshift, se bloquea de forma predeterminada para que nadie pueda obtener acceso a él. Para concederle a otros usuarios acceso de entrada a un clúster de Amazon Redshift, debe asociar el clúster a un grupo de seguridad. Si está en la plataforma de EC2-VPC, puede utilizar un grupo de seguridad de Amazon VPC ya existente o definir uno nuevo y luego asociarlo a un clúster. Para obtener más información acerca de la administración de un clúster en la plataforma de EC2-VPC, consulte Administración de clústeres en una VPC.

Si está en la plataforma EC2-Classic, defina un grupo de seguridad de clúster y asócielo a un clúster. Se retirará la plataforma EC2-Classic. Le recomendamos que lance el clúster en una plataforma EC2-VPC en lugar de hacerlo en una plataforma EC2-Classic. Sin embargo, puede restaurar una instantánea de EC2-Classic en un clúster EC2-VPC a través de la consola de Amazon Redshift. Para obtener más información, consulte Restauración de un clúster desde una instantánea .

Conexión a Amazon Redshift mediante un punto de enlace de la VPC de interfaz

Puede conectarse directamente al servicio de API de Amazon Redshift mediante un punto de enlace de la VPC de interfaz (AWS PrivateLink) en su nube virtual privada (VPC) en lugar de conectarse a través de Internet. Para obtener más información sobre las acciones de la API de Amazon Redshift, consulte Acciones en la Referencia de la API de Amazon Redshift. Para obtener más información

acerca de AWS PrivateLink, consulte Puntos de enlace de la VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC. Tenga en cuenta que la conexión JDBC/ODBC al clúster no forma parte del servicio de API de Amazon Redshift.

Cuando utiliza un punto de enlace de la VPC de interfaz, la comunicación entre la VPC y Amazon Redshift se realiza en su totalidad dentro de la red de AWS, la cual puede proporcionar más seguridad. Cada punto de enlace de la VPC está representado por una o varias interfaces de red elástica con direcciones IP privadas en las subredes de la VPC. Para obtener más información acerca de las interfaces de red elásticas, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2 para instancias de Linux.

Un punto de enlace de la VPC de interfaz conecta la VPC directamente a Amazon Redshift. No utiliza una gateway de Internet, un dispositivo de conversión de direcciones de red (NAT), una conexión de red privada virtual (VPN) o una conexión de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con la API de Amazon Redshift.

Tiene dos opciones para utilizar Amazon Redshift a través de su VPC. Una opción es conectarse desde una instancia que está dentro de su VPC. La otra opción es conectar su red privada a la VPC a través de una opción de AWS VPN o a través de AWS Direct Connect. Para obtener más información acerca de las opciones de AWS VPN, consulte Conexiones de VPN en la Guía del usuario de Amazon VPC. Para obtener información acerca de AWS Direct Connect, consulte Creación de una conexión en la Guía del usuario de AWS Direct Connect.

Puede crear un punto de enlace de la VPC de interfaz para conectarse a Amazon Redshift a través de los comandos de la AWS Management Console o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de interfaz.

Después de crear un punto de enlace de la VPC de interfaz, puede habilitar nombres de alojamiento de DNS privados para el punto de enlace. Una vez que lo hace, el punto de enlace de Amazon Redshift predeterminado (`https://redshift.Region.amazonaws.com`) se resuelve en el punto de enlace de la VPC.

Si no habilita nombres de alojamiento de DNS privados, Amazon VPC proporciona un nombre de punto de enlace de DNS que puede utilizar en el siguiente formato.

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

Para obtener más información, consulte Puntos de enlace de la VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Amazon Redshift admite las llamadas a todas las operaciones de la API dentro de la VPC.

Puede adjuntar políticas de punto de enlace de la VPC a un punto de enlace de la VPC para controlar el acceso de las entidades principales de AWS Identity and Access Management (IAM). También puede asociar grupos de seguridad a un punto de enlace de la VPC para controlar el acceso de entrada y salida en función del origen y el destino del tráfico de red. Un ejemplo es un rango de direcciones IP. Para obtener más información, consulte Controlar el acceso a servicios con puntos de conexión de VPC en la Guía del usuario de Amazon VPC.

Creación de una política de punto de enlace de la VPC para Amazon Redshift

Puede crear una política para los puntos de enlace de la VPC para Amazon Redshift y especificar lo siguiente:

- La entidad principal que puede o no puede realizar acciones
- Las acciones que se pueden realizar
- Los recursos en los que se pueden llevar a cabo las acciones

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la guía del usuario de Amazon VPC.

A continuación, encontrará ejemplos de políticas de puntos de enlace de la VPC.

Temas

- Ejemplo: Política de punto de enlace de la VPC para denegar el acceso desde una cuenta de AWS específica
- Ejemplo: política de punto de conexión de VPC que permite el acceso a la VPC solo a un rol de IAM especificado
- Ejemplo: Política de punto de enlace de la VPC que permite el acceso a la VPC solo a una entidad principal de IAM específica (usuario)
- Ejemplo: Política de punto de enlace de la VPC para permitir operaciones de solo lectura de Amazon Redshift
- Ejemplo: Política de punto de enlace de la VPC que deniega el acceso a un clúster específico

Ejemplo: Política de punto de enlace de la VPC para denegar el acceso desde una cuenta de AWS específica

La siguiente política de punto de enlace de la VPC deniega a la cuenta de AWS *123456789012* el acceso a los recursos a través del punto de enlace.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Ejemplo: política de punto de conexión de VPC que permite el acceso a la VPC solo a un rol de IAM especificado

La siguiente política de punto de conexión de VPC permite el acceso pleno solo al rol de IAM *redshiftrole* en la cuenta de AWS *123456789012*. A las demás entidades principales de IAM se les deniega el acceso a través del punto de enlace.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
```

```
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:role/redshiftrole"
                ]
            }
        }]
}
```

Solo es un ejemplo. En la mayoría de los casos de uso, recomendamos adjuntar permisos para acciones específicas a fin de reducir el alcance de los permisos.

Ejemplo: Política de punto de enlace de la VPC que permite el acceso a la VPC solo a una entidad principal de IAM específica (usuario)

La siguiente política de punto de enlace de la VPC permite el acceso pleno solo al usuario de IAM *redshiftadmin* en la cuenta de AWS *123456789012*. A las demás entidades principales de IAM se les deniega el acceso a través del punto de enlace.

```
   {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/redshiftadmin"
                ]
            }
        }]
}
```

Solo es un ejemplo. En la mayoría de los casos de uso, recomendamos adjuntar permisos a un rol antes de asignarlos a un usuario. Además, recomendamos utilizar acciones específicas para reducir el alcance de los permisos.

Ejemplo: Política de punto de enlace de la VPC para permitir operaciones de solo lectura de Amazon Redshift

La siguiente política de punto de enlace de la VPC solo permite a la cuenta de AWS *123456789012* realizar las acciones de Amazon Redshift especificadas.

Las acciones especificadas proporcionan el equivalente al acceso de solo lectura para Amazon Redshift. Las demás acciones en la VPC se deniegan para la cuenta especificada. También se les deniega el acceso a las demás cuentas. Para obtener una lista de acciones de Amazon Redshift, consulte Acciones, recursos y claves de condición para Amazon Redshift en la Guía del usuario de IAM.

```
{
  "Statement": [
      {
          "Action": [
              "redshift:DescribeAccountAttributes",
              "redshift:DescribeClusterParameterGroups",
              "redshift:DescribeClusterParameters",
              "redshift:DescribeClusterSecurityGroups",
              "redshift:DescribeClusterSnapshots",
              "redshift:DescribeClusterSubnetGroups",
              "redshift:DescribeClusterVersions",
              "redshift:DescribeDefaultClusterParameters",
              "redshift:DescribeEventCategories",
              "redshift:DescribeEventSubscriptions",
              "redshift:DescribeHsmClientCertificates",
              "redshift:DescribeHsmConfigurations",
              "redshift:DescribeLoggingStatus",
              "redshift:DescribeOrderableClusterOptions",
              "redshift:DescribeQuery",
              "redshift:DescribeReservedNodeOfferings",
              "redshift:DescribeReservedNodes",
              "redshift:DescribeResize",
              "redshift:DescribeSavedQueries",
              "redshift:DescribeScheduledActions",
              "redshift:DescribeSnapshotCopyGrants",
              "redshift:DescribeSnapshotSchedules",
              "redshift:DescribeStorage",
              "redshift:DescribeTable",
              "redshift:DescribeTableRestoreStatus",
              "redshift:DescribeTags",
```

```
                "redshift:FetchResults",
                "redshift:GetReservedNodeExchangeOfferings"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Ejemplo: Política de punto de enlace de la VPC que deniega el acceso a un clúster específico

La siguiente política de punto de enlace de la VPC permite el acceso pleno a todas las cuentas y las entidades principales. Al mismo tiempo, deniega el acceso de la cuenta de AWS *123456789012* a las acciones realizadas en el clúster de Amazon Redshift con el ID de clúster *my-redshift-cluster*. Se siguen permitiendo otras acciones de Amazon Redshift que no admiten permisos en el nivel de los recursos para los clústeres. Para obtener una lista de las acciones de Amazon Redshift y los tipos de recursos correspondientes, consulte Acciones, recursos y claves de condición para Amazon Redshift en la Guía del usuario de IAM.

```
 {
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
            "Principal": {
                "AWS": [
                    "123456789012"
```

```
                ]
            }
        }
    ]
}
```

Configuración y análisis de vulnerabilidades en Amazon Redshift

AWS se encarga de las tareas de seguridad básicas, como la aplicación de parches en la base de datos y el sistema operativo (SO) invitado, la configuración del firewall y la recuperación de desastres (RD). Terceros certificados han revisado estos procedimientos. Para obtener más información, consulte Validación de la conformidad para Amazon Redshift, el Modelo de responsabilidad compartida y las Prácticas recomendadas para seguridad, identidad y conformidad.

Amazon Redshift aplica de manera automática actualizaciones y parches al almacenamiento de datos para que pueda centrarse en la aplicación y no en su administración. Las actualizaciones y parches se aplican durante un periodo de mantenimiento configurable. Para obtener más información, consulte Periodos de mantenimiento.

El editor de consultas v2 de Amazon Redshift es una aplicación administrada por AWS. Todas las revisiones y actualizaciones son aplicadas por AWS según sea necesario.

Tareas de red

Puede realizar tareas de red, como personalizar la conexión a una base de datos de Redshift. También puede realizar tareas relacionadas con el DNS, como configurar un nombre de dominio personalizado. Estas tareas de configuración están disponibles si tiene un clúster aprovisionado de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor.

Temas

- Uso de un nombre de dominio personalizado para las conexiones de cliente
- Uso de puntos de enlace de la VPC administrados por Redshift
- Enrutamiento de VPC mejorado en Amazon Redshift

Uso de un nombre de dominio personalizado para las conexiones de cliente

Puede crear un nombre de dominio personalizado, también conocido como URL personalizada, para el clúster de Amazon Redshift y el grupo de trabajo de Amazon Redshift sin servidor. Es un registro DNS fácil de leer que dirige las conexiones de los clientes SQL hacia su punto de conexión. Puede configurarlo para un clúster o grupo de trabajo existentes en cualquier momento. Proporciona varios beneficios:

- El nombre de dominio personalizado es una cadena más simple que la URL predeterminada, que normalmente incluye el nombre del clúster o del grupo de trabajo y la región. Es más fácil de recordar y utilizar.
- Puede enrutar rápidamente el tráfico hacia un clúster o grupo de trabajo nuevos en caso de conmutación por error, por ejemplo. De este modo, los clientes no tienen que realizar un cambio de configuración cuando vuelven a conectarse. Las conexiones pueden redirigirse de forma centralizada, con una interrupción mínima.
- Puede evitar compartir información privada, como el nombre de un servidor, en una URL de conexión. Puede ocultarlo en una URL personalizada.

Cuando se configura un nombre de dominio personalizado, mediante un CNAME, no hay ningún cargo adicional por parte de Amazon Redshift. Es posible que su proveedor de DNS le facture por

un nombre de dominio, si crea uno nuevo, pero este costo suele ser pequeño. Para obtener más información, consulte Configuración de un nombre de dominio personalizado.

Seguridad de un nombre de dominio personalizado

Amazon Redshift o Amazon Redshift sin servidor requieren un certificado de capa de sockets seguros (SSL) validado para un punto de conexión personalizado a fin de mantener la seguridad de la comunicación y verificar la propiedad del nombre de dominio. Puede utilizar su cuenta de AWS Certificate Manager con una AWS KMS key para administrar certificados de forma segura. La validación de seguridad incluye la verificación completa del nombre del host (sslmode=verify-full).

Renovación de un certificado

Amazon Redshift solo administra las renovaciones de certificado cuando elige la validación DNS, en lugar de la validación por correo electrónico. Si utiliza la validación por correo electrónico, podrá utilizar el certificado, pero deberá realizar la renovación por su cuenta, antes de que caduque. Le recomendamos que elija la validación DNS para el certificado. Puede monitorear las fechas de vencimiento de los certificados importados en AWS Certificate Manager.

Configuración de un nombre de dominio personalizado

La configuración del nombre de dominio personalizado consta de varias tareas, entre ellas, registrar el nombre de dominio con su proveedor de DNS y crear un certificado. Después de realizar estos trabajos, configure el nombre de dominio personalizado en la consola de Amazon Redshift o de Amazon Redshift sin servidor, o configúrelo con comandos de la AWS CLI. En las siguientes secciones se detallan los pasos.

Registro de un nombre de dominio y selección de un certificado

Debe tener un nombre de dominio de Internet registrado para configurar un nombre de dominio personalizado en Amazon Redshift. Puede registrar un dominio de Internet mediante Route 53 o con un proveedor de registros de dominios externo. Estas tareas se llevan a cabo fuera de la consola de Amazon Redshift. Un dominio registrado es un requisito previo para completar los procedimientos restantes a fin de crear un dominio personalizado.

> **Note**
>
> Si usa un clúster aprovisionado, antes de realizar los pasos para configurar el nombre de dominio personalizado, el clúster debe estar activado para la reubicación. Para obtener

más información, consulte Reubicación del clúster. Este paso no se requiere para Amazon Redshift sin servidor.

El nombre de dominio personalizado suele incluir el dominio raíz y un subdominio, como `mycluster.example.com`. Para configurarlo, siga estos pasos:

Creación de una entrada CNAME de DNS para su nombre de dominio personalizado

1. Registre un dominio raíz, por ejemplo, `example.com`. También puede utilizar un dominio existente. Su nombre personalizado puede estar limitado por restricciones de caracteres concretos u otras validaciones de nombres. Para obtener más información sobre el registro de un dominio con Route 53, consulte Registro de un nuevo dominio.
2. Agregue un registro CNAME de DNS que dirija su nombre de dominio personalizado hacia el punto de conexión de Redshift para su clúster o grupo de trabajo. Encontrará el punto de conexión en las propiedades del clúster o grupo de trabajo, en la consola de Redshift o de Amazon Redshift sin servidor. Copie la URL de JDBC disponible en las propiedades del clúster o el grupo de trabajo enInformación general. Las URL tienen el siguiente aspecto:

   - Para un clúster de Amazon Redshift: `redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
   - Para un grupo de trabajo de Amazon Redshift sin servidor: `endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

   Si la URL tiene un prefijo JDBC, elimínelo.

   > **Note**
   >
   > Los registros DNS están sujetos a disponibilidad, ya que cada nombre debe ser único y estar disponible para utilizarlo en la organización.

Limitaciones

Existen un par de restricciones en lo que respecta a la creación de registros CNAME para un dominio personalizado:

- No se admite la creación de varios nombres de dominio personalizados para el mismo clúster aprovisionado o grupo de trabajo de Amazon Redshift sin servidor. Solo puede asociar un único registro CNAME.
- No se admite la asociación de un registro CNAME a más de un clúster o grupo de trabajo. El CNAME de cada recurso de Redshift debe ser único.

Después de registrar su dominio y crear el registro CNAME, seleccione un certificado nuevo o existente. Este paso se realiza con AWS Certificate Manager:

Solicitud de un certificado de ACM para un nombre de dominio

1. Inicie sesión en AWS Management Console y abra la consola de ACM en https://console.aws.amazon.com/cloudfront/.
2. Elija Request a certificate (Solicitar un certificado).
3. Introduzca su nombre de dominio personalizado en el campo Nombre de dominio.

   > **Note**
   >
   > Puede especificar muchos prefijos, además del dominio del certificado, con el fin de utilizar un único certificado para varios registros de dominios personalizados. Para ilustrarlo, puede utilizar registros adicionales como `one.example.com`, `two.example.com` o un registro DNS comodín como `*.example.com` con el mismo certificado.

4. Elija Review and request.
5. Elija Confirm and request.
6. Para que una solicitud sea válida, un propietario registrado del dominio de Internet debe autorizar la solicitud para que ACM emita el certificado. Asegúrese de que el estado aparece como Emitido en la consola de ACM, cuando haya terminado con los pasos.

Le recomendamos que cree un certificado validado por DNS que cumpla los requisitos para la renovación administrada, que está disponible con AWS Certificate Manager. Esto significa que ACM renovará sus certificados de forma automática o le enviará avisos por correo electrónico cuando se acerque la fecha de vencimiento. Para obtener más información, consulte Renovación administrada para certificados de ACM.

Creación del dominio personalizado

Puede utilizar la consola de Amazon Redshift o Amazon Redshift sin servidor para crear su URL de dominio personalizada. Si no la ha configurado, la propiedad Nombre de dominio personalizado aparece como un guion (–) en Información general. Después de crear el registro CNAME y el certificado, asocie el nombre de dominio personalizado para el clúster o grupo de trabajo.

Para crear una asociación de dominio personalizado, se requieren los siguientes permisos de IAM:

- `redshift:CreateCustomDomainAssociation`: puede restringir el permiso a un clúster específico si agrega su ARN.
- `redshiftServerless:CreateCustomDomainAssociation`: puede restringir el permiso a un grupo de trabajo específico si agrega su ARN.
- `acm:DescribeCertificate`

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Realice los siguientes pasos para asignar el nombre de dominio personalizado.

1. Elija el clúster en la consola de Redshift o el grupo de trabajo en la consola de Amazon Redshift sin servidor y, a continuación, elija Crear nombre de dominio personalizado en el menú Acción. Aparecerá un cuadro de diálogo.
2. Introduzca el nombre de dominio personalizado.
3. Seleccione el ARN de AWS Certificate Manager para el Certificado de ACM. Confirme los cambios. De acuerdo con los pasos que ha seguido para crear el certificado, le recomendamos que elija un certificado validado por DNS que pueda renovarse de forma gestionada a través de AWS Certificate Manager.
4. Verifique en las propiedades del clúster que el Nombre de dominio personalizado y el ARN del certificado de dominio personalizado están rellenados con sus entradas. También aparece la Fecha de vencimiento del certificado del dominio personalizado.

Una vez configurado el dominio personalizado, el uso de `sslmode=verify-full` solo funciona para el nuevo dominio personalizado. No funciona para el punto de conexión predeterminado.

Pero aún puede conectarse al punto de conexión predeterminado con otros modos ssl, como `sslmode=verify-ca`.

Cambio de nombre de un clúster que tiene asignado un dominio personalizado mediante la consola

> **Note**
>
> Esta serie de pasos no se aplica a un grupo de trabajo de Amazon Redshift sin servidor. No puede modificar el nombre del grupo de trabajo.

Para cambiar el nombre de un clúster que tiene un nombre de dominio personalizado, se requiere el permiso `acm:DescribeCertificate` de IAM.

1. Vaya a la consola de Amazon Redshift y elija el clúster cuyo nombre desee cambiar. Elija Editar para editar las propiedades del clúster.
2. Edite el Identificador de clúster. También puede cambiar otras propiedades del clúster. A continuación, elija Guardar cambios.
3. Después de cambiar el nombre del clúster, tiene que actualizar el registro DNS para cambiar la entrada CNAME del dominio personalizado de modo que apunte al punto de conexión de Amazon Redshift actualizado.

Actualización del registro CNAME en un caso práctico de recuperación de desastres

El uso de un registro CNAME para crear un dominio personalizado puede resultar útil en un caso de recuperación de desastres. Si no puede acceder a su almacenamiento de datos, en el siguiente procedimiento se detallan las acciones que puede realizar cuando no pueda acceder a su grupo de trabajo o clúster de base de datos principal.

Supongamos que sigue las prácticas de alta disponibilidad y que cuenta con recursos secundarios. En este caso, por ejemplo, podría disponer de un clúster o grupo de trabajo en espera que reciba con regularidad los datos restaurados del clúster principal. Este almacenamiento de datos de copia de seguridad podría estar en otra zona de disponibilidad de AWS o en una región independiente. Complete los siguientes pasos para redirigir a los clientes hacia dichas zonas:

1. En este paso se supone que el clúster o grupo de trabajo están disponibles en la consola. Si no es así, puede omitirlo. En su lugar, elija el clúster principal en la consola de Amazon Redshift o el grupo de trabajo principal de la consola Amazon Redshift sin servidor. El nombre de

dominio personalizado aparece en las propiedades. Seleccione Eliminar el nombre de dominio personalizado en el menú Acciones. En la ventana que aparece, escriba eliminar para confirmar y elija Eliminar.

2. Elija el nuevo clúster o grupo de trabajo. Siga los pasos de este tema para crear un nombre de dominio personalizado. Use el mismo nombre de dominio y seleccione el mismo registro CNAME que usó para el clúster o grupo de trabajo principales. Si el ecurso secundario está en una nueva región, debe crear y usar un certificado nuevo.
3. Diríjase al proveedor de registro de dominios. Puede ser Route 53 o un proveedor externo. Seleccione el registro CNAME que creó originalmente. Al crear el registro, lo configuró para que enrutara el tráfico hacia la URL del punto de conexión del clúster o grupo de trabajo principales. Cambie el valor por la URL del punto de conexión de su clúster o grupo de trabajo en espera. Tras guardar el cambio, enruta el tráfico hacia el nuevo recurso. Tenga en cuenta que es posible que tenga que esperar a que se propague el DNS.
4. Este es un paso opcional: cambie las reglas de tráfico de red de los grupos de seguridad entrantes y salientes para enrutar el tráfico hacia su clúster o grupo de trabajo en espera. Además, al activar el recurso en espera, se supone que ya ha ejecutado o tiene previsto ejecutar operaciones de restauración para alinear los datos en espera con los datos de producción.

Una de las ventajas de cambiar el valor de la URL del punto de conexión para redirigir el tráfico es que los clientes que utilizan su nombre de dominio personalizado no requieren cambios de configuración. Sus propiedades de conexión no tienen por qué cambiar.

Tenga en cuenta que cualquier medida de recuperación de desastres que tome debe ajustarse a su plan de disponibilidad actual. Otras estrategias de resiliencia, como la implementación de recursos en varias regiones o unas sofisticadas técnicas de copia de seguridad, van más allá del alcance de este documento.

> **Note**
>
> Como recordatorio, la reubicación del clúster no es un requisito previo para configurar características de red de Redshift adicionales, como las que se utilizan para la recuperación de desastres u otros fines. No es necesario que lo activa para habilitar lo siguiente:
>
> - Conexión desde una VPC con varias cuentas o regiones a Redshift: puede conectarse desde una nube privada virtual (VPC) de AWS a otra que contenga una base de datos de Redshift. Esto facilita la administración, por ejemplo, del acceso de los clientes desde cuentas o VPC dispares, sin que sea necesario proporcionar acceso de VPC local a las

identidades que se conectan a la base de datos. Para obtener más información, consulte Conexión a Amazon Redshift sin servidor desde un punto de conexión de VPC de Redshift en otra cuenta o región.

- Configuración de un nombre de dominio personalizado: puede crear un nombre de dominio personalizado, tal como se describe en este tema, para que el nombre del punto de conexión sea más relevante y sencillo.

Descripción de las asociaciones de dominios personalizadas mediante comandos de la CLI

Utilice los comandos de esta sección para obtener una lista de nombres de dominio personalizados asociados a un clúster aprovisionado específico o a un grupo de trabajo de Amazon Redshift sin servidor.

También necesita los siguientes permisos:

- Para un clúster aprovisionado: `redshift:DescribeCustomDomainAssociations`
- Para un grupo de trabajo de Amazon Redshift sin servidor: `redshiftServerless:ListCnameAssociations`

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

A continuación, se muestra un comando de ejemplo para enumerar los nombres de dominio personalizados para un determinado clúster de Amazon Redshift:

```
aws redshift describe-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainname
```

Puede ejecutar este comando si tiene un nombre de dominio personalizado habilitado para determinar los nombres de dominio personalizados asociados al clúster. Para obtener más información sobre el comando de la CLI para describir las asociaciones de dominios personalizadas, consulte describe-custom-domain-associations.

De igual modo, se muestra un comando de ejemplo para enumerar los nombres de dominio personalizados para un determinado grupo de trabajo de Amazon Redshift sin servidor. Hay varias maneras diferentes de hacerlo. Puede proporcionar únicamente el nombre de dominio personalizado:

```
aws redshift-serverless list-cname-associations --custom-domain-
name customdomainnamesample
```

También puede obtener las asociaciones proporcionando únicamente el nombre del grupo de trabajo:

```
aws redshift-serverless list-cname-associations --workgroup-name workgroupnamesample
```

También puede obtener las asociaciones proporcionando únicamente el ARN del certificado:

```
aws redshift-serverless list-cname-associations --custom-certificate-
arn certificatearnsample
```

Puede ejecutar este comando si tiene un nombre de dominio personalizado habilitado para determinar los nombres de dominio personalizados asociados al grupo de trabajo. También puede ejecutar un comando para obtener las propiedades de una asociación de dominios personalizada. Para ello, debe proporcionar el nombre de dominio personalizado y el nombre del grupo de trabajo como parámetros. Devuelve el ARN del certificado, el nombre del grupo de trabajo y la hora de caducidad del certificado del dominio personalizado:

```
aws redshift-serverless get-custom-domain-association --workgroup-
name workgroupnamesample --custom-domain-name customdomainnamesample
```

Para obtener más información sobre los comandos de referencia de la CLI disponibles para Amazon Redshift sin servidor, consulte redshift-serverless.

Asociación del dominio personalizado con un certificado diferente

Para modificar la asociación de certificados para un nombre de dominio personalizado, se requieren los siguientes permisos de IAM:

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Utilice el siguiente comando para asociar el dominio personalizado con otro certificado. Los argumentos `--custom-domain-name` y `custom-domain-certificate-arn` son obligatorios. El ARN del nuevo certificado debe ser distinto al del ARN existente.

```
aws redshift modify-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainnamesample --custom-domain-certificate-arn ARNsample
```

En el siguiente ejemplo, se muestra cómo asociar el dominio personalizado a un certificado diferente para un grupo de trabajo de Amazon Redshift sin servidor.

```
aws redshift-serverless modify-custom-domain-association --workgroup-
name redshiftworkgroupsample --custom-domain-name customdomainnamesample --custom-
domain-certificate-arn ARNsample
```

Hay un retraso máximo de 30 segundos para poder conectarse al clúster. Parte del retraso se produce cuando el clúster de Amazon Redshift actualiza sus propiedades y hay algún retraso adicional cuando se actualiza el DNS. Para obtener más información sobre la API y la configuración de cada propiedad, consulte ModifyCustomDomainAssociation.

Eliminación del dominio personalizado

Para eliminar el nombre de dominio personalizado, el usuario debe tener permisos para las siguientes acciones:

- Para un clúster aprovisionado: `redshift:DeleteCustomDomainAssociation`
- Para un grupo de trabajo de Amazon Redshift sin servidor: `redshiftServerless:DeleteCustomDomainAssociation`

En la consola

Para eliminar el nombre de dominio personalizado, seleccione el botón Acciones y elija Eliminar el nombre de dominio personalizado. Una vez hecho esto, podrá seguir conectándose al servidor actualizando sus herramientas para utilizar los puntos de conexión que aparecen en la consola.

Uso de un comando de la CLI

En el siguiente ejemplo se muestra cómo eliminar el nombre de dominio personalizado. La operación de eliminación requiere que proporcione el nombre de dominio personalizado existente para el clúster.

```
aws redshift delete-custom-domain-association --cluster-id redshiftclustersample --
custom-domain-name customdomainnamesample
```

En el siguiente ejemplo, se muestra cómo eliminar el nombre de dominio personalizado para un grupo de trabajo de Amazon Redshift sin servidor. El nombre de dominio personalizado es un parámetro obligatorio.

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname
 --custom-domain-name customdomainname
```

Para obtener más información, consulte DeleteCustomDomainAssociation.

Conexión al clúster o grupo de trabajo con un nombre de dominio personalizado mediante un cliente SQL

Para conectarse a un clúster a un nombre de dominio personalizado, se requieren los siguientes permisos de IAM para un clúster aprovisionado: `redshift:DescribeCustomDomainAssociations`. Para Amazon Redshift sin servidor, no tiene que agregar permisos.

Como práctica recomendada, aconsejamos asociar las políticas de permisos a un rol de IAM y luego asignarlo a los usuarios y grupos según sea necesario. Para obtener más información, consulte Administración de identidades y accesos en Amazon Redshift.

Una vez completados los pasos para crear su CNAME y asignarlo a su clúster o grupo de trabajo en la consola, puede proporcionar la URL personalizada en las propiedades de conexión de su cliente SQL. Tenga en cuenta que puede haber un retraso de la propagación de DNS inmediatamente posterior a la creación de un registro CNAME.

1. Abra un cliente SQL. Por ejemplo, puede utilizar SQL/Workbench J. Abra las propiedades de una conexión y agregue el nombre de dominio personalizado para la cadena de conexión. Por ejemplo, `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full`. En este ejemplo, `dev` especifica la base de datos predeterminada.
2. Agregue el Nombre de usuario y la Contraseña del usuario de la base de datos.
3. Pruebe la conexión. Su capacidad para consultar recursos de la base de datos, como tablas específicas, puede variar en función de los permisos concedidos al usuario de la base de datos o de los roles asignados a la base de datos de Amazon Redshift.

Tenga en cuenta que es posible que deba establecer su clúster o grupo de trabajo como de acceso público para conectarse a él si se encuentra en una VPC. Puede cambiar esta configuración en las propiedades de la red.

> **Note**
>
> Las conexiones a un nombre de dominio personalizado son compatibles con los controladores JDBC y Python. No se admiten las conexiones ODBC.

Uso de puntos de enlace de la VPC administrados por Redshift

De forma predeterminada, un clúster de Amazon Redshift o un grupo de trabajo de Amazon Redshift sin servidor se aprovisionan en una nube privada virtual (VPC). Se puede acceder a esa VPC desde otra VPC o subred cuando se permite el acceso público o se configura una puerta de enlace de Internet, un dispositivo NAT o una conexión de AWS Direct Connect para enrutar el tráfico a ella. Para acceder a un clúster, también puede configurar un punto de conexión de VPC administrado por Redshift (basado en AWS PrivateLink).

Usted configura un punto de conexión de VPC administrado por Redshift como una conexión privada entre una VPC que contiene un clúster o un grupo de trabajo y una VPC que ejecuta una herramienta de cliente. Si el clúster o el grupo de trabajo están en otra cuenta, el propietario de la cuenta (concedente) debe conceder acceso a la cuenta que va a conectarse (beneficiario). Con este enfoque, puede acceder al almacenamiento de datos sin usar una dirección IP pública ni enrutar el tráfico a través de Internet.

Estas son razones comunes para permitir el acceso mediante un punto de conexión de VPC administrado por Redshift:

- La cuenta de AWS A quiere permitir que una VPC en la cuenta de AWS B tenga acceso a un clúster o un grupo de trabajo.
- La cuenta de AWS A quiere permitir que una VPC que también está en la cuenta de AWS A tenga acceso a un clúster o un grupo de trabajo.
- La cuenta de AWS A quiere permitir que una subred diferente en la VPC dentro de la cuenta de AWS A tenga acceso a un clúster o a un grupo de trabajo.

El flujo de trabajo para configurar un punto de conexión de VPC administrado por Redshift para acceder a un clúster o un grupo de trabajo que está en otra cuenta es el siguiente:

1. La cuenta de propietario concede autorización de acceso a otra cuenta y especifica el ID de la cuenta de AWS y el identificador de VPC (o todas las VPC) del beneficiario.
2. Se notifica a la cuenta del beneficiario que tiene permiso para crear un punto de enlace de la VPC administrado por Redshift.
3. La cuenta del beneficiario crea un punto de enlace de la VPC administrado por Redshift.
4. La cuenta del beneficiario accede al clúster o al grupo de trabajo de la cuenta del propietario mediante el punto de conexión de VPC administrado por Redshift.

Para hacerlo, puede utilizar la consola de Amazon Redshift, la AWS CLI o la API de Amazon Redshift.

Consideraciones para el uso de puntos de enlace de la VPC administrados por Redshift

> **Note**
>
> Para crear o modificar puntos de conexión de VPC administrados por Redshift, necesita permiso `ec2:CreateVpcEndpoint` o `ec2:ModifyVpcEndpoint` en su política de IAM, además de otros permisos especificados en la política `AmazonRedshiftFullAccess` administrada por AWS.

Cuando utilice los puntos de enlace de la VPC administrados por Redshift, tenga en cuenta lo siguiente:

- Asegúrese de que el clúster al que se accede sea un tipo de nodo RA3. Un grupo de trabajo de Amazon Redshift sin servidor también sirve para hacer esto.
- En el caso de los clústeres aprovisionados, asegúrese de que el clúster al que se accede tenga activada la reubicación de clústeres. Para obtener información acerca de los requisitos para activar la reubicación de clústeres, consulte Reubicación del clúster.
- Asegúrese de que el clúster o el grupo de trabajo al que se accede a través de su grupo de seguridad esté disponible dentro de los intervalos de puertos válidos 5431-5455 y 8191-8215. El valor predeterminado es 5439.

- Puede modificar los grupos de seguridad de la VPC asociados a un punto de enlace de la VPC administrado por Redshift existente. Para modificar otros parámetros, elimine el punto de enlace de la VPC administrado por Redshift actual y cree uno nuevo.
- La cantidad de puntos de enlace de la VPC administrados por Redshift que puede crear está limitado a la cuota de puntos de enlace de la VPC.
- No se puede acceder a los puntos de enlace de la VPC administrados por Redshift desde Internet. Solo se puede acceder a un punto de conexión de VPC administrado por Redshift dentro de la VPC donde se aprovisiona el punto de conexión o desde cualquier VPC interconectada con la VPC donde se aprovisiona el punto de conexión de la forma que permitan las tablas de enrutamiento y los grupos de seguridad.
- No puede utilizar la consola de Amazon VPC para administrar los puntos de enlace de la VPC administrados por Redshift.
- Cuando cree un punto de conexión de VPC administrado por Redshift para un clúster aprovisionado, la VPC que elija debe tener un grupo de subredes. Para crear un grupo de subredes, consulte Administración de grupos de subred de clúster mediante la consola.

Para obtener información acerca de cuotas y restricciones de nomenclatura, consulte Cuotas y límites de Amazon Redshift.

Para obtener información sobre precios, consulte Precios de AWS PrivateLink.

Administración de puntos de conexión de VPC administrados por Redshift mediante la consola

Puede configurar el uso de puntos de enlace de la VPC administrados por Redshift mediante la consola de Amazon Redshift.

Concesión de acceso

Si la VPC a la que desea que su clúster o grupo de trabajo acceda se encuentra en otra cuenta de AWS, asegúrese de autorizarla desde la cuenta del propietario (concedente).

Concesión de acceso al clúster o grupo de trabajo a una VPC que está en otra cuenta de AWS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

2. En el menú de navegación, elija Clusters (Clústeres). Para Amazon Redshift sin servidor, elija Panel sin servidor.
3. En el caso de un clúster al que desea permitir acceso, para consultar los detalles del clúster, elija el nombre del clúster. Elija la pestaña Properties (Propiedades) del clúster.

   La sección Granted accounts (Cuentas concedidas) muestra las cuentas y las VPC correspondientes que tienen acceso al clúster. Para un grupo de trabajo de Amazon Redshift sin servidor, elija el grupo de trabajo. Cuentas concedidas está disponible en la pestaña Acceso a los datos.
4. Elija Grant access (Conceder acceso) para mostrar un formulario en el que se ingresa la información del beneficiario para agregar una cuenta.
5. En ID de la cuenta de AWS, ingrese el ID de la cuenta a la que está concediendo acceso. Puede conceder acceso a VPC específicas o a todas las VPC de la cuenta especificada.
6. Elija Grant access (Conceder acceso) para conceder acceso.

Creación de un punto de enlace de la VPC administrado por Redshift

Si posee un clúster o un grupo de trabajo o se le ha concedido acceso para administrarlo, puede crear un punto de conexión de VPC administrado por Redshift para él.

Para crear un punto de enlace de la VPC administrado por Redshift

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones).

   La página de Configuraciones muestra los puntos de enlace de la VPC administrados por Redshift que se han creado. Para ver los detalles de un punto de enlace, elija el nombre. En el caso de Amazon Redshift sin servidor, los puntos de conexión de VPC se encuentran en la pestaña Acceso a los datos cuando se elige el grupo de trabajo.
3. Seleccione Create endpoint (Crear punto de enlace) para mostrar un formulario en el que se ingresa la información sobre el punto de enlace que desea agregar.
4. Introduzca los valores del Nombre del punto conexión, el ID de cuenta de AWS de 12 dígitos, la Nube privada virtual (VPC) donde se encuentra el punto de conexión, la Subred y el Grupo de seguridad de la VPC.

La subred de Subred define las subredes y las direcciones IP en las que Amazon Redshift implementa el punto de conexión. Amazon Redshift elige una subred que tenga direcciones IP disponibles para la interfaz de red asociada al punto de enlace.

Las reglas del grupo de seguridad en Grupo de seguridad definen los puertos, los protocolos y los orígenes para el tráfico entrante que está autorizando para el punto de conexión. Permita el acceso al puerto seleccionado a través del grupo de seguridad o el rango CIDR donde se ejecutan las cargas de trabajo.

5. Elija Create endpoint (Crear punto de enlace) para crear el punto de enlace.

Una vez creado el punto de conexión, puede acceder al clúster o al grupo de trabajo a través de la URL que se muestra en URL de punto de conexión en los ajustes de configuración del punto de conexión de VPC administrado por Redshift.

Administración de puntos de enlace de la VPC administrados por Redshift mediante la AWS CLI

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para trabajar con puntos de enlace de la VPC administrados por Redshift. Para obtener más información, consulte Referencia de comandos de la AWS CLI.

- authorize-endpoint-access
- revoke-endpoint-access
- create-endpoint-access
- modify-endpoint-access
- delete-endpoint-access
- describe-endpoint-access
- describe-endpoint-authorization

Administración de puntos de enlace de la VPC administrados por Redshift mediante las operaciones de la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para trabajar con puntos de enlace de la VPC administrados por Redshift. Para obtener más información, consulte la referencia de la API de Amazon Redshift.

- AuthorizeEndpointAccess
- RevokeEndpointAccess
- CreateEndpointAccess
- ModifyEndpointAccess
- DeleteEndpointAccess
- DescribeEndpointAccess
- DescribeEndpointAuthorization

Administración de puntos de conexión de VPC administrados por Redshift mediante AWS CloudFormation

Para obtener información sobre el tipo de recurso AWS CloudFormation que se debe utilizar para crear un punto de conexión de VPC administrado por Redshift mediante AWS CloudFormation, consulte AWS::Redshift::EndpointAccess en la Guía del usuario de AWS CloudFormation.

Enrutamiento de VPC mejorado en Amazon Redshift

Cuando utiliza el enrutamiento de VPC mejorado de Amazon Redshift, este servicio fuerza todo el tráfico COPY y UNLOAD entre el clúster y los repositorios de datos a que pase por la nube virtual privada (VPC) en función del servicio Amazon VPC. Mediante el enrutamiento de VPC mejorado, puede utilizar características de VPC estándar, como grupos de seguridad de VPC, listas de control de acceso (ACL) a la red, puntos de conexión de la VPC, políticas de punto de conexión de la VPC, gateways de Internet y servidores de sistema de nombres de dominio (DNS), tal como se describe en la Guía del usuario de Amazon VPC. Puede usar estas características para administrar de forma precisa el flujo de los datos entre el clúster de Amazon Redshift y otros recursos. Cuando utiliza el direccionamiento de VPC mejorado para direccionar el tráfico a través de la VPC, también puede utilizar registros de flujo de VPC para supervisar el tráfico COPY y UNLOAD.

Los clústeres de Amazon Redshift y los grupos de trabajo Amazon Redshift sin servidor admiten un enrutamiento de VPC mejorado. No puede utilizar el enrutamiento de VPC mejorado con Redshift Spectrum. Para obtener más información, consulte Redshift Spectrum y enrutamiento de VPC mejorado.

Si el enrutamiento de VPC mejorado no está activado, Amazon Redshift dirige el tráfico a través de Internet, incluido el tráfico a otros servicios dentro de la red de AWS.

> **Important**
>
> Puesto que el enrutamiento de VPC mejorado afecta la forma en la que Amazon Redshift accede a otros recursos, los comandos COPY y UNLOAD podrían presentar error a menos que configure la VPC correctamente. Debe crear una ruta de acceso a la red específica entre la VPC del clúster y los recursos de datos, como se describe a continuación.

Cuando ejecuta un comando COPY o UNLOAD en un clúster que tiene el enrutamiento de VC mejorado activado, la VPC dirige el tráfico al recurso especificado mediante la ruta de red más estricta, o más específica, disponible.

Por ejemplo, puede configurar las siguientes rutas en la VPC:

- Puntos de conexión de la VPC: en el caso del tráfico dirigido a un bucket de Amazon S3 en la misma región de AWS que el clúster, puede crear un punto de conexión de la VPC para dirigir el tráfico al bucket de forma directa. Cuando utiliza los puntos de conexión de la VPC, puede adjuntar una política de punto de conexión para administrar el acceso a Amazon S3. Para obtener más información acerca del uso de puntos de enlace con Amazon Redshift, consulte Uso de los puntos de enlace de la VPC. Si utiliza Lake Formation, puede encontrar más información sobre cómo establecer una conexión privada entre la VPC y AWS Lake Formation en Puntos de conexión de VPC de AWS Lake Formation y de interfaz (AWS PrivateLink).
- Gateway NAT: puede conectarse a un bucket de Amazon S3 en otra región de AWS y a otro servicio dentro de la red de AWS. También puede obtener acceso a una instancia de alojamiento fuera de la red de AWS. Para ello, configure una gateway de conversión de la dirección de red (NAT), tal como se describe en la Guía del usuario de Amazon VPC.
- Gateway de Internet: para conectarse a servicios de AWS fuera de la VPC, puede adjuntar una gateway de Internet a la subred de la VPC, tal como se describe en la Guía del usuario de Amazon VPC. Para utilizar un gateway de Internet, el clúster debe tener una IP pública para permitir a otros servicios comunicarse con el clúster.

Para obtener más información, consulte Puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

El uso de Enhanced VPC Routing no supone ningún cargo adicional. Es posible que incurra en cargos adicionales por transferencia de datos para determinadas operaciones. Estos incluyen distintas operaciones, como utilizar UNLOAD en Amazon S3 en una región de AWS diferente. COPY de Amazon EMR o Secure Shell (SSH) con direcciones IP públicas. Para obtener más información acerca de los precios, consulte Precios de Amazon EC2.

Temas

- Uso de los puntos de enlace de la VPC
- Enhanced VPC Routing
- Redshift Spectrum y enrutamiento de VPC mejorado

Uso de los puntos de enlace de la VPC

Puede utilizar un punto de conexión de la VPC para crear una conexión administrada entre el clúster de Amazon Redshift de una VPC y Amazon Simple Storage Service (Amazon S3). Cuando lo haga, el tráfico de COPY y UNLOAD entre el clúster y los datos de Amazon S3 permanecerá en Amazon VPC. Puede adjuntar una política de punto de conexión al punto de conexión para administrar con más precisión el acceso a los datos. Por ejemplo, puede agregar una política al punto de conexión de la VPC que permita la descarga de datos únicamente en un bucket específico de Amazon S3 en la cuenta.

> **Important**
>
> Actualmente, Amazon Redshift admite los puntos de enlace de la VPC solo para conectarse a Amazon S3. Cuando Amazon VPC agregue soporte para que otros servicios de AWS utilicen los puntos de conexión de la VPC, Amazon Redshift también admitirá esas conexiones de punto de conexión de la VPC. Para conectarse a un bucket de Amazon S3 utilizando un punto de conexión de la VPC, el clúster de Amazon Redshift y el bucket de Amazon S3 a los que se conecta deben estar en la misma región de AWS.

Para utilizar los puntos de conexión de VPC, cree un punto de conexión de VPC para la VPC en la que está el almacenamiento de datos y, a continuación, active el enrutamiento de VPC mejorado. Puede activar el enrutamiento de VPC mejorado cuando cree su clúster o grupo de trabajo, o

puede modificar un clúster o grupo de trabajo en una VPC para que utilice el enrutamiento de VPC mejorado.

Un punto de conexión de VPC utiliza tablas de enrutamiento para controlar el enrutamiento del tráfico entre un clúster o grupo de trabajo de la VPC y Amazon S3. Todos los clústeres y grupos de trabajo de subredes asociados a las tablas de enrutamiento especificadas utilizan automáticamente ese punto de conexión para acceder al servicio.

La VPC utiliza la ruta más específica, o más restrictiva, que coincida con el tráfico para determinar cómo enrutarlo. Por ejemplo, suponga que tiene una ruta en la tabla de enrutamiento para todo el tráfico de Internet (0.0.0.0/0) que apunta a una gateway de Internet y un punto de conexión de Amazon S3. En este caso, se prefiere la ruta del punto de conexión para todo el tráfico destinado a Amazon S3. Esto se debe a que el rango de direcciones IP para el servicio Amazon S3 es más específico que 0.0.0.0/0. En este ejemplo, el resto del tráfico de Internet se dirige a su puerta de enlace de Internet, incluido el tráfico destinado a los buckets de Amazon S3 de otras Regiones de AWS.

Para obtener más información sobre creación de puntos de conexión, consulte Crear un punto de conexión de VPC en la Guía del usuario de Amazon VPC.

Las políticas de punto de conexión se utilizan para controlar el acceso desde su clúster o grupo de trabajo a los buckets de Amazon S3 que contienen sus archivos de datos. Para tener un control más específico, de forma opcional, puede adjuntar una política de puntos de enlace personalizada. Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink.

El uso de puntos de enlace no supone ningún cargo adicional. Se aplicará la tarifa estándar por la transferencia de datos y el uso de recursos. Para obtener más información acerca de los precios, consulte Precios de Amazon EC2.

Enhanced VPC Routing

Puede activar el enrutamiento de VPC mejorado cuando cree o modifique un clúster y cuando cree o modifique un grupo de trabajo de Amazon Redshift sin servidor.

Para trabajar con el enrutamiento de VPC mejorado para un clúster, su clúster debe cumplir los siguientes requisitos y restricciones:

- El clúster debe estar en una VPC.

Si adjunta un punto de conexión de la VPC de Amazon S3, el clúster utiliza el punto de conexión de la VPC únicamente para obtener acceso a los buckets de Amazon S3 de la misma región de AWS. Para obtener acceso a los buckets de otra región de AWS (sin utilizar el punto de conexión de la VPC) o para acceder a otros servicios de AWS, haga que el clúster sea accesible públicamente o utilice una gateway de conversión de las direcciones de red (NAT). Para obtener más información, consulte Creación de un clúster en una VPC.

- Debe habilitar la resolución del servicio de nombres de dominio (DNS) en la VPC. O bien, si está utilizando su propio servidor de DNS, asegúrese de que las solicitudes de DNS a Amazon S3 se resuelvan correctamente en las direcciones IP mantenidas por AWS. Para obtener más información, consulte Utilización de DNS con su VPC en la Guía del usuario de Amazon VPC.
- Los nombres de host de DNS deben estar habilitados en la VPC. Los nombres de host DNS están habilitados de forma predeterminada.
- Las políticas de punto de conexión de la VPC deben permitir el acceso a cualquier bucket de Amazon S3 utilizado con llamadas a COPY, UNLOAD o CREATE LIBRARY en Amazon Redshift, incluido el acceso a cualquier archivo de manifiesto involucrado. Para utilizar COPY desde hosts remotos, las políticas de puntos de enlace deben permitir el acceso a cada máquina del host. Para obtener más información, consulte Permisos de IAM para COPY, UNLOAD y CREATE LIBRARY en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para crear un clúster con enhanced VPC routing

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Provisioned clusters dashboard (Panel de clústeres aprovisionados) y, a continuación, elija Create cluster (Crear clúster) e ingrese las propiedades de Cluster details (Detalles del clúster).
3. Para mostrar la sección Additional configurations (Configuraciones adicionales), seleccione Use defaults (Usar valores predeterminados).
4. Vaya a la sección Network and security (Red y seguridad).
5. Para activar Enhanced VPC routing (Enrutamiento de VPC mejorado), elija Turn on (Activar) para forzar el tráfico del clúster a través de la VPC.
6. Seleccione Create cluster (Crear clúster) para crearlo. El clúster tardará varios minutos antes de estar listo para su uso.

Para crear un grupo de trabajo de Amazon Redshift sin servidor con enrutamiento de VPC mejorado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Serverless dashboard (Panel de control sin servidor) y, a continuación, elija Create workgroup (Crear grupo de trabajo) e ingrese las propiedades del grupo de trabajo.
3. Vaya a la sección Network and security (Red y seguridad).
4. Seleccione Turn on enhanced VPC routing (Activar enrutamiento de VPC mejorado) para enrutar el tráfico de red a través de la VPC.
5. Elija Next (Siguiente) y termine de ingresar las propiedades de su grupo de trabajo hasta que use Create (Crear) para crear el grupo de trabajo.

Redshift Spectrum y enrutamiento de VPC mejorado

Amazon Redshift Spectrum no admite el enrutamiento de VPC mejorado con clústeres aprovisionados. El enrutamiento de VPC mejorado de Amazon Redshift dirige tráfico específico a través de la VPC. Todo el tráfico entre el clúster y los buckets de Amazon S3 está obligado a pasar por la VPC de Amazon VPC. Redshift Spectrum se ejecuta en recursos administrados por AWS que son propiedad de Amazon Redshift. Como estos recursos están fuera de la VPC, Redshift Spectrum no usa Enhanced VPC Routing.

El tráfico entre Redshift Spectrum y Amazon S3 se enruta de forma segura a través de la red privada de AWS, fuera de su VPC. El tráfico en tránsito se firma con el protocolo Signature Version 4 (SIGv4) de Amazon y se cifra mediante HTTPS. La autorización para este tráfico se basa en el rol de IAM que se adjunta a su clúster de Amazon Redshift. Para administrar aún más el tráfico de Redshift Spectrum, puede modificar el rol de IAM de su clúster y la política adjunta al bucket de Amazon S3. Es posible que también deba configurar su VPC de manera que permita que su clúster acceda a AWS Glue o a Athena, tal como se detalla a continuación.

Tenga en cuenta que el enrutamiento de VPC mejorado afecta a la forma en la que Amazon Redshift accede a otros recursos, las consultas podrían presentar error a menos que configure la VPC correctamente. Para obtener más información, consulte Enrutamiento de VPC mejorado en Amazon Redshift, que analiza con más detalle la creación de un punto de conexión de VPC, una puerta de enlace NAT y otros recursos de red para dirigir el tráfico a los buckets de Amazon S3.

> **Note**
>
> Amazon Redshift sin servidor admite el enrutamiento de VPC mejorado para consultas a tablas externas en Amazon S3.

Consideraciones sobre el uso de Amazon Redshift Spectrum

A continuación, se incluyen las consideraciones que se deben tener en cuenta al usar Redshift Spectrum:

- Políticas de acceso a buckets
- Rol de IAM de clúster
- Registro y auditoría del acceso a Amazon S3
- Acceso a AWS Glue o Amazon Athena

Políticas de acceso a buckets

Puede controlar el acceso a los datos en sus buckets de Amazon S3 usando una política de bucket adjunta al bucket y un rol de IAM adjunto al clúster.

Redshift Spectrum en clústeres aprovisionados no puede acceder a los datos almacenados en buckets de Amazon S3 que usen una política de bucket que limite el acceso únicamente a los puntos de conexión de VPC especificados. En su lugar, use una política de bucket que limite el acceso a únicamente entidades principales específicas, como a una cuenta de AWS específica o usuarios específicos.

Para el rol de IAM al cual se le concede acceso al bucket, utilice una relación de confianza que permita que únicamente la entidad principal del servicio Amazon Redshift asuma el rol. Cuando se adjunta al clúster, el rol solo se puede usar en el contexto de Amazon Redshift y no se puede compartir fuera del clúster. Para obtener más información, consulte Restricción de acceso a los roles de IAM. También se puede utilizar una política de control de servicio (SCP) para restringir aún más el rol; consulte Impedir que los usuarios y roles de IAM realicen los cambios especificados, con una excepción para un rol de administrador especificado en la Guía del usuario de AWS Organizations.

Para utilizar Redshift Spectrum, no puede haber ninguna política de IAM que bloquee el uso de direcciones URL prefirmadas.

El siguiente ejemplo de política de bucket solo permite acceder al bucket especificado desde el tráfico originado en Redshift Spectrum que es propiedad de la cuenta de AWS 123456789012.

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "BucketPolicyForSpectrum",
  "Effect": "Allow",
  "Principal": {
   "AWS": ["arn:aws:iam::123456789012:role/redshift"]
  },
  "Action": ["s3:GetObject", "s3:List*"],
  "Resource": ["arn:aws:s3:::examplebucket/*"],
  "Condition": {
   "StringEquals": {
    "aws:UserAgent": "AWS Redshift/Spectrum"
   }
  }
 }]
}
```

Rol de IAM de clúster

El rol que se adjuntó a su clúster debería tener una relación de confianza que permita que el servicio Amazon Redshift sea el único en asumirlo, tal como se muestra a continuación.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Puede agregar una política al rol del clúster que impida el acceso de COPY y UNLOAD a un bucket específico. La siguiente política solo permite tráfico al bucket especificado procedente de Redshift Spectrum.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["s3:Get*", "s3:List*"],
        "Resource": "arn:aws:s3:::myBucket/*",
               "Condition": {"StringEquals": {"aws:UserAgent": "AWS Redshift/
Spectrum"}}
    }]
}
```

Para obtener más información, consulte Políticas de IAM para Redshift Spectrum en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Registro y auditoría del acceso a Amazon S3

Uno de los beneficios de usar el enrutamiento de VPC mejorado de Amazon Redshift es que todo el tráfico COPY y UNLOAD queda registrado en los registros de flujo de la VPC. El tráfico originado en Redshift Spectrum que se dirige a Amazon S3 no pasa por la VPC, por lo que no queda registrado en el registro de flujo de la VPC. Cuando Redshift Spectrum accede a los datos en Amazon S3, realiza estas operaciones en el contexto de la cuenta de AWS y de los respectivos privilegios del rol. Puede registrar y auditar el acceso a Amazon S3 mediante el registro de acceso al servidor en AWS CloudTrail y Amazon S3.

Asegúrese de que los rangos de IP de S3 estén agregados a la lista de permitidos. Para obtener más información acerca de los rangos de IP de S3 necesarios, consulte Aislamiento de red.

Registros de AWS CloudTrail

Para rastrear todo el acceso a objetos en Amazon S3, incluido el acceso a Redshift Spectrum, habilite el registro de CloudTrail para objetos de Amazon S3.

Puede utilizar CloudTrail para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en su infraestructura de AWS. Para obtener más información, consulte Introducción a CloudTrail.

De forma predeterminada, CloudTrail solo realiza un seguimiento de las acciones en el nivel de bucket. Para realizar un seguimiento de las acciones en el nivel del objeto (como `GetObject`), habilite eventos de datos y administración para cada bucket registrado.

Registro de acceso al servidor de Simple Storage Service (Amazon S3)

El registro de acceso al servidor brinda registros detallados para las solicitudes realizadas a un bucket. La información del registro de acceso puede ser útil en auditorías de acceso y seguridad. Para obtener más información, consulte Cómo habilitar el registro de acceso al servidor en la Guía del usuario de Amazon Simple Storage Service.

Para obtener más información, consulte la publicación How to Use Bucket Policies and Apply Defense-in-Depth to Help Secure Your Amazon S3 Data en el blog de seguridad de AWS.

Acceso a AWS Glue o Amazon Athena

Redshift Spectrum accede a su catálogo de datos en AWS Glue o Athena. Otra opción es utilizar un metaalmacén de Hive específico para su catálogo de datos.

Para habilitar el acceso a AWS Glue o Athena, configure su VPC con una gateway de Internet o una gateway NAT. Configure los grupos de seguridad de la VPC de manera que permitan el tráfico saliente hacia los puntos de enlace públicos de AWS Glue y Athena. Alternativamente, puede configurar un punto de conexión de la VPC de la interfaz para que AWS Glue acceda a su AWS Glue Data Catalog. Cuando se utiliza un punto de conexión de interfaz de la VPC, la comunicación entre la VPC y AWS Glue se lleva a cabo dentro de la red de AWS. Para obtener más información, consulte Creación de un punto de conexión de interfaz.

Puede configurar las siguientes rutas en la VPC:

- Gateway de Internet: para conectarse a servicios de AWS fuera de la VPC, puede adjuntar una gateway de Internet a la subred de la VPC, tal como se describe en la Guía del usuario de Amazon VPC. Para utilizar una gateway de Internet, el clúster debe tener una dirección IP pública para permitir a otros servicios comunicarse con el clúster.
- Gateway NAT: para conectarse a un bucket de Amazon S3 que esté en otra región de AWS o a otro servicio de la red de AWS, configure una gateway de conversión de las direcciones de red (NAT), tal como se describe en la Guía del usuario de Amazon VPC. También use esta configuración para obtener acceso a una instancia de alojamiento fuera de la red de AWS.

Para obtener más información, consulte Enrutamiento de VPC mejorado en Amazon Redshift.

Monitoreo del rendimiento de clústeres de Amazon Redshift

Amazon Redshift proporciona métricas y datos de rendimiento para que pueda realizar un seguimiento del estado y el rendimiento de sus clústeres y bases de datos. En esta sección, analizaremos los tipos de datos con los que puede trabajar en Amazon Redshift, específicamente en la consola de Amazon Redshift.

Temas

- Información general
- Monitoreo de Amazon Redshift mediante las métricas de CloudWatch
- Uso de los datos de rendimiento en la consola de Amazon Redshift

Información general

Los datos de rendimiento que puede usar en la consola de Amazon Redshift entran en dos categorías:

- Métricas de Amazon CloudWatch: las métricas de Amazon CloudWatch ayudan a monitorear los aspectos físicos del clúster, como la utilización de la CPU, la latencia y el rendimiento. Los datos de métricas se muestran directamente en la consola de Amazon Redshift. También puede verlos en la consola de CloudWatch. De modo alternativo, puede consumirlos de cualquier otra forma en la que trabaje con métricas, como en la AWS CLI o en uno de los AWS SDK.
- Datos de rendimiento de cargas o consultas: estos datos ayudan a monitorear la actividad y el rendimiento de la base de datos. Estos datos se incorporan en la consola de Amazon Redshift para que le resulte fácil relacionar lo que ve en las métricas de CloudWatch con los eventos de carga y consulta específicos de la base de datos. También puede crear sus propias consultas de rendimiento personalizadas y ejecutarlas directamente en la base de datos. Los datos de rendimiento de cargas y consultas solo se muestran en la consola de Amazon Redshift. No se publican como métricas de CloudWatch.

Los datos de rendimiento se integran a la consola de Amazon Redshift, lo que produce una mejor experiencia de las siguientes maneras:

- Los datos de rendimiento asociados a un clúster se muestran de forma contextual cuando ve un clúster, caso en el que es posible que los necesite para tomar decisiones sobre el clúster, como cambiar el tamaño.
- Algunas métricas de rendimiento se muestran en unidades con escalas más adecuadas en la consola de Amazon Redshift que en CloudWatch. Por ejemplo, `WriteThroughput` se muestra en GB/s (mientras que en CloudWatch lo hace en bytes/s), que es una unidad más pertinente para el espacio de almacenamiento normal de un nodo.
- Puede visualizar fácilmente los datos de rendimiento de los nodos de un clúster conjuntamente en el mismo gráfico. De este modo, podrá monitorear de forma sencilla el rendimiento de todos los nodos de un clúster. También puede ver los datos de rendimiento de cada nodo.

Amazon Redshift proporciona los datos de rendimiento (tanto las métricas de CloudWatch como los datos de carga y consulta) sin ningún cargo adicional. Los datos de rendimiento se registran cada minuto. Puede obtener acceso a los valores históricos de los datos de rendimiento en la consola de Amazon Redshift. Para obtener información detallada acerca del uso de CloudWatch para obtener acceso a los datos de rendimiento de Amazon Redshift que se exponen como métricas de CloudWatch, consulte ¿Qué es CloudWatch? en la Guía del usuario de Amazon CloudWatch.

Monitoreo de Amazon Redshift mediante las métricas de CloudWatch

Con las métricas de CloudWatch para Amazon Redshift, puede obtener información acerca del rendimiento y el estado del clúster y ver los datos en el nivel del nodo. Al trabajar con estas métricas, hay que recordar que cada métrica tiene una o más dimensiones asociadas. Estas dimensiones le indican a qué se puede aplicar la métrica; es decir, el alcance de la métrica. Amazon Redshift tiene las dos dimensiones siguientes:

- Las métricas que tienen una dimensión `NodeID` son métricas que proporcionan los datos de rendimiento de los nodos de un clúster. Este conjunto de métricas incluye el nodo principal y los de computación. Entre los ejemplos de estas métricas se incluyen `CPUUtilization`, `ReadIOPS` y `WriteIOPS`.
- Las métricas que tienen solo una dimensión `ClusterIdentifier` son métricas que proporcionan datos de rendimiento de los clústeres. Entre los ejemplos de estas métricas se incluyen `HealthStatus` y `MaintenanceMode`.

> **Note**
>
> En algunos casos de métricas, una métrica específica del clúster representa una acumulación del comportamiento de los nodos. En estos casos, hay que prestar especial atención al interpretar el valor de las métricas, ya que el comportamiento del nodo principal se agrega al del nodo de computación.

Para obtener más información acerca de las métricas y las dimensiones de CloudWatch, consulte Conceptos de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Si desea obtener más detalles acerca de las métricas de CloudWatch para Amazon Redshift, consulte las siguientes secciones.

Temas

- Métricas de Amazon Redshift
- Dimensiones de métricas de Amazon Redshift
- Datos de rendimiento de cargas y consultas de Amazon Redshift

Métricas de Amazon Redshift

El espacio de nombres de `AWS/Redshift` incluye las siguientes métricas. A menos que se indique lo contrario, las métricas se recopilan en intervalos de 1 minuto.

Título

Métrica	Descripción
`CommitQueueLength`	El número de transacciones en espera de confirmación en un momento determinado. Unidades: recuento Dimensiones: `ClusterIdentifier`
`ConcurrencyScaling ActiveClusters`	El número de clústeres de escalado de simultaneidad que procesan activamente consultas en un momento dado.

Métrica	Descripción
	Unidades: recuento Dimensiones: `ClusterIdentifier`
`ConcurrencyScaling Seconds`	El número de segundos usados por los clústeres de escalado de simultaneidad que tienen actividad de procesamiento de consultasactivas. Unidades: recuento Dimensiones: `ClusterIdentifier`
`CPUUtilization`	El porcentaje de utilización de CPU. Para los clústeres, esta métrica representa la suma de los valores de utilización de CPU de todos los nodos (principales y de computación). Unidades: porcentaje Dimensiones: `ClusterIdentifier` , `NodeID` Dimensiones: `ClusterIdentifier`
`DatabaseConnections`	El número de conexiones de base de datos a un clúster. Unidades: recuento Dimensiones: `ClusterIdentifier`

Métrica	Descripción
`HealthStatus`	Indica el estado del clúster. Cada minuto el clúster se conecta a su base de datos y realiza una consulta sencilla. Si puede realizar esta operación correctamente, se considera que el clúster está en buen estado. De lo contrario, se considera que el clúster está en mal estado. Un estado incorrecto se puede producir cuando la base de datos del clúster está sobrecargada en exceso o cuando hay un problema de configuración con una base de datos del clúster. **Note** En Amazon CloudWatch, esta métrica se registra como 1 o 0, mientras que, en la consola de Amazon Redshift, se muestra con las palabras `HEALTHY` o `UNHEALTHY` para facilitar su lectura. Cuando esta métrica se muestra en la consola de Amazon Redshift, se omiten los promedios de muestreo y solo se muestra `HEALTHY` o `UNHEALTHY` . En Amazon CloudWatch, pueden aparecer otros valores además de 0 y 1 por cuestiones de muestreo. Cualquier valor inferior a 1 para `HealthStatus` se registra como 0 (`UNHEALTHY`). Unidades: recuento (1/0) (`HEALTHY/UNHEALTHY` en la consola de Amazon Redshift) Dimensiones: `ClusterIdentifier`

Métrica	Descripción
MaintenanceMode	Indica si los datos del clúster se encuentran en modo de mantenimiento. **Note** En Amazon CloudWatch, esta métrica se registra como 1 o 0, mientras que, en la consola de Amazon Redshift, se muestra con las palabras ON o OFF para facilitar su lectura. Cuando esta métrica se muestra en la consola de Amazon Redshift, se omiten los promedios de muestreo y solo se muestra ON o OFF. En Amazon CloudWatch, pueden aparecer otros valores además de 0 y 1 por cuestiones de muestreo. Cualquier valor mayor que 0 para MaintenanceMode se registra como 1 (ON). Unidades: recuento (1/0) (ON/OFF en la consola de Amazon Redshift). Dimensiones: ClusterIdentifier
MaxConfiguredConcurrencyScalingClusters	El número máximo de clústeres de escalado de simultaneidad configurados desde el grupo de parámetros. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift. Unidades: recuento Dimensiones: ClusterIdentifier

Métrica	Descripción
NetworkReceiveThroughput	La velocidad a la que el nodo o el clúster reciben datos. Unidades: bytes/segundo (MB/s en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier
NetworkTransmitThroughput	La velocidad a la que el nodo o el clúster escriben datos. Unidades: bytes/segundo (MB/s en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier
PercentageDiskSpaceUsed	El porcentaje del espacio en disco usado. Unidades: porcentaje Dimensiones: ClusterIdentifier Dimensiones: ClusterIdentifier , NodeID
QueriesCompletedPerSecond	Promedio de consultas completadas por segundo. La información se envía en intervalos de 5 minutos. Esta métrica no se admite en los clústeres de un solo nodo. Unidades: recuento/segundo Dimensiones: ClusterIdentifier , latency Dimensiones: ClusterIdentifier , wlmid

Métrica	Descripción
QueryDuration	Tiempo medio que tarda en completarse una consulta. La información se envía en intervalos de 5 minutos. Esta métrica no se admite en los clústeres de un solo nodo. Unidades: microsegundos Dimensiones: ClusterIdentifier , NodeID, latency Dimensiones: ClusterIdentifier , latency Dimensiones: ClusterIdentifier , NodeID, wlmid
QueryRuntimeBreakdown	El tiempo total que las consultas dedican a ejecutarse por etapa de consulta. La información se envía en intervalos de 5 minutos. Unidades: milisegundos Dimensiones: ClusterIdentifier, NodeID, etapa Dimensiones: ClusterIdentifier, etapa
ReadIOPS	El número medio de operaciones de lectura en disco por segundo. Unidades: recuento/segundo Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier
ReadLatency	Tiempo medio de cada operación de E/S de lectura en disco. Unidades: segundos Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier

Métrica	Descripción
ReadThroughput	El número medio de bytes leídos del disco por segundo. Unidades: bytes (GB/s en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier
RedshiftManagedStorageTotalCapacity	Capacidad total de almacenamiento administrado. Unidades: megabytes Dimensiones: ClusterIdentifier
TotalTableCount	Número de tablas de usuario abiertas en un momento determinado. Este total no incluye tablas de Amazon Redshift Spectrum. Unidades: recuento Dimensiones: ClusterIdentifier
WLMQueueLength	El número de consultas en la cola para una cola de administración de carga de trabajo (WLM). Unidades: recuento Dimensiones: ClusterIdentifier , service class Dimensiones: ClusterIdentifier , QueueName

Métrica	Descripción
WLMQueueWaitTime	El tiempo de consultas invertido en esperar en la cola de administración de carga de trabajo (WLM). La información se envía en intervalos de 5 minutos. Unidades: milisegundos. Dimensiones: ClusterIdentifier , QueryPriority Dimensiones: ClusterIdentifier , wlmid Dimensiones: ClusterIdentifier , QueueName
WLMQueriesCompletedPerSecond	Número medio de consultas completadas por segundo en una cola de administración de carga de trabajo (WLM). La información se envía en intervalos de 5 minutos. Esta métrica no se admite en los clústeres de un solo nodo. Unidades: recuento/segundo Dimensiones: ClusterIdentifier , wlmid Dimensiones: ClusterIdentifier , QueueName
WLMQueryDuration	Tiempo medio que tarda en completarse una consulta en una cola de administración de carga de trabajo (WLM). La información se envía en intervalos de 5 minutos. Esta métrica no se admite en los clústeres de un solo nodo. Unidades: microsegundos Dimensiones: ClusterIdentifier , wlmid Dimensiones: ClusterIdentifier , QueueName

Métrica	Descripción
WLMRunningQueries	El número de consultas que se ejecutan desde el clúster principal y el clúster de escalado de simultaneidad por cola de WLM. Unidades: recuento Dimensiones: ClusterIdentifier , wlmid Dimensiones: ClusterIdentifier , QueueName
WriteIOPS	El número medio de operaciones de escritura en disco por segundo. Unidades: recuento/segundo Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier
WriteLatency	Tiempo medio de cada operación de E/S de escritura en disco. Unidades: segundos Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier
WriteThroughput	Número medio de bytes que se escriben en el disco por segundo. Unidades: bytes (GB/s en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier , NodeID Dimensiones: ClusterIdentifier

Métrica	Descripción
SchemaQuota	La cuota configurada para un esquema. Unidades: megabytes Dimensiones: ClusterIdentifier , Database, Schema Periódica/push: Periodic Frecuencia: 5 minutes Criterios de detención: esquema eliminado o cuota eliminada
NumExceededSchemaQuotas	El número de esquemas con cuotas superadas. Unidades: recuento Dimensiones: ClusterIdentifier Periódica/push: Periodic Frecuencia: 5 minutes Criterios de detención: N/A
StorageUsed	El espacio de almacenamiento o disco utilizado por un esquema. Unidades: megabytes Dimensiones: ClusterIdentifier , Database, Schema Periódica/push: Periodic Frecuencia: 5 minutes Criterios de detención: esquema eliminado o cuota eliminada

Métrica	Descripción
PercentageQuotaUsed	El porcentaje de espacio de almacenamiento o disco utilizado en relación con la cuota de esquema configurada. Unidades: porcentaje Dimensiones: ClusterIdentifier , Database, Schema Periódica/push: Periodic Frecuencia: 5 minutes Criterios de detención: esquema eliminado o cuota eliminada
UsageLimitAvailable	Según el FeatureType, UsageLimitAvailable devuelve lo siguiente: • Si el FeatureType es CONCURRENCY_SCALING , UsageLimitAvailable devuelve la cantidad total de tiempo que puede utilizar el escalado simultáneo en incrementos de 1 minuto. • Si el FeatureType es CROSS_REGION_DATASHARING , UsageLimitAvailable devuelve la cantidad total de datos que se puede escanear en incrementos de 1 minuto. • Si el FeatureType es SPECTRUM, UsageLimitAvailable devuelve la cantidad total de datos que se puede escanear en incrementos de 1 minuto. Unidades: minutos o TB Dimensiones: ClusterIdentifier , FeatureType , UsageLimitId

Métrica	Descripción
UsageLimitConsumed	Según el FeatureType, UsageLimitConsumed devuelve lo siguiente: • Si el FeatureType es CONCURRENCY_SCALING , UsageLimitAvailable devuelve la cantidad total de tiempo que utiliza el escalado simultáneo en incrementos de 1 minuto. • Si el FeatureType es CROSS_REGION_DATASHARING , UsageLimitAvailable devuelve la cantidad total de datos escaneada en incrementos de 1 minuto. • Si el FeatureType es SPECTRUM, UsageLimitAvailable devuelve la cantidad total de datos escaneada en incrementos de 1 minuto. Unidades: minutos o TB Dimensiones: ClusterIdentifier , FeatureType , UsageLimitId

Dimensiones de métricas de Amazon Redshift

Los datos de Amazon Redshift se pueden filtrar con algunas de las dimensiones de la tabla siguiente.

Dimensión	Descripción
latency	Los valores posibles son los siguientes: • corta: menos de 10 segundos • mediana: entre 10 segundos y 10 minutos • larga: más de 10 minutos
NodeID	Filtra los datos solicitados que son específicos de los nodos de un clúster. NodeID puede ser "Leader (Principal)", "Shared (Compartido)", o "Compute-N (N-computación)", donde N puede ser 0, 1, etc. en función del número de nodos del

Dimensión	Descripción
	clúster. "Shared" significa que el clúster tiene un solo nodo, es decir, que el nodo principal y el nodo de computación están combinados. Las métricas de `CPUUtilization` , `NetworkTransmitThroughput` y `ReadIOPS` se registran únicamente para el nodo principal y los nodos de computación. Otras métricas que usan la dimensión `NodeId` se registran solo para los nodos de computación.
`ClusterIdentifier`	Filtra los datos solicitados que son específicos del clúster. Las métricas específicas del clúster son `HealthStatus` , `MaintenanceMode` y `DatabaseConnections` . Las métricas generales de esta dimensión (por ejemplo, `ReadIOPS`), que también son métricas de nodos, representan el total acumulado de datos de métricas de nodos. Preste especial atención cuando interprete estas métricas, ya que incluyen el comportamiento acumulado tanto del nodo principal como de los nodos de computación.
`service class`	El identificador de una clase de servicio `WLM`.

Dimensión	Descripción
stage	Fases de ejecución de una consulta. Los valores posibles son los siguientes: • QueryPlanning: tiempo invertido en procesar y optimizar instrucciones SQL. • QueryWaiting: tiempo invertido en esperar en la cola de WLM. • QueryExecutingRead: tiempo invertido en ejecutar consultas de lectura. • QueryExecutingInsert: tiempo invertido en ejecutar consultas de inserción. • QueryExecutingDelete: tiempo invertido en ejecutar consultas de eliminación. • QueryExecutingUpdate: tiempo invertido en ejecutar consultas de actualización. • QueryExecutingCtas: tiempo invertido en ejecutar consultas CREATE TABLE AS. • QueryExecutingUnload: tiempo invertido en ejecutar consultas de descarga. • QueryExecutingCopy: tiempo invertido en ejecutar consultas de copia. • QueryCommit: tiempo invertido en confirmar operaciones.
wlmid	Es el identificador de una cola de administración de carga de trabajo.
QueryPriority	La prioridad de la consulta. Los valores posibles son CRITICAL, HIGHEST, HIGH, NORMAL, LOW y LOWEST.
QueueName	El nombre de la cola de administración de cargas de trabajo.
FeatureType	La característica que está limitada por un límite de uso. Los posibles valores son CONCURRENCY_SCALING , CROSS_REGION_DATASHARING y SPECTRUM.

Dimensión	Descripción
`UsageLimitId`	El identificador del límite de uso.

Datos de rendimiento de cargas y consultas de Amazon Redshift

Además de las métricas de CloudWatch, Amazon Redshift proporciona datos de rendimiento de cargas y consultas. Los datos de rendimiento de cargas y consultas se pueden utilizar para ayudarle a comprender la relación entre el rendimiento de la base de datos y las métricas de clúster. Por ejemplo, si observa que la CPU de un clúster alcanzo su pico, puede encontrar el pico en el gráfico de CPU del clúster y ver las consultas que se estaban ejecutando en ese momento. De igual forma, si está revisando una consulta específica, los datos de métricas (como los de CPU) se muestran en contexto para que pueda comprender el impacto de la consulta en las métricas de clúster.

Los datos de rendimiento de cargas y consultas no se publican como las métricas de CloudWatch y solo pueden verse en la consola de Amazon Redshift. Los datos de rendimiento de cargas y consultas se generan a partir de consultas de las tablas de sistema de la base de datos (para obtener más información, consulte Referencia de las tablas de sistema en la Guía para desarrolladores de Amazon Redshift). También puede generar sus propias consultas personalizadas de rendimiento de la base de datos, pero recomendamos comenzar con los datos de rendimiento de cargas y consultas que se presentan en la consola. Para obtener más información acerca de la medición y el monitoreo del rendimiento de la base de datos, consulte Administración del rendimiento en la Guía para desarrolladores de Amazon Redshift.

En la siguiente tabla, se describen los diferentes aspectos de los datos de cargas y consultas a los que puede obtener acceso en la consola de Amazon Redshift.

Datos de cargas/consultas	Descripción
Resumen de consultas	Lista de consultas en un período de tiempo específico. La lista se puede ordenar por valores como el ID de consulta, tiempo de ejecución de la consulta y el estado. Consulte estos datos en la pestaña Monitoreo de consultas de la página de detalles del clúster.
Detalle de consulta	Proporciona detalles de una consulta en particular, incluidos:

Datos de cargas/consultas	Descripción
	• Las propiedades de la consulta como el ID de consulta, el tipo, el clúster en el que se ejecutó la consulta y el tiempo de ejecución. • Detalles como el estado de consulta y el número de errores. • La instrucción SQL que se ejecutó. • Un plan de explicación, si está disponible. • Datos de rendimiento del clúster durante la ejecución de la consulta (para obtener más información, consulte Visualización de datos del historial de consultas).
Resumen de cargas	Muestra todas las cargas en un período de tiempo específico. La lista se puede ordenar por valores como el ID de consulta, tiempo de ejecución de la consulta y el estado. Consulte estos datos en la pestaña Monitoreo de consultas de la página de detalles del clúster.
Detalle de carga	Proporciona detalles de una operación de carga en particular, incluidos: • Las propiedades de la carga, como el ID de consulta, el tipo, el clúster en el que se ejecutó la consulta y el tiempo de ejecución. • Detalles como el estado de carga y el número de errores. • La instrucción SQL que se ejecutó. • Una lista de archivos cargados. • Datos de rendimiento del clúster durante la operación de carga (para obtener más información, consulte Visualización de datos del historial de consultas).

Uso de los datos de rendimiento en la consola de Amazon Redshift

En esta sección, encontrará cómo ver los datos de rendimiento en la consola de Amazon Redshift, que incluye información acerca del rendimiento del clúster y de las consultas. Además, puede crear alarmas en las métricas de clúster directamente desde la consola de Amazon Redshift.

Cuando ve los datos de rendimiento en la consola de Amazon Redshift, lo hace según clúster. Los gráficos de datos de rendimiento para un clúster están diseñados para brindarle acceso a los datos

para responder a las preguntas de rendimiento más comunes. Para algunos datos de rendimiento (consulte Monitoreo de Amazon Redshift mediante las métricas de CloudWatch), también puede utilizar CloudWatch para personalizar aún más los gráficos de métricas. Por ejemplo, puede elegir tiempos más largos o combinar métricas entre clústeres. Para obtener más información acerca del uso de la consola de CloudWatch, consulte Uso de métricas de rendimiento en la consola de CloudWatch.

Vea el siguiente video para obtener información acerca de cómo monitorear, aislar y optimizar las consultas usando las características de monitoreo de las consultas de la consola de Amazon Redshift: Query Monitoring with Amazon Redshift.

Temas

- Visualización de datos de rendimiento del clúster
- Visualización de datos del historial de consultas
- Visualización de datos de rendimiento de la base de datos
- Visualización de datos de escalado de simultaneidad y simultaneidad de cargas de trabajo
- Visualización de consultas y cargas
- Visualización de métricas de clúster durante las operaciones de carga
- Análisis del rendimiento de las cargas de trabajo
- Administración de alarmas
- Uso de métricas de rendimiento en la consola de CloudWatch

Visualización de datos de rendimiento del clúster

Cuando utiliza las métricas de clúster en Amazon Redshift, puede realizar las siguientes tareas de rendimiento comunes:

- Determinar si las métricas de clúster están fuera de lo normal en un intervalo de tiempo especificado y, si es así, identificar las consultas responsables de este error en el rendimiento.
- Comprobar si las consultas actuales o históricas están impactando en el rendimiento del clúster. Si identifica una consulta problemática, puede ver sus detalles incluyendo el rendimiento del clúster durante la ejecución de la consulta. Puede utilizar esta información a la hora de diagnosticar el motivo por el que la consulta es lenta y lo que se puede hacer para mejorar su rendimiento.

Para ver los datos de desempeño

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre de un clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).
3. Elija la pestaña Cluster performance (Rendimiento del clúster) para ver la información del rendimiento, incluido:

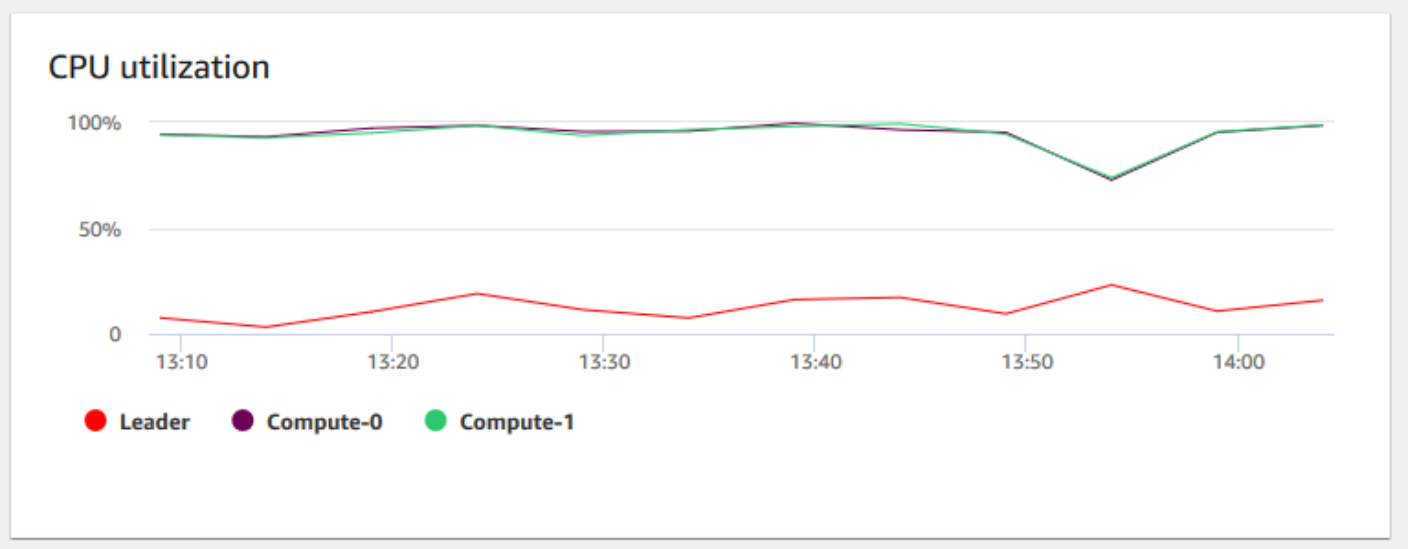
   - Utilización de la CPU
   - Porcentaje de espacio del disco usado
   - Conexiones a base de datos
   - Estado
   - Query duration
   - Query throughput
   - Actividad de escalado de simultaneidad

   Hay muchas más métricas disponibles. Para ver las métricas disponibles y elegir cuáles se muestran, seleccione el icono Preferencias.

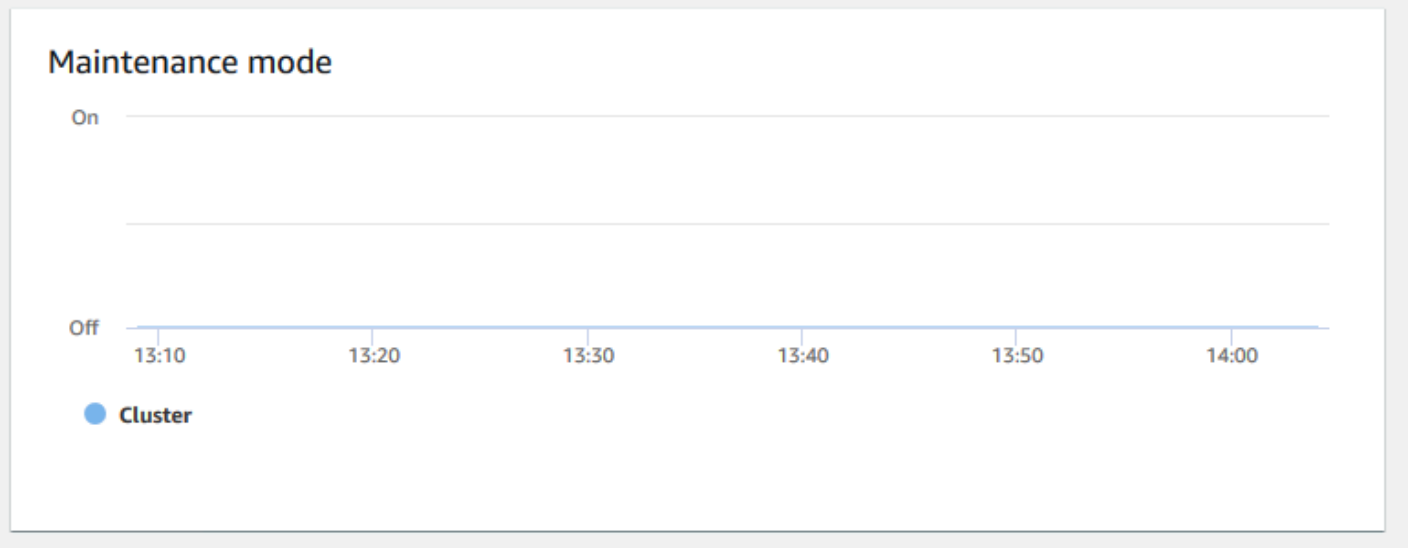
Gráficos de rendimiento del clúster

En los siguientes ejemplos se pueden observar algunos de los gráficos que se muestran en la nueva consola de Amazon Redshift.

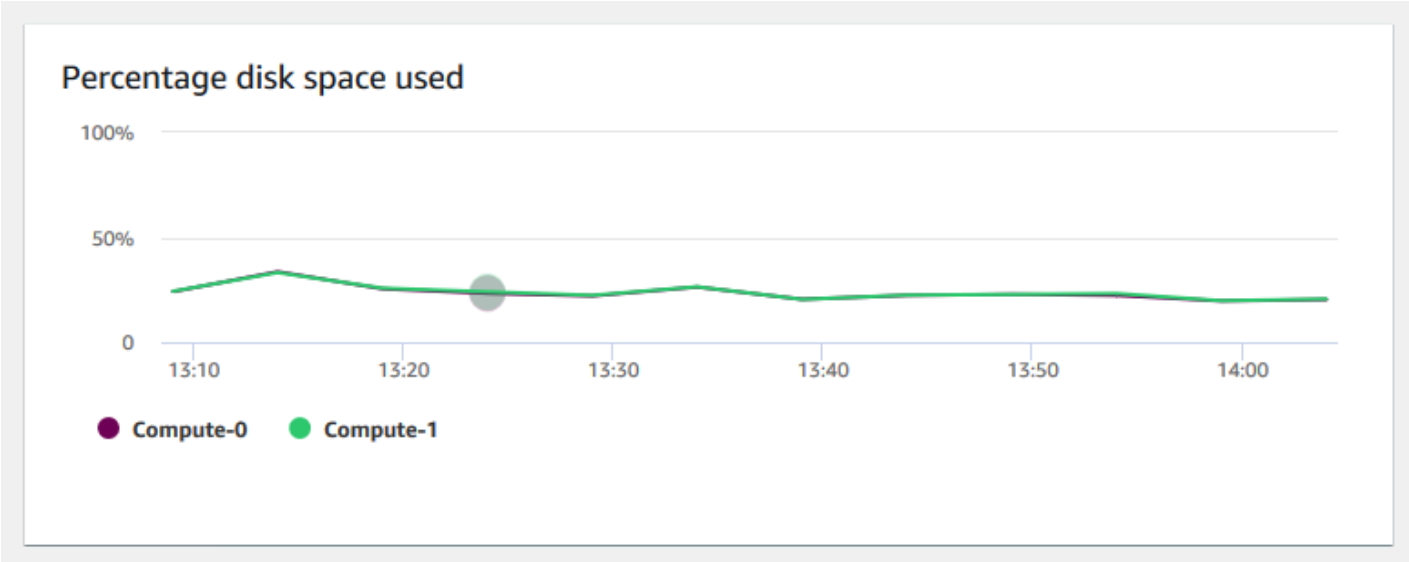
- Utilización de la CPU: muestra el porcentaje de utilización de la CPU para todos los nodos (principales y de informática). Para encontrar un momento en el que el uso del clúster sea inferior antes de programar la migración del clúster u otras operaciones que consumen recursos, monitoree este gráfico para ver la utilización de la CPU en cada uno de los nodos o en todos ellos.



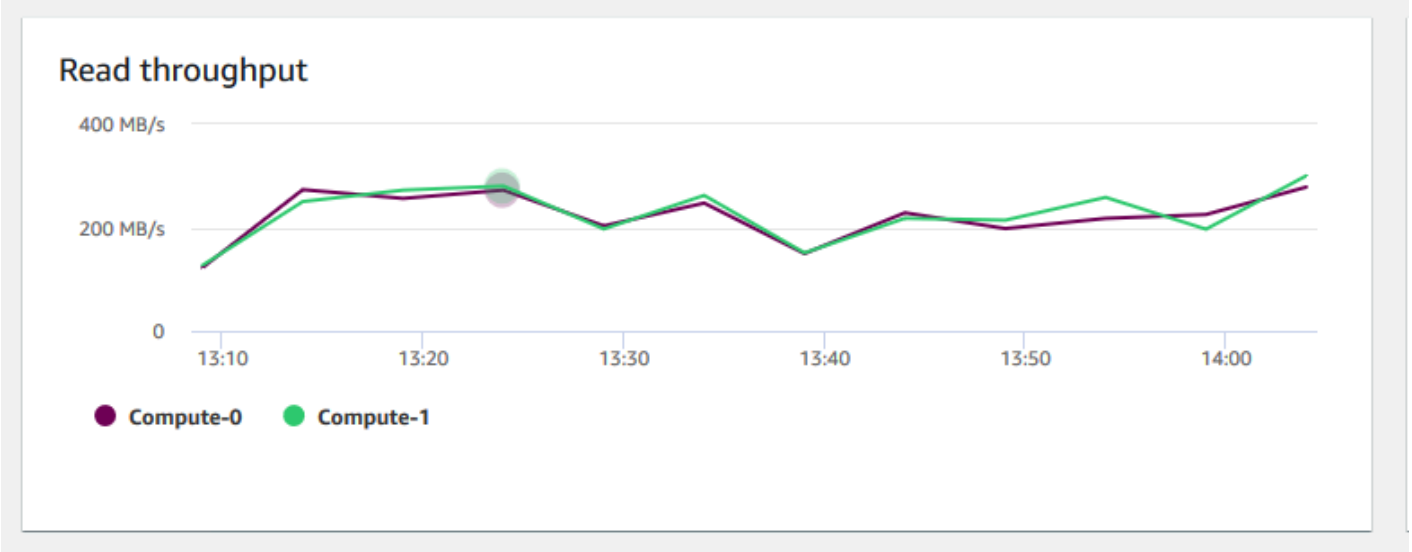
- Modo de mantenimiento: muestra si el clúster está en el modo de mantenimiento en un momento elegido mediante los indicadores `On` y `Off`. Puede ver la hora en que el clúster está en proceso de mantenimiento. A continuación, puede correlacionar esta hora con las operaciones que se realizan en el clúster para estimar períodos de inactividad futuros para eventos recurrentes.



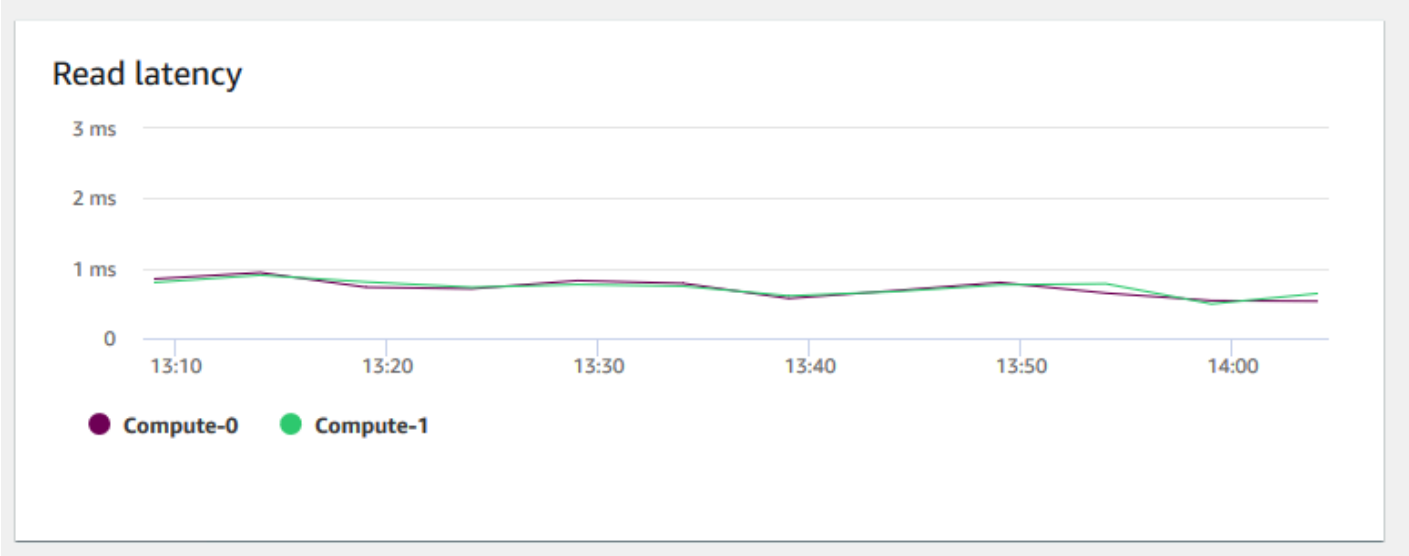
- Porcentaje de espacio del disco usado: muestra el porcentaje de uso de espacio en disco por cada nodo informático, y no para el clúster como un todo. Puede explorar este gráfico para monitorear la utilización del disco. Las operaciones de mantenimiento como VACUUM y COPY utilizan espacio de almacenamiento temporal intermedio para sus operaciones de clasificación, por lo que se espera un aumento en el uso del disco.



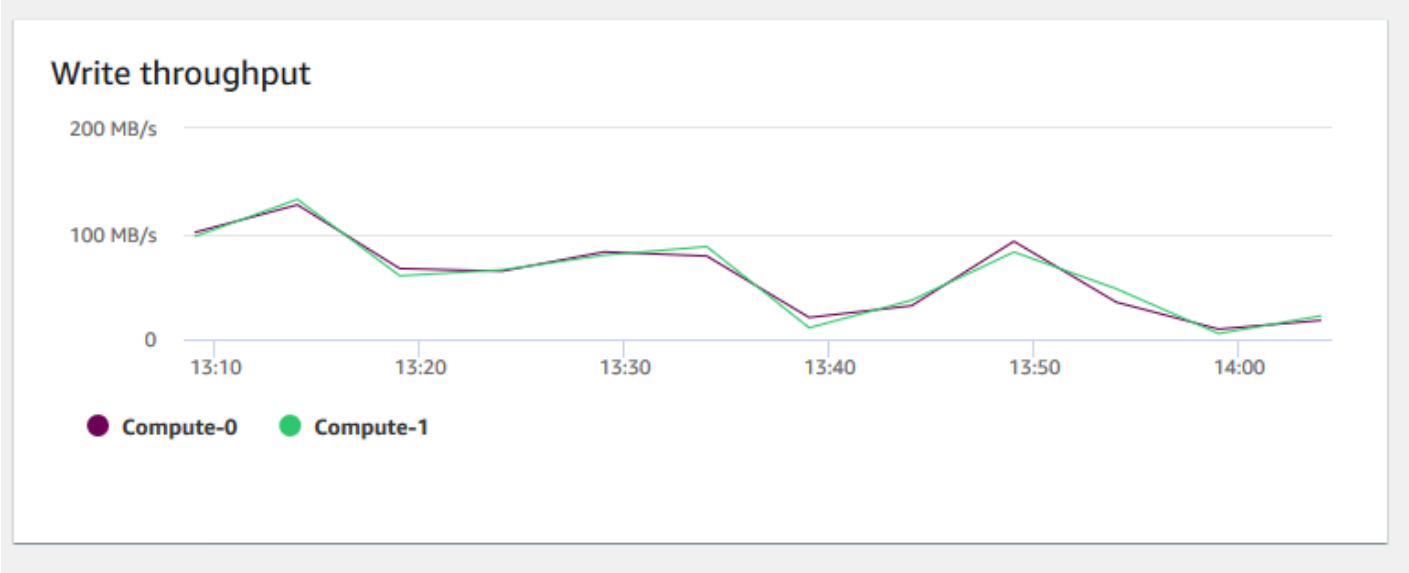
- Rendimiento de lectura: muestra el número promedio de megabytes leídos en el disco por segundo. Puede evaluar este gráfico para monitorear el aspecto físico correspondiente del clúster. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y su volumen.



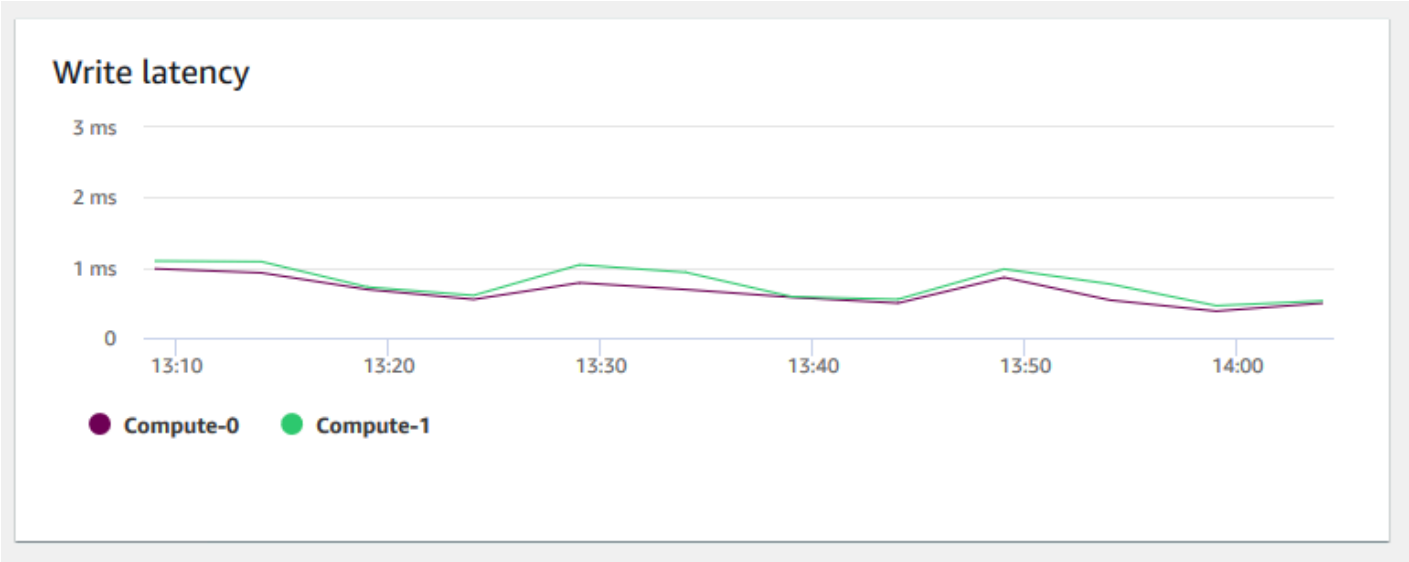
- Latencia de lectura: muestra el tiempo promedio de cada operación de E/S de lectura en disco por milisegundo. Puede ver los tiempos de respuesta para que se devuelvan los datos. Cuando la latencia es alta, significa que el remitente pasa más tiempo inactivo (sin enviar paquetes nuevos), lo que reduce la rapidez con que crece el rendimiento.



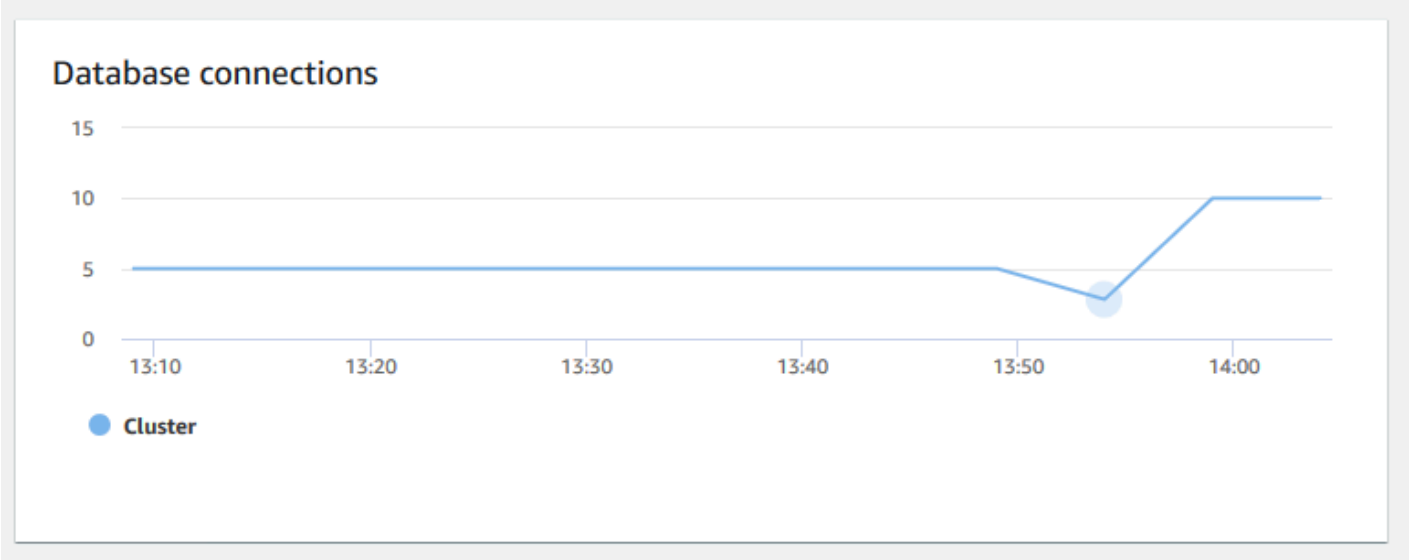
- Rendimiento de escritura: muestra el número promedio de megabytes escritos en el disco por segundo. Puede evaluar esta métrica para monitorear el aspecto físico correspondiente del clúster. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y su volumen.



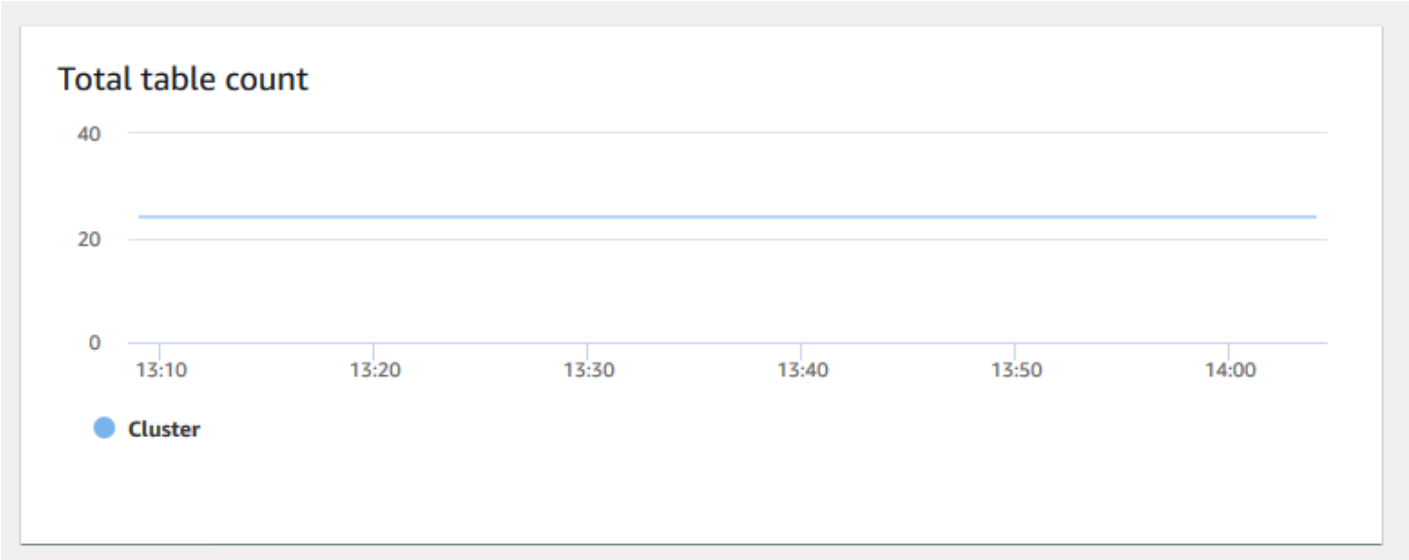
- Latencia de escritura: muestra el tiempo promedio en milisegundos de cada operación de E/S de escritura en disco. Puede evaluar el tiempo para que se devuelva el reconocimiento de la escritura. Cuando la latencia es alta, significa que el remitente pasa más tiempo inactivo (sin enviar paquetes nuevos), lo que reduce la rapidez con que crece el rendimiento.



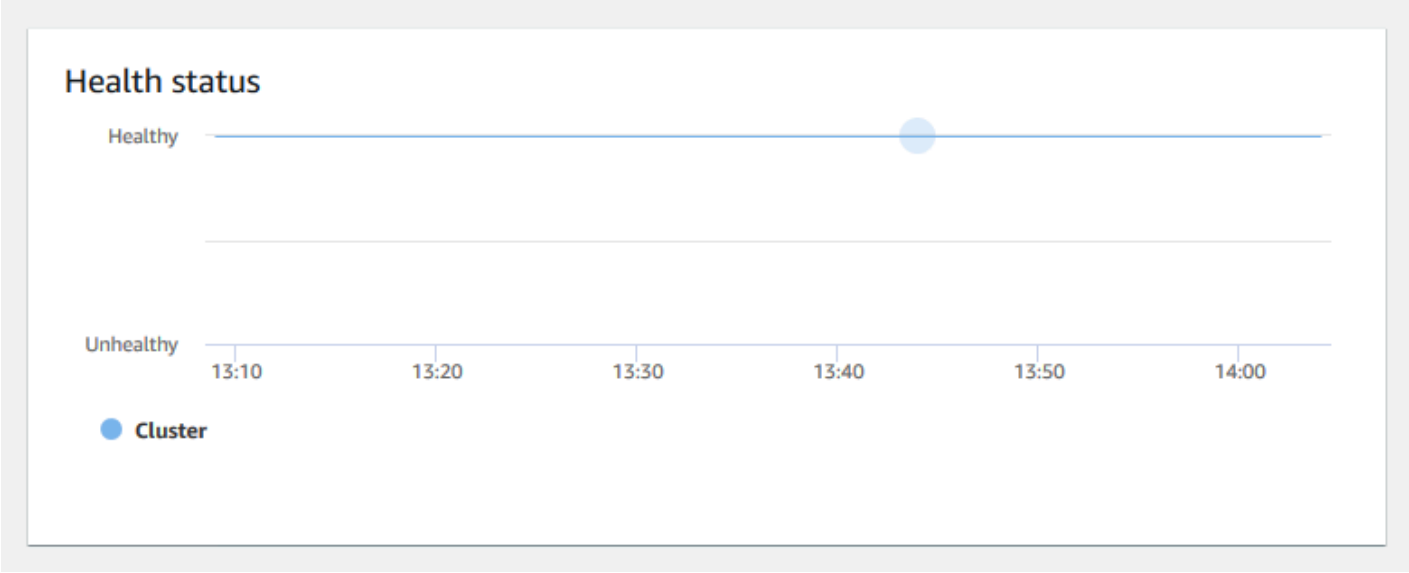
- Conexiones de bases de datos: muestra el número de conexiones de bases de datos a un clúster. Puede utilizar este gráfico para ver cuántas conexiones se establecen a la base de datos y encontrar una hora en la que el uso del clúster es menor.



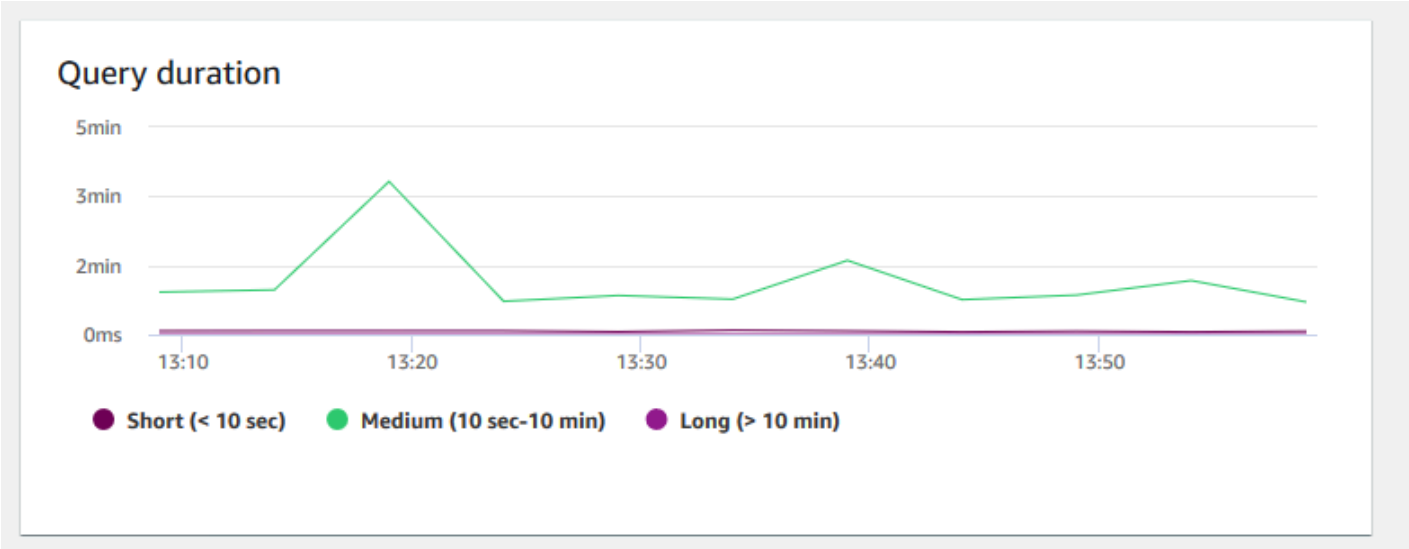
- Recuento total de tablas: muestra el número de tablas de usuario abiertas en un momento determinado en un clúster. Puede monitorear el rendimiento del clúster cuando el recuento de tablas abiertas es alto.



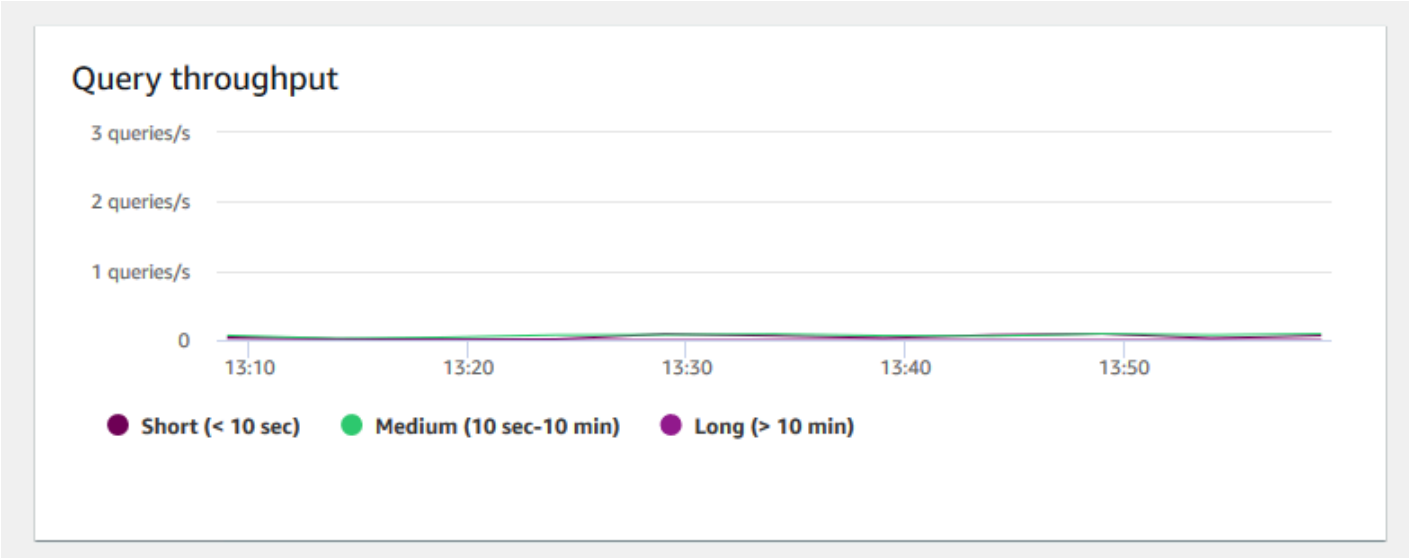
- Estado: indica si el estado del clúster es `Healthy` o `Unhealthy`. Si el clúster puede conectarse a su base de datos y realiza correctamente una consulta sencilla, se considera que el clúster está en buen estado. De lo contrario, se considera que el clúster está en mal estado. Un estado incorrecto se puede producir cuando la base de datos del clúster está sobrecargada en exceso o cuando hay un problema de configuración con una base de datos del clúster.



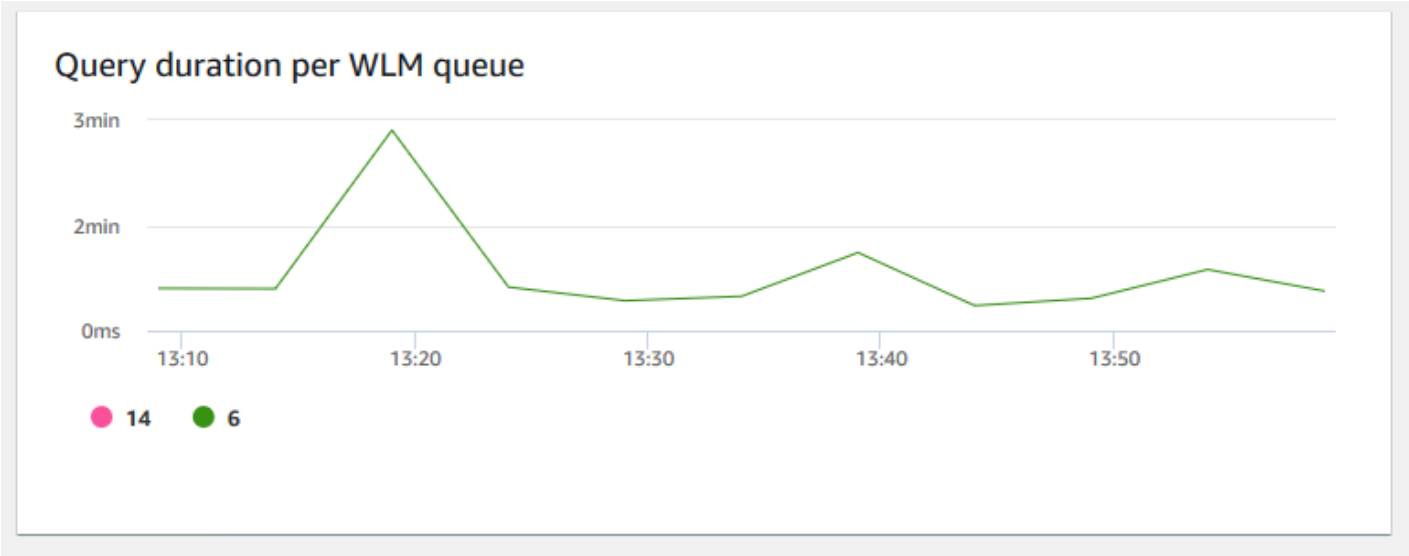
- Duración de la consulta: muestra el tiempo promedio que tarda en completarse una consulta en microsegundos. Puede comparar los datos de este gráfico para medir el rendimiento de E/S dentro del clúster y ajustar sus consultas más largas si es necesario.



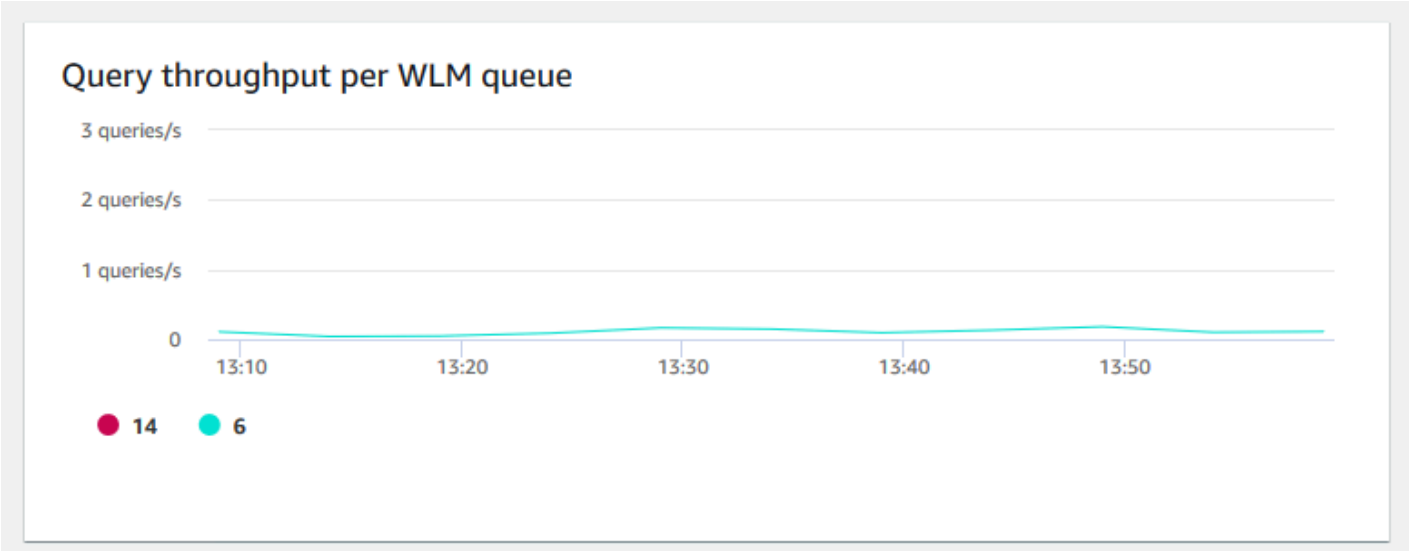
- Rendimiento de la consulta: muestra el número promedio de consultas completadas por segundo. Puede analizar los datos de este gráfico para medir el rendimiento de la base de datos y caracterizar la capacidad del sistema para admitir una carga de trabajo multiusuario de manera equilibrada.



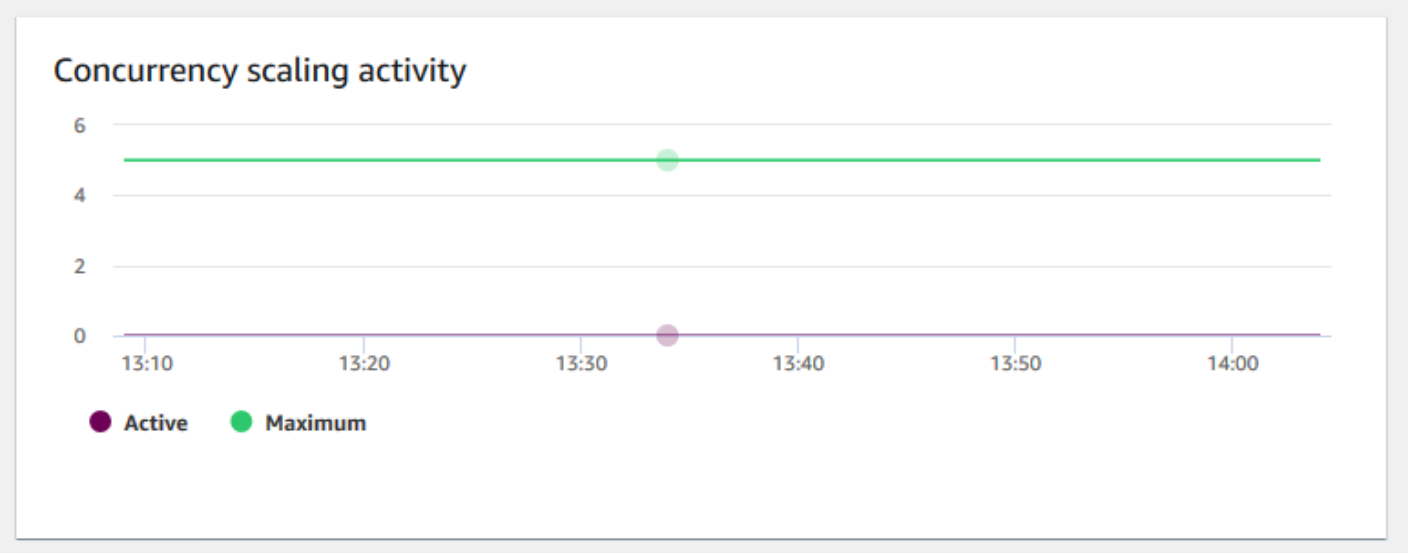
- Duración de la consulta por cola de WLM: muestra el tiempo promedio que tarda en completarse una consulta en microsegundos. Puede comparar los datos de este gráfico para medir el rendimiento de E/S por cola de WLM y ajustar sus consultas más largas si es necesario.



- Rendimiento de consulta por cola de WLM: muestra el número promedio de consultas completadas por segundo. Puede analizar los datos de este gráfico para medir el rendimiento de la base de datos por cola de WLM.



- Actividad de escalado de simultaneidad: muestra el número de clústeres de escalado de simultaneidad activos. Cuando el escalado de simultaneidad está habilitado, Amazon Redshift agrega capacidad del clúster de manera automática si se necesita para procesar un aumento de las consultas de lectura simultáneas.



Visualización de datos del historial de consultas

Puede utilizar métricas del historial de consultas en Amazon Redshift para realizar lo siguiente:

- Aislar y diagnosticar problemas de rendimiento de consultas.
- Comparar las métricas de tiempo de ejecución de la consulta y las métricas de rendimiento del clúster en la misma línea temporal para ver cómo pueden estar relacionadas ambas. Al hacerlo, podrá identificar consultas con mal rendimiento, buscar consultas con cuellos de botella y determinar si necesita cambiar el tamaño del clúster para la carga de trabajo.
- Acceda a los detalles de una consulta específica eligiéndola en la línea temporal. Cuando el ID de consulta y otras propiedades se muestran en una fila debajo del gráfico, puede elegir la consulta para ver los detalles de la consulta. Los detalles incluyen, por ejemplo, la instrucción SQL de la consulta, los detalles de ejecución y el plan de consulta. Para obtener más información, consulte Visualización de detalles de consultas.
- Determine si los trabajos de carga se realizan correctamente y cumplen los acuerdos de nivel de servicio (SLA).

Para mostrar datos del historial de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden

incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).

3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija la pestaña Historial de consultas.

   Mediante los controles de la ventana, puede alternar entre Lista de consultas y Métricas de clúster.

   Al elegir Lista de consultas, la pestaña incluye los siguientes gráficos:

   - Tiempo de ejecución de consultas: la actividad de consulta en una línea temporal. Utilice este gráfico para ver qué consultas se están ejecutando en el mismo periodo de tiempo. Elija una consulta para ver más detalles de ejecución de la consulta. El eje x muestra el periodo seleccionado. Puede filtrar las consultas gráficas por: en ejecución, finalizadas, cargadas, etc. Cada barra representa una consulta y la longitud de la barra representa su tiempo de ejecución desde el principio de la barra hasta el final. Las consultas pueden incluir instrucciones de manipulación de datos SQL (como SELECT, INSERT, DELETE) y cargas (como COPY). De forma predeterminada, las 100 consultas en ejecución más largas se muestran para el periodo de tiempo seleccionado.
   - Consultas y cargas: lista de consultas y cargas que se ejecutaron en el clúster. La ventana incluye una opción para Terminar la consulta si una consulta se está ejecutando actualmente.

   Al elegir Métricas de clúster, la pestaña incluye los siguientes gráficos:

   - Tiempo de ejecución de consultas: la actividad de consulta en una línea temporal. Utilice este gráfico para ver qué consultas se están ejecutando en el mismo periodo de tiempo. Elija una consulta para ver más detalles de ejecución de la consulta.
   - Utilización de la CPU: la utilización de la CPU del clúster por nodo principal y el promedio de nodos informáticos.
   - Capacidad de almacenamiento utilizada: el porcentaje de la capacidad de almacenamiento utilizada.
   - Conexiones de base de datos activas: el número de conexiones de base de datos al clúster activas.

Tenga en cuenta lo siguiente al trabajar con los gráficos del historial de consultas:

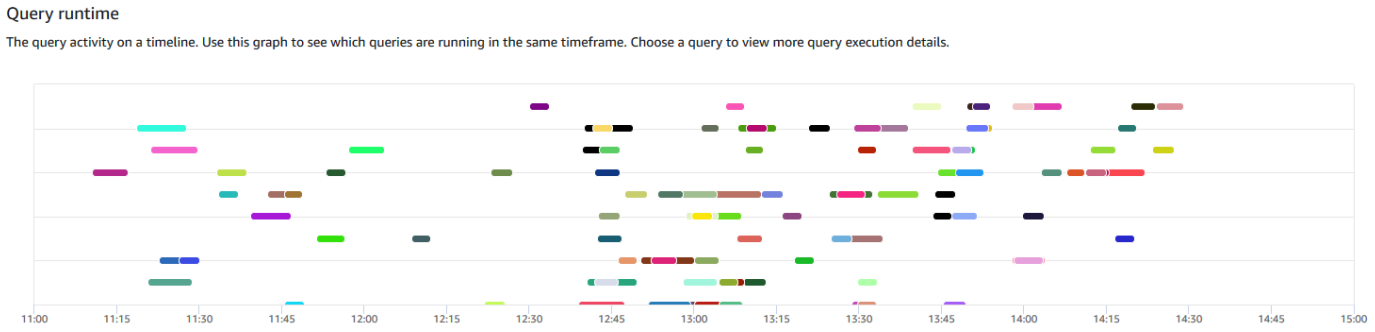
- Elija una barra que represente una consulta específica en el gráfico Tiempo de ejecución de consultas para ver detalles sobre esa consulta. También puede elegir un ID de consulta en la lista de Consultas y cargas para ver sus detalles.
- Puede seleccionar una sección del gráfico Tiempo de ejecución de consultas para ampliar y mostrar un periodo de tiempo específico.
- En el gráfico Tiempo de ejecución de consultas, para que el filtro elegido considere todos los datos y pase por todas las páginas mostradas en la lista Consultas y cargas.
- Puede cambiar las columnas y el número de filas que se muestran en la lista Consultas y cargas mediante la ventana de preferencias mostrada por el icono de engranaje de configuración.
- La lista de Consultas y cargas también se puede mostrar navegando desde el icono de Consultas del navegador izquierdo, Consultas y cargas. Para obtener más información, consulte Visualización de consultas y cargas.

Gráficos de historial de consultas

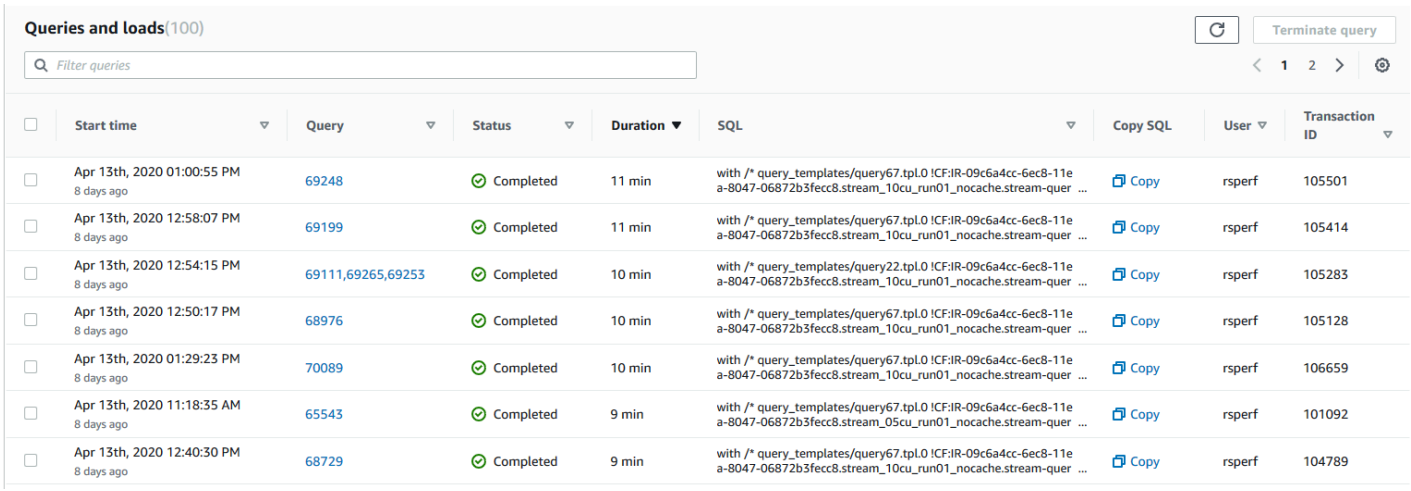
En los siguientes ejemplos, se pueden observar gráficos que se muestran en la nueva consola de Amazon Redshift.

> **Note**
>
> Los gráficos de la consola de Amazon Redshift solo contienen datos de las 100 000 consultas más recientes.

- Tiempo de ejecución de consultas



- Consultas y cargas



Queries and loads(100)

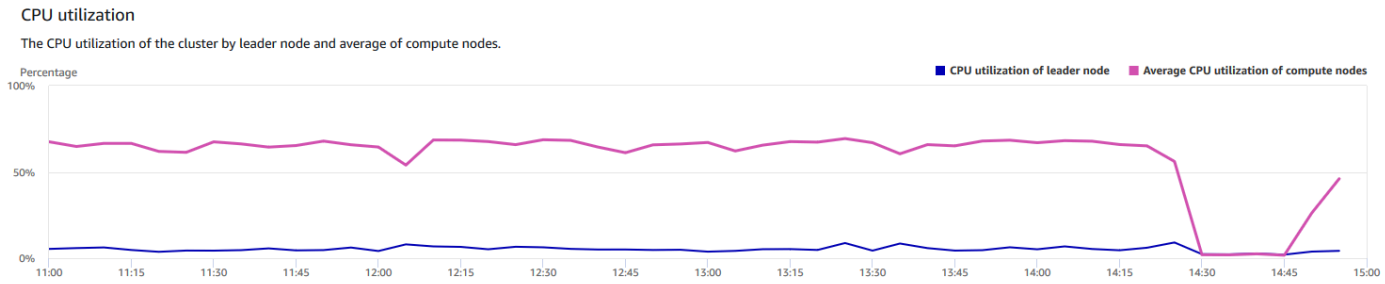
Terminate query

Filter queries

1 2

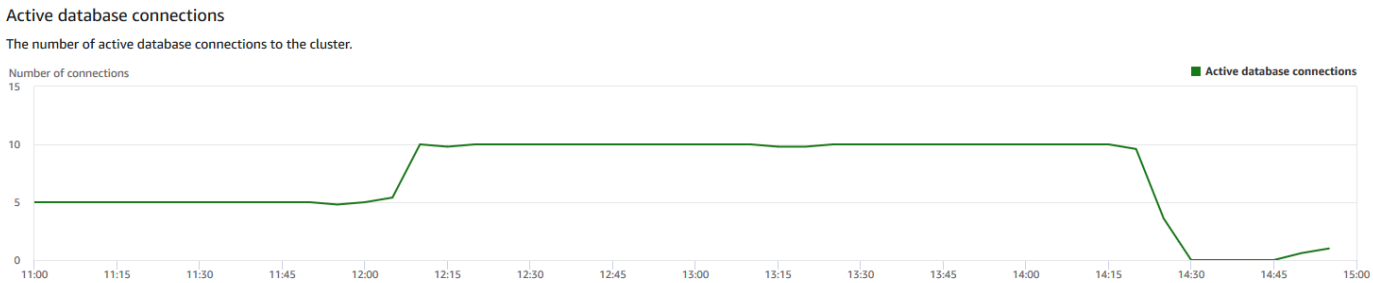
Start time	Query	Status	Duration	SQL	Copy SQL	User	Transaction ID
Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105501
Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105414
Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105283
Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105128
Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	106659
Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ...	Copy	rsperf	101092
Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tpl.0 !CF:IR-09c6a4cc-6ec8-11ea-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	104789

- Utilización de la CPU



- Capacidad de almacenamiento utilizada

- Conexiones de base de datos activas



Visualización de datos de rendimiento de la base de datos

Puede utilizar las métricas de rendimiento de la base de datos en Amazon Redshift para realizar lo siguiente:

- Analizar el tiempo empleado por las consultas por etapas de procesamiento. Puede buscar tendencias inusuales en el tiempo que pasa en una etapa.
- Analizar el número de consultas, la duración y el rendimiento de las consultas por intervalos de duración (corto, medio y largo).
- Buscar tendencias acerca del tiempo de espera de la consulta por prioridad de la consulta (más baja, baja, normal, alta, más alta, crítica).
- Buscar tendencias acerca de la duración de la consulta, el rendimiento o el tiempo de espera de la cola de WLM.

Para mostrar los datos de rendimiento de la base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, incluidas las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija la pestaña Rendimiento de la base de datos.

   Mediante los controles de la ventana, puede alternar entre Métricas de clúster y Métricas de cola de WLM.

   Al elegir Métricas de clúster, la pestaña incluye los siguientes gráficos:

   - Desglose de ejecuciones de cargas de trabajo: tiempo utilizado en las etapas de procesamiento de consultas.
   - Consultas por intervalo de duración: número de consultas cortas, medianas y largas.
   - Rendimiento de las consultas: promedio de consultas completadas por segundo.

- Duración de la consulta: tiempo promedio que tarda en completarse una consulta.
- Tiempo promedio de espera en cola por prioridad: tiempo total que las consultas esperaron en la cola de WLM por prioridad de consulta.

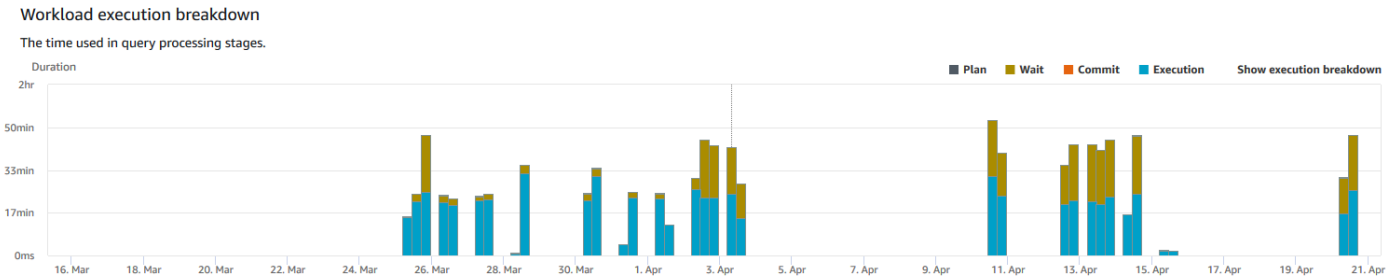
Al elegir Métricas de cola de WLM, la pestaña incluye los siguientes gráficos:

- Duración de la consulta por cola: duración promedio de la consulta por cola de WLM.
- Rendimiento de la consulta por cola: número promedio de consultas completadas por segundo por cola de WLM.
- Tiempo de espera de consulta por cola: duración promedio que las consultas estuvieron en espera en la cola de WLM.

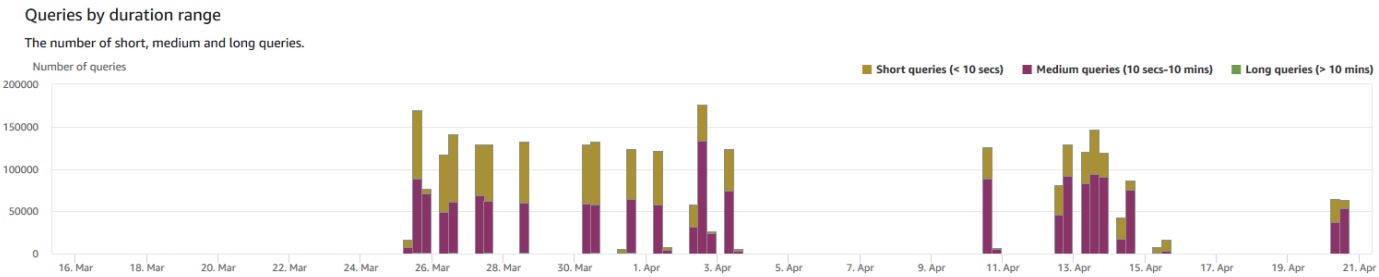
Gráficos de rendimiento de la base de datos

En los siguientes ejemplos, se pueden observar gráficos que se muestran en la nueva consola de Amazon Redshift.

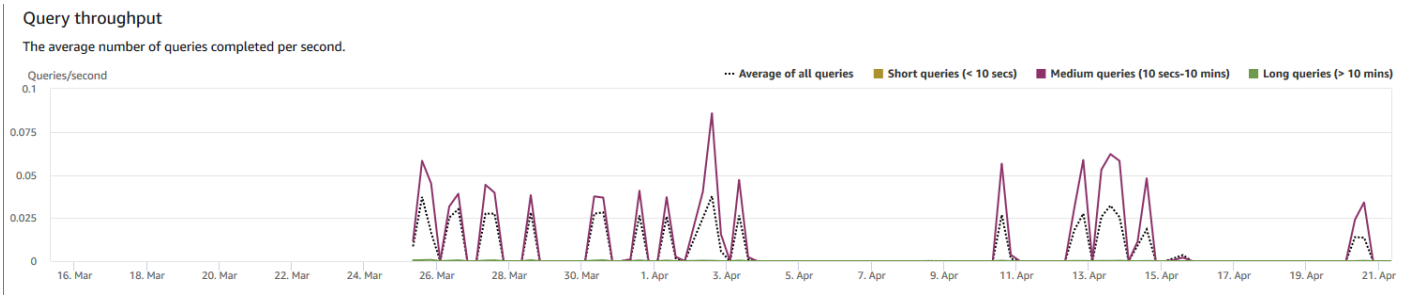
- Desglose de la ejecución de las cargas de trabajo



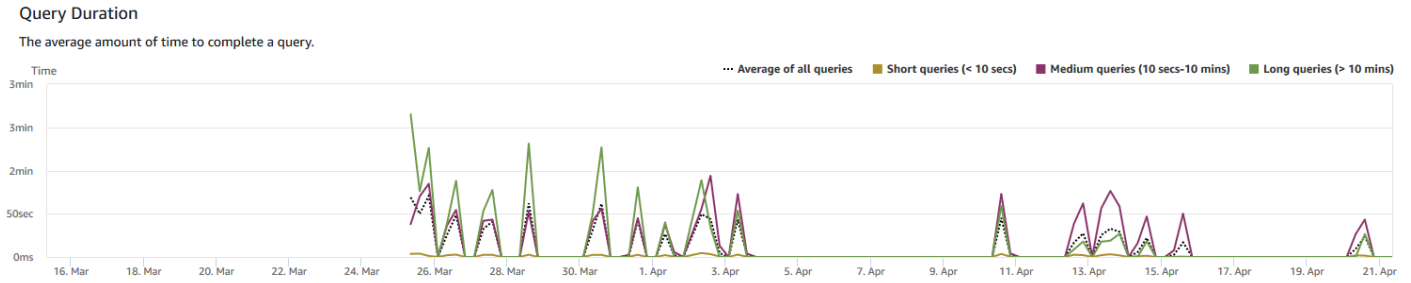
- Consultas por intervalo de duración



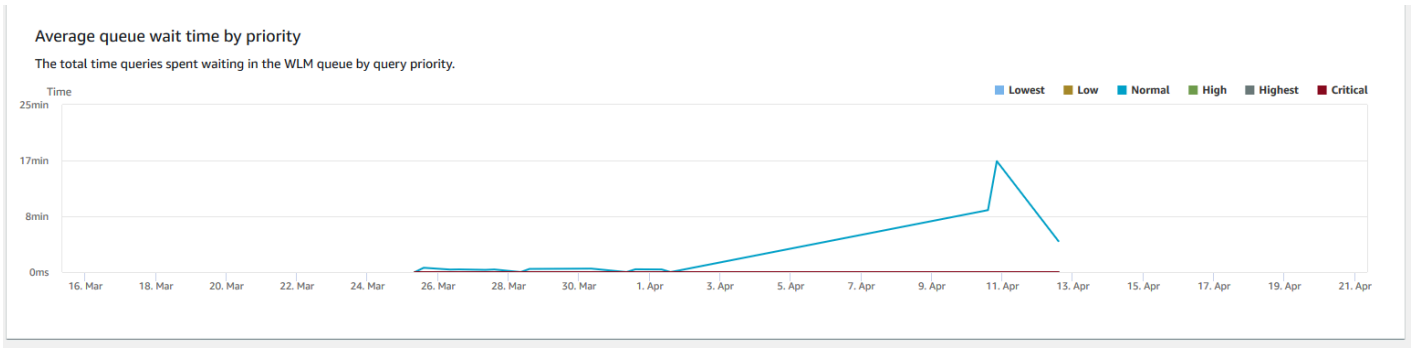
- Query throughput



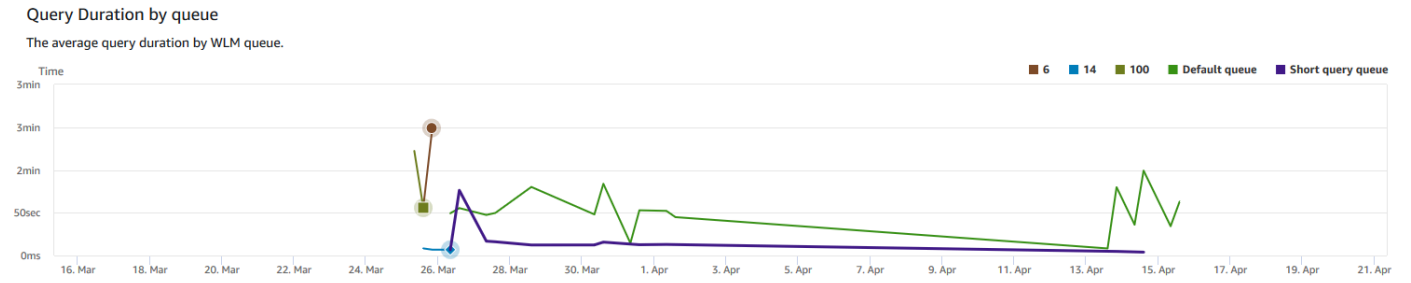
- Query duration



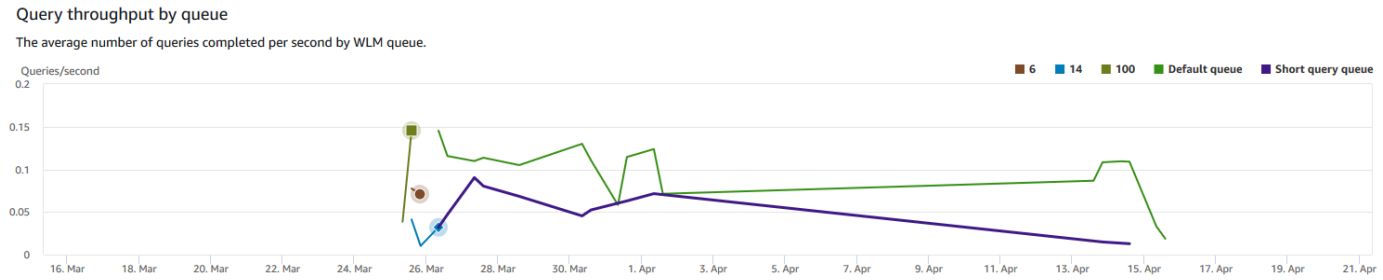
- Tiempo medio de espera de cola por prioridad



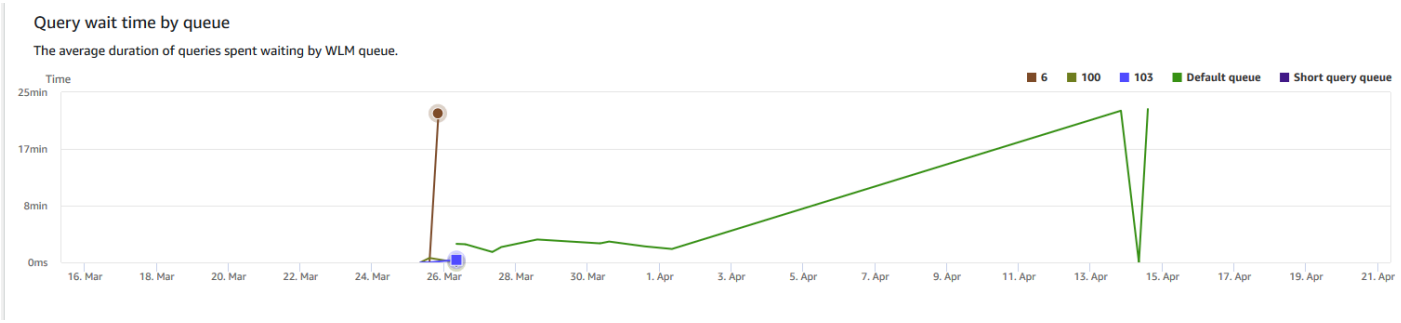
- Duración de la consulta por cola



- Rendimiento de la consulta por cola



- Tiempo de espera de consulta por cola



Visualización de datos de escalado de simultaneidad y simultaneidad de cargas de trabajo

Si utiliza las métricas de escalado de simultaneidad en Amazon Redshift, puede realizar lo siguiente:

- Analice si puede reducir el número de consultas en cola habilitando el escalado de simultaneidad. Puede comparar por cola de WLM o para todas las colas de WLM.
- Ver la actividad de escalado de simultaneidad en clústeres de escalado de simultaneidad. Esto le puede indicar si el escalado de simultaneidad está limitado por el valor de `max_concurrency_scaling_clusters`. En tal caso, puede elegir aumentar el valor `max_concurrency_scaling_clusters` en el parámetro de base de datos.
- Ver el uso total de escalado de simultaneidad de todos los clústeres de escalado de simultaneidad.

Para mostrar los datos de escalado de simultaneidad

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden

incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).

3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija la pestaña Simultaneidad de cargas de trabajo.

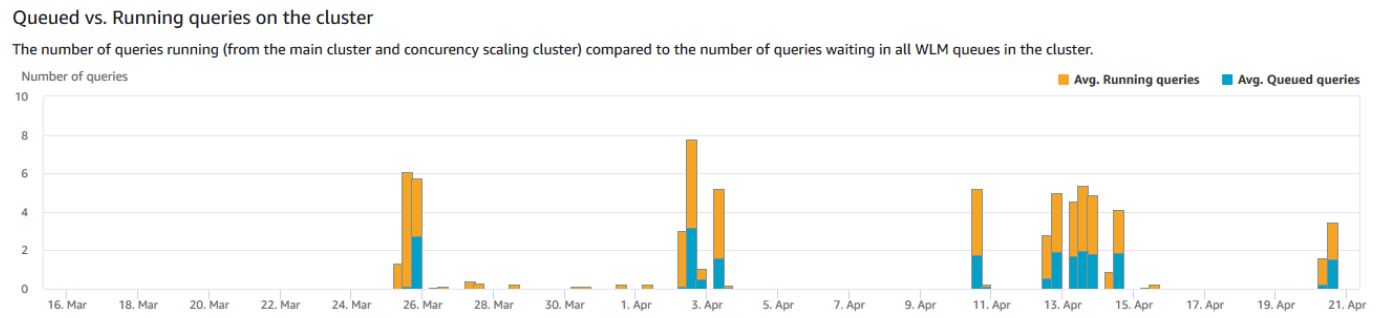
   La pestaña incluye los siguientes gráficos:

   - Comparación entre consultas en cola y consultas en ejecución en el clúster: el número de consultas que se ejecutan (desde el clúster principal y el clúster de escalado de simultaneidad) en comparación con el número de consultas en espera en todas las colas de WLM del clúster.
   - Comparación entre consultas en cola y consultas en ejecución por cola: el número de consultas en ejecución (desde el clúster principal y el clúster de escalado de simultaneidad) en comparación con el número de consultas en espera en cada cola de WLM.
   - Actividad de escalado de simultaneidad: el número de clústeres de escalado de simultaneidad que procesan consultas de forma activa.
   - Uso de escalado de simultaneidad: el uso de clústeres de escalado de simultaneidad que tienen actividad de procesamiento de consultas activa.

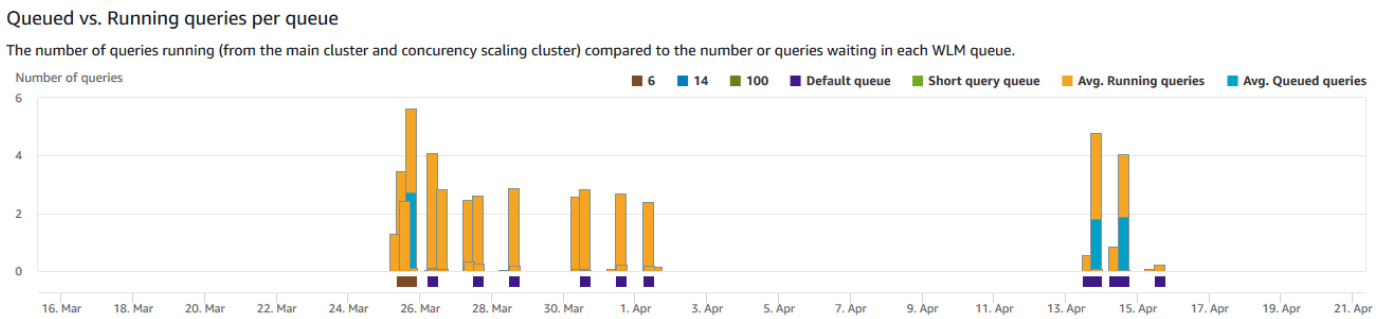
Gráficos de simultaneidad de carga de trabajo

En los siguientes ejemplos, se pueden observar gráficos que se muestran en la nueva consola de Amazon Redshift. Para crear gráficos similares en Amazon CloudWatch, puede utilizar el escalado simultáneo y las métricas de WLM CloudWatch. Para obtener más información acerca de las métricas de CloudWatch para Amazon Redshift, consulte Monitoreo de Amazon Redshift mediante las métricas de CloudWatch.

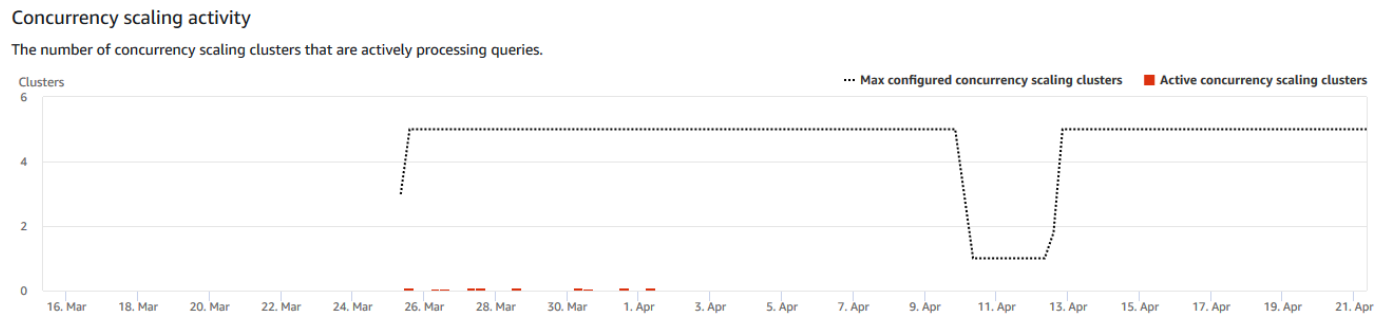
- Comparación entre consultas en cola y consultas en ejecución en el clúster



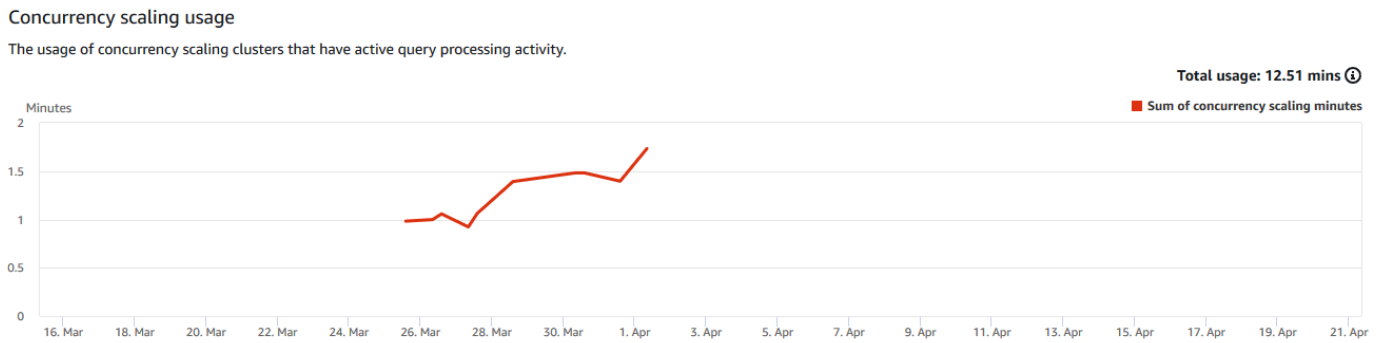
- Comparación entre consultas en cola y consultas en ejecución por cola



- Actividad de escalado de simultaneidad



- Uso de escalado de simultaneidad



Visualización de consultas y cargas

La consola de Amazon Redshift proporciona información acerca de las consultas y las cargas que se ejecutan en la base de datos. Puede utilizar esta información para identificar y solucionar problemas de las consultas que tardan demasiado tiempo para procesarse y provocan cuellos de botella que impiden que las otras consultas se procesen de forma eficaz. Puede utilizar la información de las consultas en la consola de Amazon Redshift para monitorear el procesamiento de consultas.

Para mostrar datos de rendimiento de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Queries and loads (Consultas y cargas) para mostrar la lista de consultas de la cuenta.

   Por defecto, la lista muestra consultas de todos sus clústeres durante las últimas 24 horas. Puede cambiar el alcance de los datos mostrados en la consola.

   > **Important**
   >
   > La pestaña Queries and loads (Consultas y cargas) muestra las consultas que han tardado más tiempo en ejecutarse en el sistema (hasta 100 consultas).

Finalizar una consulta en ejecución

También puede utilizar la página Queries (Consultas) para finalizar una consulta que esté en proceso.

> **Note**
>
> La capacidad para terminar consultas y cargas en la consola de Amazon Redshift requiere un permiso específico. Si desea que los usuarios puedan terminar consultas y cargas, asegúrese de añadir la acción `redshift:CancelQuerySession` a la política de AWS Identity and Access Management (IAM). Este requisito se aplica si selecciona la política administrada por AWS de solo lectura de Amazon Redshift o si crea una política personalizada en IAM. Los usuarios que tienen la política de acceso completo de Amazon Redshift ya cuentan con los permisos necesarios para terminar las consultas y las

cargas. Para obtener más información acerca de las acciones de las políticas de IAM para Amazon Redshift, consulte Administrar el acceso a los recursos.

Para finalizar una consulta en ejecución

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Queries and loads (Consultas y cargas) para mostrar la lista de consultas de la cuenta.
3. Seleccione la consulta en ejecución que quiera finalizar en la lista, y luego seleccione Terminate query (Finalizar consulta).

Visualización de detalles de consultas

Puede analizar los detalles de la consulta en la consola de Amazon Redshift. Con un identificador de consulta, puede consultar los detalles de una consulta. Los detalles pueden incluir, por ejemplo, el estado de finalización de la consulta, la duración, la instrucción SQL y si se trata de una consulta de usuario o una que ha sido reescrita por Amazon Redshift. Una consulta de usuario es una consulta que se envía a Amazon Redshift, ya sea desde un cliente de SQL o mediante una herramienta de inteligencia empresarial. Es posible que Amazon Redshift reescriba la consulta para optimizarla, y esto puede dar lugar a varias consultas reescritas. Aunque Amazon Redshift realiza el proceso, verá las consultas reescritas en la página de detalles de la consulta junto con la consulta de usuario.

Para ver una consulta

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Queries and loads (Consultas y cargas) para mostrar la lista de consultas de la cuenta. Es posible que necesite cambiar los ajustes de esta página para encontrar su consulta.
3. Seleccione el identificador Query (Consulta) en la lista para mostrar los Query details (Detalles de la consulta).

   La página Query details (Detalles de la consulta) incluye las pestañas Query details (Detalles de la consulta) y Query plan (Plan de la consulta) con métricas sobre la consulta.

Las métricas incluyen detalles sobre una consulta, como la hora de inicio, el ID de consulta, el estado y la duración. Otros detalles incluyen si una consulta se ejecutó en un clúster principal o en un clúster de escalado de simultaneidad y si se trata de una consulta primaria o reescrita.

Análisis de ejecución de consulta

Para analizar una consulta

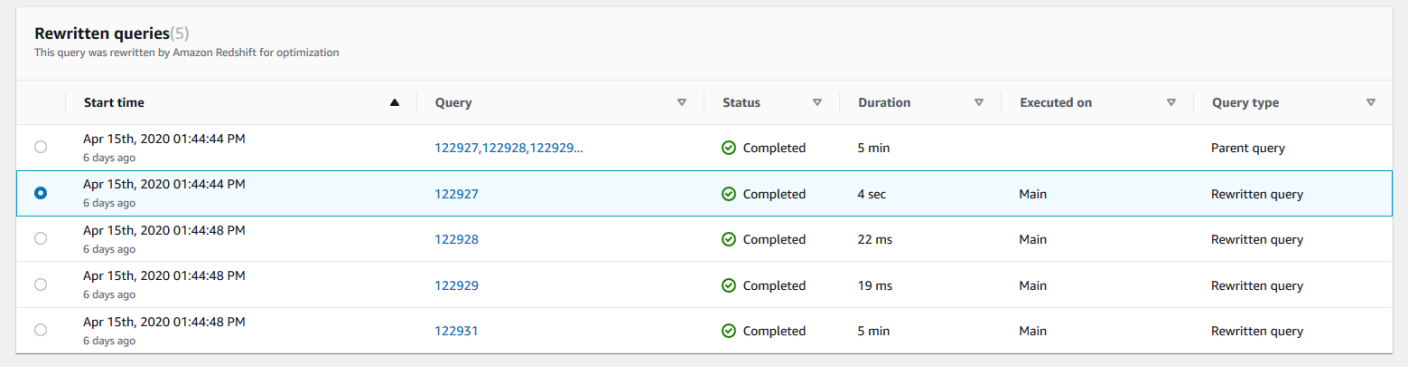
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Queries and loads (Consultas y cargas) para mostrar la lista de consultas de la cuenta. Es posible que necesite cambiar los ajustes de esta página para encontrar su consulta.
3. Seleccione el identificador Query (Consulta) en la lista para mostrar los Query details (Detalles de la consulta).

   La página Query details (Detalles de la consulta) incluye las pestañas Query details (Detalles de la consulta) y Query plan (Plan de la consulta) con métricas sobre la consulta.

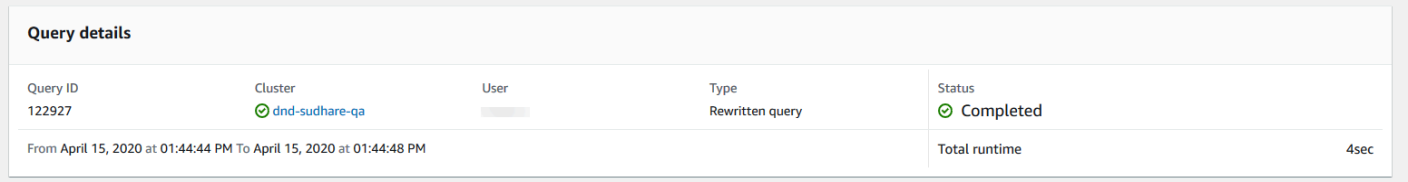
   > **Note**
   >
   > También puede desplazarse a la página Query details (Detalles de la consulta) desde una página Cluster details (Detalles del clúster), en la pestaña Query history (Historial de consultas) cuando navega en una consulta de un gráfico Query runtime (Tiempo de ejecución de consultas).

La página Detalles de la consulta contiene las siguientes secciones:

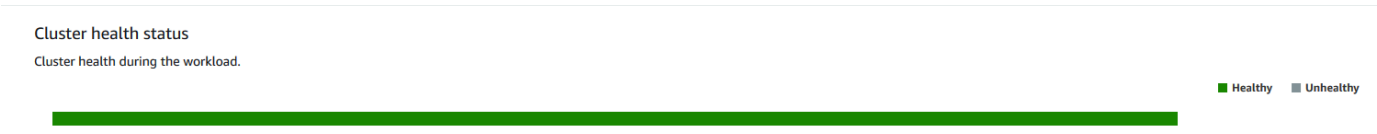
- Una lista de Consultas reescritas, como se muestra en la siguiente captura de pantalla.



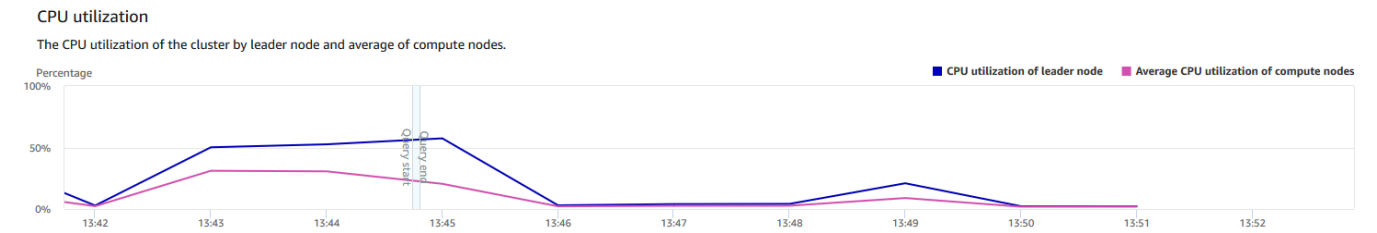
- Una sección de Detalles de la consulta, como se muestra en la siguiente captura de pantalla.



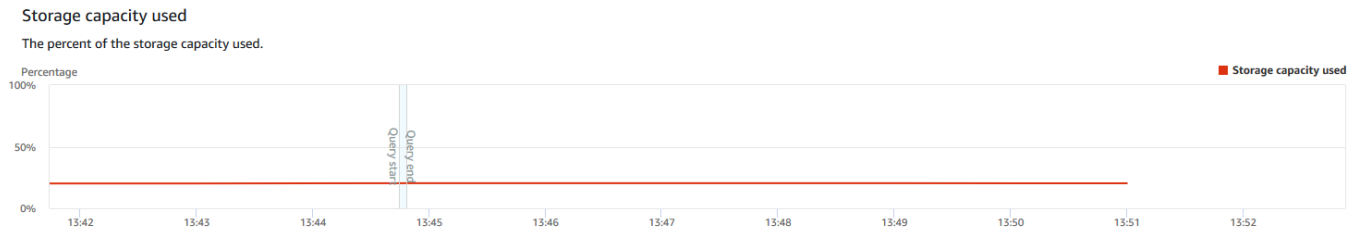
- Una pestaña Detalles de la consulta que contiene el SQL que se ejecutó y Detalles de ejecución sobre la ejecución.
- Una pestaña Plan de consulta que contiene los pasos del Plan de consulta y otra información sobre el plan de consulta. Esta tabla también contiene gráficos sobre el clúster cuando se ejecutó la consulta.
  - Estado del clúster



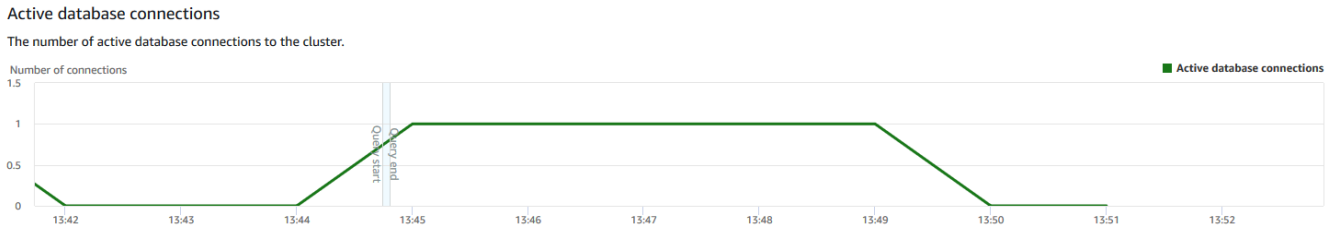
  - Utilización de la CPU



  - Capacidad de almacenamiento utilizada



- Conexiones de base de datos activas



Visualización del rendimiento del clúster durante la ejecución de consultas

Para mostrar el rendimiento del clúster durante la ejecución de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver más detalles.

   Para obtener más información, consulte Visualización de datos del historial de consultas.

Visualización de métricas de clúster durante las operaciones de carga

Cuando observa el rendimiento del clúster durante las operaciones de carga, puede identificar consultas que estén consumiendo recursos y tomar medidas para mitigar su efecto. Puede terminar una carga si no desea que se complete su ejecución.

> **Note**
>
> La capacidad para terminar consultas y cargas en la consola de Amazon Redshift requiere un permiso específico. Si desea que los usuarios puedan terminar consultas y cargas, asegúrese de añadir la acción `redshift:CancelQuerySession` a la política de AWS Identity and Access Management (IAM). Este requisito se puede aplicar tanto si selecciona la política administrada por AWSde solo lectura de Amazon Redshift como si crea una política personalizada en IAM. Los usuarios que tienen la política de acceso completo de Amazon Redshift ya cuentan con los permisos necesarios para terminar las consultas y las cargas. Para obtener más información acerca de las acciones de las políticas de IAM para Amazon Redshift, consulte Administrar el acceso a los recursos.

Para mostrar el rendimiento del clúster durante operaciones de carga

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver más detalles.
4. En la sección Queries and loads (Consultas y cargas), seleccione Loads (Cargas) para ver las operaciones de carga de un clúster. Si se está ejecutando una carga, puede terminarla seleccionando Terminate query (Terminar consulta).

Análisis del rendimiento de las cargas de trabajo

Puede obtener una vista detallada del rendimiento de las cargas de trabajo consultando el gráfico de desglose de ejecuciones de cargas de trabajo en la consola. El gráfico se crea con datos proporcionados por la métrica QueryRuntimeBreakdown. Con este gráfico, puede ver cuánto tiempo pasan las consultas en las distintas fases de procesamiento, como la espera y la planificación.

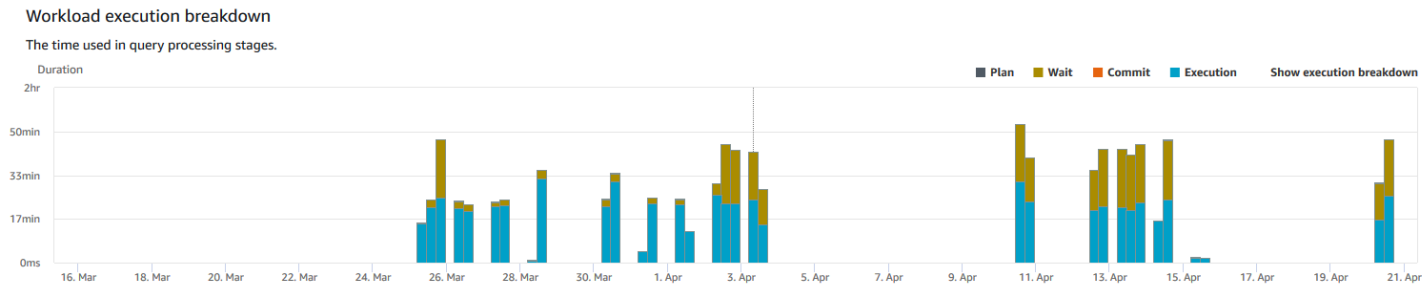
> **Note**
>
> El gráfico de desglose de ejecuciones de cargas de trabajo no se muestra para clústeres de un nodo.

En la siguiente lista de métricas, se describen las distintas fases de procesamiento:

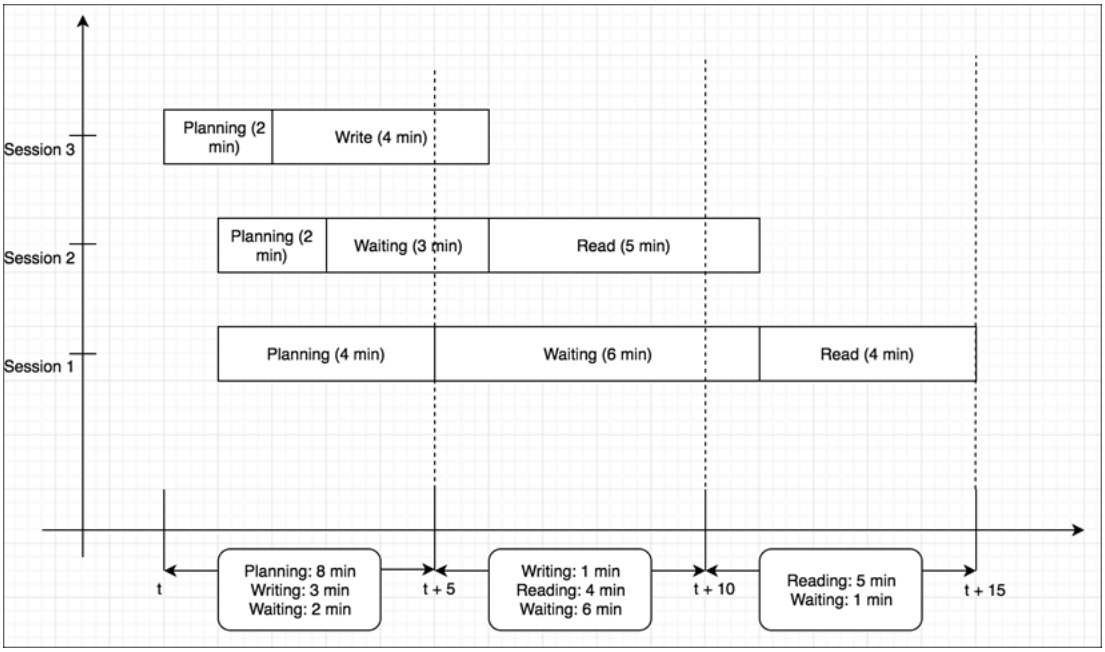
- `QueryPlanning`: tiempo invertido en analizar y optimizar instrucciones SQL.
- `QueryWaiting`: tiempo invertido en esperar en la cola de administración de carga de trabajo (WLM).
- `QueryExecutingRead`: tiempo invertido en ejecutar consultas de lectura.
- `QueryExecutingInsert`: tiempo invertido en ejecutar consultas de inserción.
- `QueryExecutingDelete`: tiempo invertido en ejecutar consultas de eliminación.
- `QueryExecutingUpdate`: tiempo invertido en ejecutar consultas de actualización.
- `QueryExecutingCtas`: tiempo invertido en ejecutar consultas CREATE TABLE AS.
- `QueryExecutingUnload`: tiempo invertido en ejecutar consultas de descarga.
- `QueryExecutingCopy`: tiempo invertido en ejecutar consultas de copia.

Por ejemplo, en el gráfico siguiente de la consola de Amazon Redshift, se muestra la cantidad de tiempo que las consultas han dedicado a las fases de planificación, espera, lectura y escritura. Puede combinar los resultados de este gráfico con otras métricas para ampliar el análisis. En algunos casos, el gráfico podría mostrar que las consultas con una duración corta (medida con la métrica `QueryDuration`) están esperando mucho tiempo en la fase de espera. En estos casos, puede aumentar la tasa de simultaneidad de WLM para una cola determinada con el fin de aumentar el rendimiento.

A continuación, se muestra un ejemplo del gráfico de desglose de la ejecución de la carga de trabajo. En el gráfico, el valor del eje Y es la duración media de cada etapa en el tiempo especificado que se muestra como gráfico de barras apiladas.



En el diagrama siguiente, se ilustra el modo en que Amazon Redshift. agrupa el procesamiento de consultas para las sesiones simultáneas.



Para mostrar el gráfico de desglose de la carga de trabajo del clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Clusters (Clústeres) y, a continuación, elija el nombre del clúster de la lista para abrir sus detalles. Se mostrarán los detalles del clúster, que pueden incluir las pestañas Cluster performance (Rendimiento del clúster), Query monitoring (Monitoreo de consultas), Databases (Bases de datos), Datashares (Recursos para compartir datos), Schedules (Programaciones), Maintenance (Mantenimiento) y Properties (Propiedades).
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.

4. En la sección Monitoreo de consultas, elija Rendimiento de la base de datos y elija Métricas del clúster.

   Las siguientes métricas muestran gráficos para el rango de tiempo seleccionado como un gráfico de barras apilado:

   - Tiempo de planificación
   - Tiempo de espera
   - Hora de confirmación
   - Hora de ejecución

Administración de alarmas

Las alarmas que crea en la consola de Amazon Redshift son alarmas de CloudWatch. Las alarmas son útiles porque le ayudan a tomar decisiones proactivas sobre el clúster o la instancia sin servidor. Puede establecer una o más alarmas en cualquiera de las métricas enumeradas en Monitoreo de Amazon Redshift mediante las métricas de CloudWatch. Por ejemplo, establecer una alarma para una `CPUUtilization` alta en un nodo del clúster ayuda a indicar los momentos en los que el nodo está sobrecargado. Una alarma para un valor de `DataStorage` alto mantendría un registro del espacio de almacenamiento que el espacio de nombres sin servidor utiliza para sus datos.

Desde Actions (Acciones), puede modificar o eliminar alarmas. También puede crear una alerta de Chime o Slack para enviar una alerta de CloudWatch a Slack o Amazon Chime especificando una URL de webhook de Slack o Amazon Chime.

En esta sección, se explica cómo crear una alarma mediante la consola de Amazon Redshift. Puede crear una alarma mediante la consola de CloudWatch o mediante cualquier otro mecanismo que utilice con las métricas, como con la AWS CLI o un AWS SDK.

Para crear una alarma de CloudWatch con la consola de Amazon Redshift.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.

   Si utiliza Amazon Redshift sin servidor, elija Go to Serverless (Ir a Sin servidor) en la parte superior derecha del panel.
2. En el menú de navegación, elija Alarms (Alarmas) y, a continuación, elija Create alarm (Crear alarma).

3. En la página Create alarm (Crear alarma), ingrese las propiedades para crear una alarma de CloudWatch.
4. Elija Crear alarma.

Uso de métricas de rendimiento en la consola de CloudWatch

Cuando trabaje con métricas de Amazon Redshift en la consola de CloudWatch, hay algunas cosas que debe tener en cuenta:

- Los datos de rendimiento de cargas y consultas están disponibles únicamente en la consola de Amazon Redshift.
- Algunas métricas de CloudWatch tienen unidades diferentes a las que se utilizan en la consola de Amazon Redshift. Por ejemplo, `WriteThroughput` se muestra en GB/s (mientras que en CloudWatch lo hace en bytes/s), que es una unidad más pertinente para el espacio de almacenamiento normal de un nodo.

Cuando trabaje con métricas de Amazon Redshift en la consola de CloudWatch, las herramientas de línea de comandos o un Amazon SDK, tenga en cuenta estos conceptos:

1. Primero, especifique la dimensión de la métrica con la que va a trabajar. Una dimensión es un par de nombre-valor que le ayuda a identificar una métrica de forma inequívoca. Las dimensiones de Amazon Redshift son `ClusterIdentifier` y `NodeID`. En la consola de CloudWatch, se proporcionan las vistas `Redshift Cluster` y `Redshift Node` para que pueda seleccionar fácilmente dimensiones específicas de nodos y clústeres. Para obtener más información acerca de las dimensiones, consulte Dimensiones en la Guía para desarrolladores de CloudWatch.
2. Luego, especifique el nombre de métrica, como `ReadIOPS`.

En la tabla siguiente, se resumen los tipos de dimensiones de métricas de Amazon Redshift que están disponibles para usted. En función de la métrica, los datos estarán disponibles en intervalos de 1 minuto o de 5 minutos sin ningún cargo adicional. Para obtener más información, consulte Métricas de Amazon Redshift.

Espacio de nombres de CloudWatch	Dimensión	Descripción
AWS/Redshift	NodeID	Filtra los datos solicitados que son específicos de los nodos de un clúster. NodeID puede ser "Leader (Principal)", "Shared (Compartido)", o "Compute-N (N-computación)", donde N puede ser 0, 1, etc. en función del número de nodos del clúster. "Shared" significa que el clúster tiene un solo nodo, es decir, que el nodo principal y el nodo de computación están combinados.
	ClusterIdentifier	Filtra los datos solicitados que son específicos del clúster. Las métricas específicas del clúster son HealthStatus , MaintenanceMode y DatabaseConnections . Las métricas generales de esta dimensión (por ejemplo, ReadIOPS), que también son métricas de nodos, representan el total acumulado de datos de métricas de nodos. Preste especial atención cuando interprete estas métricas, ya que incluyen el comportamiento acumulado tanto del nodo principal como de los nodos de computación.

Trabajar con métricas de gateway y de volumen es similar a trabajar con otras métricas de servicio. Muchas de las tareas comunes se describen en la documentación de CloudWatch, incluidas las siguientes:

- Ver métricas disponibles
- Obtener estadísticas de una métrica
- Creación de alarmas de CloudWatch

Eventos de Amazon Redshift

Temas

- Información general de eventos de clúster
- Uso de Amazon Simple Notification Service
- Suscripción a notificaciones de eventos de clúster de Amazon Redshift
- Visualización de eventos de clúster mediante la consola
- Visualización de eventos de clúster mediante la AWS CLI y la API de Amazon Redshift
- Administración de las notificaciones de eventos de clúster
- Notificaciones de eventos de Amazon Redshift
- Notificaciones de eventos de Amazon Redshift sin servidor con Amazon EventBridge
- Notificaciones de eventos de integración sin ETL con Amazon EventBridge

Información general de eventos de clúster

Amazon Redshift realiza un seguimiento de los eventos de clúster y retiene información sobre ellos durante varias semanas en su cuenta de AWS. Amazon Redshift brinda información sobre cada evento, como la fecha en la que se produjo, una descripción de él, su fuente (por ejemplo, un clúster, un grupo de parámetros o una instantánea) y el ID de la fuente.

Amazon Redshift proporciona una notificación con antelación para algunos eventos. Estos eventos tienen una categoría de evento de `pending`. Por ejemplo, enviamos una notificación con antelación si se requiere una actualización de hardware para alguno de los nodos de su clúster. Puede suscribirse a los eventos pendientes de la misma forma que a otros eventos de Amazon Redshift. Para obtener más información, consulte Suscripción a notificaciones de eventos de clúster de Amazon Redshift.

Puede utilizar la consola de administración de Amazon Redshift, la API de Amazon Redshift o el AWS SDK para obtener información de los eventos. Puede obtener una lista de todos los eventos o aplicar filtros, como duración del evento o fecha de comienzo y finalización, para obtener la información de eventos en un período específico.

También puede obtener eventos generados por un tipo de origen específico, como eventos de clúster o de grupo de parámetros. La columna Source (Fuente) muestra el nombre de recurso y el tipo de recurso que desencadena una acción determinada.

Puede crear suscripciones de notificaciones de eventos de Amazon Redshift que especifiquen un conjunto de filtros de eventos. Cuando un evento coincide con los criterios de filtro, Amazon Redshift usa Amazon Simple Notification Service para informarle activamente que se ha producido el evento.

Para ver una lista de los eventos de Amazon Redshift por categoría y tipo de fuente, consulte the section called “Categorías y mensajes de eventos de Amazon Redshift”.

Uso de Amazon Simple Notification Service

Amazon Redshift utiliza Amazon Simple Notification Service (Amazon SNS) para comunicar notificaciones de eventos de Amazon Redshift. Habilita las notificaciones mediante la creación de una suscripción a eventos de Amazon Redshift. En la suscripción de Amazon Redshift, especifica un conjunto de filtros para los eventos de Amazon Redshift y un tema de Amazon SNS. Siempre que se produce un evento que coincide con los criterios de filtrado, Amazon Redshift publica un mensaje de notificación en el tema de Amazon SNS. Luego, Amazon SNS transmite el mensaje a cualquier consumidor de Amazon SNS que tenga una suscripción de Amazon SNS al tema. Los mensajes que se envían a los consumidores de Amazon SNS pueden estar en cualquier formato que Amazon SNS admita en una región de AWS, como un email, un mensaje de texto o una llamada a un punto de conexión HTTP. Por ejemplo, todas las regiones admiten notificaciones por correo electrónico, pero las notificaciones por SMS solo pueden crearse en la región Este de EE. UU. (Norte de Virginia).

> **Note**
>
> Actualmente, solo puede crear una suscripción a eventos a un tema estándar de Amazon SNS (no a un tema FIFO de Amazon SNS). Para obtener más información, consulte Fuentes de eventos de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Cuando crea una suscripción a notificaciones de eventos, debe especificar uno o más filtros de eventos. Amazon Redshift envía notificaciones a través de la suscripción cada vez que se produzca un evento que coincida con todos los criterios de filtrado. Los criterios de filtro incluyen el tipo de origen (como un clúster o una snapshot), el ID de origen (como el nombre de un clúster o de una snapshot), la categoría del evento (como supervisión o seguridad) y la gravedad del evento (como INFO o ERROR).

Puede desactivar las notificaciones fácilmente y sin eliminar una suscripción mediante la configuración del botón de opción Enabled (Habilitado) en No en la AWS Management Console

o mediante la configuración del parámetro `Enabled` en `false` a través de la API o la CLI de Amazon Redshift.

La facturación de la notificación de eventos de Amazon Redshift se efectúa a través de Amazon Simple Notification Service (Amazon SNS). Cuando se utiliza la notificación de eventos, se aplican tarifas de Amazon SNS. Para obtener más información acerca de la facturación de Amazon SNS, consulte Precios de Amazon Simple Notification Service.

También puede ver los eventos de Amazon Redshift que hayan ocurrido a través de la consola de administración. Para obtener más información, consulte Eventos de Amazon Redshift.

Suscripción a notificaciones de eventos de clúster de Amazon Redshift

Puede crear una suscripción a notificaciones de eventos de Amazon Redshift para recibir notificaciones cada vez que se produzca un evento en un clúster, una instantánea, un grupo de seguridad o un grupo de parámetros determinados. La forma más sencilla de crear una suscripción es a través de la consola de Amazon SNS. Para obtener información sobre cómo crear un tema de Amazon SNS y suscribirse a él, consulte Introducción a Amazon SNS.

Puede crear una suscripción a notificaciones de eventos de Amazon Redshift para recibir notificaciones cada vez que se produzca un evento en un clúster, una instantánea, un grupo de seguridad o un grupo de parámetros determinados. La forma más sencilla de crear una suscripción es con la AWS Management Console. Si decide crear las suscripciones de notificaciones de eventos a través de la CLI o la API, debe crear un tema de Amazon Simple Notification Service y suscribirse a dicho tema con la consola de Amazon SNS o la API de Amazon SNS. También deberá conservar el Nombre de recurso de Amazon (ARN) del tema, ya que este se utiliza al enviar los comandos de la CLI o las acciones de la API. Para obtener información sobre cómo crear un tema de Amazon SNS y suscribirse a él, consulte Introducción a Amazon SNS.

En una suscripción a un evento de Amazon Redshift, se pueden especificar los siguientes criterios para el evento:

- Para el tipo de origen, los valores son clúster, snapshot, grupos de parámetros y grupos de seguridad.
- El ID de origen de un recurso como `my-cluster-1` o `my-snapshot-20130823`. El ID debe corresponder a un recurso en la misma región de AWS que la suscripción a eventos.

- Para la categoría del evento, los valores son configuración, administración, supervisión, seguridad y pendiente.
- Para la gravedad del evento, los valores son INFO o ERROR.

Los criterios de evento pueden especificarse de manera independiente, con la excepción de que debe especificar un tipo de origen antes de poder especificar los ID de origen en la consola. Por ejemplo, puede especificar una categoría de evento sin tener que especificar un tipo de origen, un ID de origen o la gravedad. Si bien puede especificar el ID de origen para recursos que no son del tipo especificado en el tipo de origen, no se enviarán notificaciones para eventos desde esos recursos. Por ejemplo, si especifica un tipo de origen de un clúster y el ID de un grupo de seguridad, ninguno de los eventos suscitados por ese grupo de seguridad coincidirá con los criterios del filtro del tipo de origen, por lo que no se enviarán notificaciones para esos eventos.

Amazon Redshift envía una notificación cada vez que hay un evento que coincide con todos los criterios especificados en una suscripción. Algunos ejemplos de los conjuntos de eventos que se devuelven son:

- La suscripción especifica un tipo de origen de un clúster, un ID de origen de my-cluster-1, una categoría de supervisión y una gravedad ERROR. La suscripción enviará notificaciones solo para los eventos de supervisión con una gravedad ERROR desde my-cluster-1.
- La suscripción especifica un tipo de origen de un clúster, una categoría de configuración y una gravedad INFO. La suscripción enviará notificaciones por los eventos de configuración con la severidad INFO desde cualquier clúster de Amazon Redshift en la cuenta de AWS.
- La suscripción especifica una categoría de configuración y una gravedad INFO. La suscripción enviará notificaciones por los eventos de configuración con la severidad INFO desde cualquier recurso de Amazon Redshift en la cuenta de AWS.
- La suscripción especifica una gravedad ERROR. La suscripción enviará notificaciones por todos los eventos con la severidad ERROR desde cualquier recurso de Amazon Redshift en la cuenta de AWS.

Si elimina o cambia el nombre de un objeto al que se hace referencia como ID de origen en una suscripción existente, la suscripción permanecerá activa, pero no habrá eventos para reenviar desde ese objeto. Si luego crea un objeto nuevo con el mismo nombre al que se hace referencia en la suscripción como ID de origen, la suscripción comenzará a enviar notificaciones de eventos desde ese nuevo objeto.

Amazon Redshift publica notificaciones de eventos en un tema de Amazon SNS, que se identifica por su nombre de recurso de Amazon (ARN). Cuando crea una subscripción a eventos con la consola de Amazon Redshift, puede especificar un tema de Amazon SNS existente o solicitar que la consola cree el tema cuando genere la suscripción. Todas las notificaciones de eventos de Amazon Redshift enviadas al tema de Amazon SNS se transmiten, a su vez, a todos los consumidores de Amazon SNS que estén suscritos a ese tema. Utilice la consola de Amazon SNS para realizar cambios en el tema de Amazon SNS, como agregar suscripciones al tema de los consumidores o quitarlas. Para obtener información sobre cómo crear temas de Amazon SNS y suscribirse a ellos, consulte Introducción a Amazon Simple Notification Service.

En las siguientes secciones, se enumeran todas las categorías y eventos de los que puede recibir notificaciones. Además, se proporciona información sobre cómo suscribirse a los eventos de Amazon Redshift y cómo trabajar con esas suscripciones.

Visualización de eventos de clúster mediante la consola

Para ver eventos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Events (Eventos).

Visualización de eventos de clúster mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar la siguiente operación de la CLI de Amazon Redshift para ver los eventos.

- describe-events

Amazon Redshift proporciona la API siguiente para visualizar los eventos.

- DescribeEvents

Administración de las notificaciones de eventos de clúster

Puede crear una suscripción a notificaciones de eventos de Amazon Simple Notification Service (Amazon SNS) para enviar notificaciones cada vez que se produzca un evento en determinado clúster, instantánea, grupo de seguridad o grupo de parámetros de Amazon Redshift. Estas notificaciones se envían a un tema de SNS, que a su vez, transmite mensajes a todos los consumidores de SNS que están suscritos al tema. Los mensajes de SNS que reciben los consumidores pueden estar en cualquier formato de notificación que Amazon SNS admita para una región de AWS, como un email, un mensaje de texto o una llamada a un punto de conexión HTTP. Por ejemplo, todas las regiones admiten notificaciones por email, pero las notificaciones por SMS solo se pueden crear en la región EE. UU. Este (Norte de Virginia). Para obtener más información, consulte Notificaciones de eventos de Amazon Redshift.

Administración de las notificaciones de eventos de clúster con la consola de Amazon Redshift

Creación de una suscripción a la notificación de eventos

Para crear una suscripción de evento

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Events (Eventos).
3. Elija la pestaña Event Subscriptions (Suscripciones de eventos) y, a continuación, elija Create event subscriptions (Crear suscripciones de eventos).
4. Introduzca las propiedades de su suscripción de evento, como nombre, tipo de fuente, categoría y gravedad. También puede habilitar temas de Amazon SNS para recibir notificaciones de eventos.
5. Haga clic en Create event subscriptions (Crear suscripciones de eventos) para crear su suscripción.

Administración de notificaciones de eventos de clúster con la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar las notificaciones de eventos de clúster.

- create-event-subscription
- delete-event-subscription
- describe-event-categories
- describe-event-subscriptions
- describe-events
- modify-event-subscription

Puede utilizar las siguientes acciones de la API de Amazon Redshift para administrar las notificaciones de eventos.

- CreateEventSubscription
- DeleteEventSubscription
- DescribeEventCategories
- DescribeEventSubscriptions
- DescribeEvents
- ModifyEventSubscription

Para obtener más información acerca de las notificaciones de eventos de Amazon Redshift, consulte Notificaciones de eventos de Amazon Redshift.

Notificaciones de eventos de Amazon Redshift

Categorías y mensajes de eventos de Amazon Redshift

En esta sección, se muestran los ID de eventos y las categorías para cada tipo de origen de Amazon Redshift.

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un clúster como tipo de origen.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1000	INFO	El grupo de parámetros [nombre del grupo de parámetros] se actualizó a las [hora]. Si solo cambió parámetros dinámicos, los clústeres asociados se modificarán ahora. Si cambió parámetros estáticos, todas las actualizaciones, incluidos los parámetros dinámicos, se aplicarán cuando reinicie los clústeres asociados.
Configuración	REDSHIFT-EVENT-1001	INFO	Se modificó el clúster [nombre del clúster] de Amazon Redshift para utilizar el grupo de parámetros [nombre del grupo de parámetros] a la(s) [hora].
Configuración	REDSHIFT-EVENT-1500	ERROR	La VPC [nombre de la VPC] de Amazon VPC no existe. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Configuración	REDSHIFT-EVENT-1501	ERROR	Las subredes del cliente [nombre de la subred] que especificó para [nombre de la VPC] de Amazon VPC no existen o no son válidas. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Configuración	REDSHIFT-EVENT-1502	ERROR	Subredes en un grupo de subredes de clúster [nombre de grupo de subredes] no tienen direcciones IP disponibles. No se pudo crear el clúster [nombre de clúster].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1503	ERROR	La VPC [nombre de la VPC] de Amazon VPC no tiene una gateway de Internet adjunta. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Configuración	REDSHIFT-EVENT-1504	ERROR	No se puede tener acceso al HSM para el clúster [nombre del clúster].
Configuración	REDSHIFT-EVENT-1505	ERROR	No se puede registrar el HSM para el clúster [nombre del clúster]. Pruebe con una configuración diferente.
Configuración	REDSHIFT-EVENT-1506	ERROR	Amazon Redshift superó el límite de interfaz de red elástica de su cuenta. Elimine hasta [número máximo de interfaces de red elásticas] interfaces de red elásticas o solicite un aumento de límite del número de interfaces de red por región de AWS con EC2.
Configuración	REDSHIFT-EVENT-1509	ERROR	No se puede crear el clúster [nombre del clúster] de Amazon Redshift porque se ha alcanzado el límite del punto de conexión de la VPC de su cuenta. Elimine los puntos de enlace de la VPC no utilizados o solicite un aumento en el límite de los puntos de enlace de la VPC. Para obtener más información, consulte Puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1510	ERROR	Hemos detectado que el intento de cargar datos de ejemplo en el clúster de Amazon Redshift [nombre del clúster] no se ha realizado correctamente. Para cargar datos de ejemplo, configure primero la VPC con objeto de que tenga acceso a los buckets de Amazon S3 y, a continuación, cree un clúster y cargue datos de ejemplo. Para obtener más información, consulte Habilitación del enrutamiento de VPC mejorado en la Guía de administración de Amazon Redshift.
Configuración	REDSHIFT-EVENT-1511	ERROR	No se puede crear el clúster [nombre del clúster] de Amazon Redshift porque se superó el límite de direcciones IP elásticas de la cuenta. Elimine las direcciones IP elásticas no utilizadas o solicite un aumento del límite a Amazon EC2.
Administración	REDSHIFT-EVENT-2000	INFO	Se ha creado el clúster [nombre del clúster] de Amazon Redshift y está listo para utilizarse.
Administración	REDSHIFT-EVENT-2001	INFO	Se eliminó el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora]. [Se guardó/no se guardó] una snapshot final.
Administración	REDSHIFT-EVENT-2002	INFO	Grupos de seguridad de la VPC para el clúster [nombre del clúster] actualizados a las [hora en UTC].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2003	INFO	Comenzaron las tareas de mantenimiento en su clúster [nombre del clúster] de a las [hora en UTC].
Administración	REDSHIFT-EVENT-2004	INFO	Se terminaron las tareas de mantenimiento en su clúster [nombre del clúster] de a las [hora en UTC].
Administración	REDSHIFT-EVENT-2006	INFO	Comenzó el cambio de tamaño del clúster [nombre del clúster] a las [hora en UTC]. El clúster está en modo de solo lectura.
Administración	REDSHIFT-EVENT-2007	INFO	Se ha confirmado una solicitud para cambiar tamaño del clúster [nombre del clúster].
Administración	REDSHIFT-EVENT-2008	INFO	Se inició una operación de restauración para crear la instantánea nueva [nombre de la instantánea] del clúster [nombre del clúster] de Amazon Redshift a la(s) [hora]. Para supervisar el progreso de la restauración, revise la AWS Management Console.
Administración	REDSHIFT-EVENT-2013	INFO	Se cambió el nombre del clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Administración	REDSHIFT-EVENT-2014	INFO	Se recibió una solicitud para restaurar una tabla para el clúster [nombre del clúster] de Amazon Redshift.
Administración	REDSHIFT-EVENT-2015	INFO	Se canceló la restauración de la tabla para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Administración	REDSHIFT-EVENT-2016	INFO	Se inició el reemplazo del clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2017	INFO	Mantenimiento iniciado por el cliente comenzado en el clúster de Amazon Redshift [nombre del clúster] a las [hora]. Es posible que el clúster no esté disponible durante las tareas de mantenimiento.
Administración	REDSHIFT-EVENT-2018	INFO	Mantenimiento iniciado por el cliente completado en el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Administración	REDSHIFT-EVENT-2019	ERROR	Error del mantenimiento iniciado por el cliente en el clúster de Amazon Redshift [nombre del clúster] a las [hora]. Devolviendo el clúster a su estado original.
Administración	REDSHIFT-EVENT-2020	INFO	Se ha modificado la pista del clúster de Amazon Redshift [nombre del clúster] de [de pista] a [a pista].
Administración	REDSHIFT-EVENT-2021	ERROR	La [operación] del clúster [nombre del clúster] de Amazon Redshift no se realizó correctamente mientras adquiría capacidad de nuestro grupo de capacidad. Estamos trabajando para adquirir capacidad, pero por el momento hemos cancelado su solicitud. Elimine este clúster y vuelva a intentarlo más adelante.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2022	ERROR	La [operación] del clúster [nombre del clúster] de Amazon Redshift no se realizó correctamente mientras adquiría capacidad de nuestro grupo de capacidad. Estamos trabajando para adquirir capacidad, pero por el momento hemos cancelado su solicitud. La capacidad está disponible en [zonas de disponibilidad alternativas]. Elimine este clúster y pruebe de nuevo en una zona de disponibilidad alternativa.
Administración	REDSHIFT-EVENT-2023	ERROR	Hemos detectado un error de hardware en el clúster de Amazon Redshift con un único nodo [nombre del clúster], que puede haber producido errores en las consultas o intermitencias en la disponibilidad del clúster. El clúster no se reemplazó correctamente mientras se adquiría capacidad de nuestro grupo de capacidad. Tiene que restaurar un nuevo clúster a partir de una instantánea. Elimine este clúster, seleccione la última instantánea disponible y restaure un nuevo clúster a partir de la instantánea. De este modo, dispondrá automáticamente de un hardware en buen estado.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2024	ERROR	Hemos detectado un error de hardware en el clúster de Amazon Redshift con un único nodo [nombre del clúster], que puede haber producido errores en las consultas o intermitencias en la disponibilidad del clúster. El clúster no se reemplazó correctamente mientras se adquiría capacidad de nuestro grupo de capacidad. La capacidad está disponible en la zona de disponibilidad: [zonas de disponibilidad alternativas]. Elimine este clúster, seleccione la última instantánea disponible y restaure un nuevo clúster a partir de la instantánea. De este modo, dispondrá automáticamente de un hardware en buen estado.
Administración	REDSHIFT-EVENT-3011	INFO	Se inició el cambio de tamaño elástico del clúster “[nombre del clúster]” de Amazon Redshift a la(s) [hora]. Durante el cambio de tamaño, se retendrán las conexiones de las bases de datos. Durante esta operación, es posible que algunas consultas y conexiones terminen o agoten el tiempo de espera.
Administración	REDSHIFT-EVENT-3012	INFO	Se recibió una solicitud de cambio de tamaño elástico para el clúster '[nombre del clúster]' iniciado a las [hora]. Le proporcionaremos una notificación de evento cuando comience el cambio de tamaño.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Pendiente	REDSHIFT-EVENT-2025	INFO	La base de datos para el clúster <nombre de clúster> se actualizará entre las <hora de inicio> y las <hora de finalización>. No será posible obtener acceso al clúster. Planifíquelo en consecuencia.
Pendiente	REDSHIFT-EVENT-2026	INFO	El clúster <nombre de clúster> se actualizará entre las <hora de inicio> y las <hora de finalización>. No será posible obtener acceso al clúster. Planifíquelo en consecuencia.
Supervisión	REDSHIFT-EVENT-2050	INFO	Se detectó un problema de hardware en el clúster [nombre del clúster] de Amazon Redshift. Se inició una solicitud de reemplazo a las [hora].
Supervisión	REDSHIFT-EVENT-3000	INFO	Se reinició el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3001	INFO	Se reemplazó de forma automática un nodo del clúster [nombre del clúster] de Amazon Redshift a la(s) [hora] y el clúster está funcionando con normalidad.
Supervisión	REDSHIFT-EVENT-3002	INFO	Se completó el cambio de tamaño del clúster [nombre del clúster] de Amazon Redshift que está disponible para lecturas y escrituras. El cambio de tamaño se inició a las [hora] y tardó [horas] horas en completarse.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Supervisión	REDSHIFT-EVENT-3003	INFO	Se creó correctamente el clúster [nombre del clúster] de Amazon Redshift a partir de la instantánea [nombre de la instantánea] y está disponible para su uso.
Supervisión	REDSHIFT-EVENT-3007	INFO	Se copió correctamente la instantán ea [nombre de la instantánea] de Amazon Redshift de [región de AWS de origen] a [región de AWS de destino] a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3008	INFO	La restauración de la tabla para el clúster [nombre del clúster] de Amazon Redshift comenzó a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3009	INFO	Se completó correctamente la restauración de la tabla para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3010	ERROR	Se produjo un error en la restauración de la tabla para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3013	ERROR	Se produjo un error en la operación solicitada de cambio de tamaño elástico para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora] debido a [motivo].
Supervisión	REDSHIFT-EVENT-3014	INFO	Se reinició el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Supervisión	REDSHIFT-EVENT-3500	ERROR	Se produjo un error en el cambio de tamaño para el clúster [nombre del clúster] de Amazon Redshift. El cambio de tamaño se volverá a ejecutar automáticamente en unos minutos.
Supervisión	REDSHIFT-EVENT-3501	ERROR	Se produjo un error en la operación de restauración para crear el clúster [nombre del clúster] de Amazon Redshift a partir de la instantánea [nombre de la instantánea] a la(s) [hora]. Vuelva a realizar la operación.
Supervisión	REDSHIFT-EVENT-3504	ERROR	El bucket [nombre del bucket] de Amazon S3 no es válido para el registro del clúster [nombre del clúster].
Supervisión	REDSHIFT-EVENT-3505	ERROR	El bucket [nombre del bucket] de Amazon S3 no tiene las políticas de IAM correctas para el clúster [nombre del clúster].
Supervisión	REDSHIFT-EVENT-3506	ERROR	El bucket [nombre del bucket] de Amazon S3 no existe. No se puede continuar con el registro del clúster [nombre del clúster].
Supervisión	REDSHIFT-EVENT-3507	ERROR	No se puede crear el clúster [nombre del clúster] de Amazon Redshift con la EIP [dirección IP]. Esta EIP ya está en uso.
Supervisión	REDSHIFT-EVENT-3508	ERROR	No se puede crear el clúster [nombre del clúster] de Amazon Redshift con la EIP [dirección IP]. No se ha encontrado la EIP.
Supervisión	REDSHIFT-EVENT-3509	ERROR	La copia de snapshot no está habilitada entre regiones para el clúster [nombre del clúster].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Supervisión	REDSHIFT-EVENT-3510	ERROR	Se produjo un error en el inicio de la restauración de la tabla para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora]. Motivo: [motivo].
Supervisión	REDSHIFT-EVENT-3511	ERROR	Se produjo un error en la restauración de la tabla para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3512	ERROR	Se produjo un error en el clúster [nombre del clúster] de Amazon Redshift por un problema de hardware. El clúster se está restaurando automáticamente desde la última snapshot [nombre de la snapshot] creada a las [hora].
Supervisión	REDSHIFT-EVENT-3513	ERROR	Se produjo un error en el clúster [nombre del clúster] de Amazon Redshift por un problema de hardware. El clúster se está restaurando automáticamente desde la última snapshot [nombre de la snapshot] creada a las [hora]. Se deberá volver e enviar cualquier cambio en la base de datos que se haya realizado después de esta hora.
Supervisión	REDSHIFT-EVENT-3514	ERROR	Se produjo un error en el clúster [nombre del clúster] de Amazon Redshift por un problema de hardware. El clúster se pondrá en estado de error de hardware. Elimine y restaure el clúster desde la última snapshot [nombre de la snapshot] creada a las [hora].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Supervisión	REDSHIFT-EVENT-3515	ERROR	Se produjo un error en el clúster [nombre del clúster] de Amazon Redshift por un problema de hardware. El clúster se pondrá en estado de error de hardware. Elimine y restaure el clúster desde la última snapshot [nombre de la snapshot] creada a las [hora]. Se deberá volver e enviar cualquier cambio en la base de datos que se haya realizado después de esta hora.
Supervisión	REDSHIFT-EVENT-3516	ERROR	Se produjo un error en el clúster [nombre del clúster] de Amazon Redshift debido a un problema de hardware y no hay copias de seguridad del clúster. El clúster se pondrá en estado de error de hardware y se puede eliminar.
Supervisión	REDSHIFT-EVENT-3519	INFO	El clúster comenzó a reiniciarse [nombre del clúster] a las [hora].
Supervisión	REDSHIFT-EVENT-3520	INFO	Se terminó de reiniciar el clúster [nombre del clúster] a las [hora].
Supervisión	REDSHIFT-EVENT-3521	INFO	Detectamos un problema de conectividad en el clúster '[nombre del clúster]'. Se inició un control diagnóstico automatizado a las [hora].
Supervisión	REDSHIFT-EVENT-3522	INFO	Se produjo un error en la acción de recuperación del clúster '[nombre del clúster]' a las [hora]. El equipo de Amazon Redshift está buscando una solución.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Supervisión	REDSHIFT-EVENT-3533	ERROR	Se canceló el cambio de tamaño del clúster '[nombre del clúster]' a las [hora]. La operación se canceló porque [motivo]. [acción necesaria].
Supervisión	REDSHIFT-EVENT-3534	INFO	Se completó el cambio de tamaño elástico para el clúster “[nombre del clúster]” de Amazon Redshift a la(s) [hora]. El clúster está ahora disponible para operaciones de lectura y escritura mientras se realiza la transferencia de datos. Es posible que algunas consultas tarden más tiempo hasta que se complete la transferencia de datos.
Supervisión	REDSHIFT-EVENT-3537	INFO	Se completó la transferencia de datos del clúster “[nombre del clúster]” a la(s) [hora en UTC].
Supervisión	REDSHIFT-EVENT-3600	INFO	La operación de cambio de tamaño solicitad a para el clúster '[nombre del clúster]' de Amazon Redshift se canceló anteriormente. La reversión se completó a las [hora].
Pendiente	REDSHIFT-EVENT-3601	INFO	Un nodo del clúster <nombre de clúster> se sustituirá entre las <hora de inicio> y las <hora de finalización>. No puede posponer este mantenimiento. Planifíquelo en consecuencia.
Pendiente	REDSHIFT-EVENT-3602	INFO	La sustitución de un nodo del clúster <nombre de clúster> está programada entre las <hora de inicio> y las <hora de finalización>. No será posible obtener acceso al clúster. Planifíquelo en consecuencia.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-3603	INFO	La operación de restauración para crear el clúster [nombre del clúster] a partir de la instantánea [nombre de la instantánea] produjo un error interno. El clúster se pondrá en estado de restauración incompatible y se puede eliminar. Intente restaurar la instantánea en un clúster con otra configuración.
Administración	REDSHIFT-EVENT-3614	INFO	La acción programada [nombre de acción programada] se creó a las [hora en UTC]. La primera invocación está programada a las [hora en UTC].
Administración	REDSHIFT-EVENT-3615	INFO	La acción programada [nombre de acción programada] está programada a las [hora en UTC].
Supervisión	REDSHIFT-EVENT-3616	INFO	La acción programada [nombre de la acción programada] a las [hora en UTC] finalizó con el estado "SUCCEEDED".
Supervisión	REDSHIFT-EVENT-3617	ERROR	La acción programada [nombre de acción programada] se omitió a las [hora en UTC] debido a un retraso.
Supervisión	REDSHIFT-EVENT-3618	INFO	Se inició la operación de pausa del clúster [nombre del clúster] a la(s) [hora en UTC]. Pausa iniciada
Supervisión	REDSHIFT-EVENT-3619	INFO	Se pausó correctamente el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora UTC].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-3626	INFO	La acción programada [nombre de acción programada] se modificó a las [hora en UTC]. La primera invocación está programada a las [hora en UTC].
Administración	REDSHIFT-EVENT-3627	INFO	La acción programada [nombre de acción programada] se eliminó a las [hora en UTC].
Supervisión	REDSHIFT-EVENT-3628	ERROR	La acción programada [nombre de acción programada] a las [hora en UTC] finalizó con el estado "FAILED".
Administración	REDSHIFT-EVENT-3629	INFO	El clúster [nombre del clúster] de Amazon Redshift ha recibido su solicitud de reubicación. Cuando se completa la reubicación de la zona de disponibilidad, Amazon Redshift envía una notificación de evento.
Administración	REDSHIFT-EVENT-3630	INFO	El clúster [nombre del clúster] de Amazon Redshift se reubicó correctamente de [zona de disponibilidad] a [zona de disponibilidad]. Ya puede utilizar el clúster.
Administración	REDSHIFT-EVENT-3631	INFO	Amazon Redshift reubicó correctamente el clúster [nombre del clúster] de Amazon Redshift de [zona de disponibilidad] a [zona de disponibilidad] para recuperarlo.
Administración	REDSHIFT-EVENT-3632	INFO	Amazon Redshift desactivó de forma temporal la reubicación de clústeres para el clúster [nombre del clúster] de Amazon Redshift debido a cambios en la configuración. Intente reubicar el clúster otra vez más tarde.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Monitoreo	REDSHIFT-EVENT-3658	ERROR	Error de la migración de EC2-Classic a EC2-VPC para el clúster de Redshift [id del clúster].
Supervisión	REDSHIFT-EVENT-3659	INFO	Migración de EC2-Classic a EC2-VPC exitosa para el clúster de Redshift [id del clúster].
Supervisión	REDSHIFT-EVENT-3660	INFO	El clúster se pondrá en estado de error de hardware. Elimine el clúster EC2-Classic y restaure a un clúster EC2-VPC desde la última instantánea [nombre de la instantánea] creada a las [hora en UTC].
Administración	REDSHIFT-EVENT-3666	INFO	El clúster multi-AZ [nombre del clúster] de Amazon Redshift detectó un error a las [hora en UTC] y activó una recuperación automática.
Administración	REDSHIFT-EVENT-3667	INFO	El clúster multi-AZ [nombre del clúster] de Amazon Redshift se recuperó correctamente a las [hora en UTC] y está disponible para su uso en [primera zona de disponibilidad]. Habrá disponibles recursos de computación secundarios en otra zona de disponibilidad en breve.
Monitoreo	REDSHIFT-EVENT-3668	ERROR	El clúster multi-AZ [nombre del clúster] de Amazon Redshift no se pudo recuperar a las [hora en UTC].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-3669	INFO	El clúster multi-AZ [nombre del clúster] de Amazon Redshift se recuperó correctamente a las [hora en UTC] y está disponible para su uso con recursos de computación de [primera zona de disponibilidad] y de [segunda zona de disponibilidad].
Administración	REDSHIFT-EVENT-3670	INFO	Las tareas de mantenimiento en el clúster multi-AZ [nombre del clúster] de Amazon Redshift se terminaron a las [hora en UTC] y está disponible para su uso con los recursos de computación de [primera zona de disponibilidad]. Habrá disponibles recursos de computación secundarios en otra zona de disponibilidad en breve.
Administración	REDSHIFT-EVENT-3671	INFO	El cambio de tamaño en el clúster multi-AZ [nombre del clúster] de Amazon Redshift se terminó a las [hora en UTC] y está disponible para su uso en [primera zona de disponibilidad]. Habrá disponibles recursos de computación secundarios en otra zona de disponibilidad en breve.
Administración	REDSHIFT-EVENT-3672	INFO	El clúster multi-AZ [nombre del clúster] de Amazon Redshift detectó un error en [segunda zona de disponibilidad] a las [hora en UTC] y activó una recuperación automática.
Administración	REDSHIFT-EVENT-3673	INFO	La operación para habilitar multi-AZ para el clúster [nombre del clúster] de Amazon Redshift comenzó a las [hora en UTC].

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-3674	INFO	La operación para habilitar multi-AZ para el clúster [nombre del clúster] de Amazon Redshift se completó correctamente a las [hora en UTC].
Monitoreo	REDSHIFT-EVENT-3675	ERROR	La operación para habilitar multi-AZ para el clúster [nombre del clúster] de Amazon Redshift falló a las [hora en UTC].
Administración	REDSHIFT-EVENT-3676	INFO	La operación para deshabilitar multi-AZ para el clúster multi-AZ [nombre del clúster] de Amazon Redshift comenzó a las [hora en UTC].
Administración	REDSHIFT-EVENT-3677	INFO	La operación para deshabilitar multi-AZ para el clúster [nombre del clúster] de Amazon Redshift se completó correctamente a las [hora en UTC].
Monitoreo	REDSHIFT-EVENT-3678	ERROR	La operación para deshabilitar multi-AZ para el clúster [nombre del clúster] de Amazon Redshift falló a las [hora en UTC].
Configuración	REDSHIFT-EVENT-3679	INFO	Se ha modificado correctamente el puerto del clúster [nombre del clúster] de Amazon Redshift.
Configuración	REDSHIFT-EVENT-3680	ERROR	Amazon Redshift no ha podido crear el clúster [nombre del clúster] porque no se puede acceder al rol vinculado al servicio (SLR) necesario para esta operación. Intente crearlo de nuevo desde la consola de Amazon Redshift. Amazon Redshift creará el SLR automáticamente.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Monitoreo	REDSHIFT-EVENT-3684	ERROR	El bucket [nombre del bucket] de Amazon S3 se ha cifrado con un nombre desconocido o una clave AWS KMS inaccesible. Modifique el cifrado del bucket de Amazon S3.
Administración	REDSHIFT-EVENT-3685	ERROR	La operación de restauración en el clúster [nombre del clúster] ha producido un error porque no hay suficiente espacio en disco disponible. La operación tiene un proceso de reversión en curso. Intente restaurar en un clúster con otra configuración.
Administración	REDSHIFT-EVENT-3686	ERROR	La operación de cambio de tamaño en el clúster [nombre del clúster] ha producido un error porque no hay suficiente espacio en disco disponible. La operación tiene un proceso de reversión en curso. Intente cambiar de tamaño en un clúster con otra configuración.
Seguridad	REDSHIFT-EVENT-4000	INFO	Sus credenciales de administrador para el clúster [nombre del clúster] de Amazon Redshift se actualizaron a la(s) [hora].
Seguridad	REDSHIFT-EVENT-4001	INFO	Se modificó el grupo de seguridad [nombre del grupo de seguridad] a las [hora]. Los cambios en todos los clústeres asociados se efectuarán de manera automática.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Seguridad	REDSHIFT-EVENT-4500	ERROR	El grupo de seguridad [nombre del grupo de seguridad] que proporcionó no es válido. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Seguridad	REDSHIFT-EVENT-4501	ERROR	No se pudo encontrar el grupo de seguridad [nombre del grupo de seguridad] especificado en el grupo de seguridad de clúster [nombre del grupo de seguridad de clúster]. No se pudo completar la autorización.
Seguridad	REDSHIFT-EVENT-4502	ERROR	Se produjo un error en la actualización de las credenciales del administrador para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora] debido a actividades simultáneas. Permita que la carga de trabajo actual complete o reduzca la carga de trabajo activa y, luego, vuelva a intentar completar la operación.
Seguridad	REDSHIFT-EVENT-4503	ERROR	Amazon Redshift no puede acceder al secreto del clúster [nombre del clúster].
Seguridad	REDSHIFT-EVENT-4504	ERROR	Amazon Redshift no puede acceder a la clave de KMS [clave de KMS] que se ha utilizado para cifrar el secreto de las credenciales de administrador del clúster [nombre del clúster].
Seguridad	REDSHIFT-EVENT-4505	ERROR	Amazon Redshift no puede cambiar el secreto del clúster [nombre del clúster] porque hay una operación en curso en el clúster.

Categoría de Amazon Reds	ID de evento	Gravedad del evento	Descripción
Seguridad	REDSHIFT-EVENT-4506	ERROR	El clúster [nombre del clúster] de Amazon Redshift está en pausa. Amazon Redshift no puede cambiar los secretos de los clústeres en pausa.

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un grupo de parámetros como tipo de origen.

Categorías y eventos de un grupo de parámetros como tipo de origen

Categoría de Amazon Redsh	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1002	INFO	El grupo de parámetros [nombre del grupo de parámetros] pasó del valor [valor] al [valor] a las [hora].
Configuración	REDSHIFT-EVENT-1003	INFO	Se creó el grupo [nombre del grupo] de parámetros del clúster.
Configuración	REDSHIFT-EVENT-1004	INFO	Se eliminó el grupo [nombre del grupo] de parámetros del clúster.
Configuración	REDSHIFT-EVENT-1005	INFO	Se actualizó el grupo [nombre] de parámetros del clúster a las [hora]. Si solo cambió parámetros dinámicos, los clústeres asociados se modificarán ahora. Si cambió parámetros estáticos, todas las actualizaciones, incluidos los parámetro s dinámicos, se aplicarán cuando reinicie los clústeres asociados.

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un grupo de seguridad como tipo de origen.

Categorías y eventos de un grupo de seguridad como tipo de origen

Categoría de Amazon Redsh	ID de evento	Gravedad del evento	Descripción
Seguridad	REDSHIFT-EVENT-4002	INFO	Se creó el grupo de seguridad [nombre del grupo] del clúster.
Seguridad	REDSHIFT-EVENT-4003	INFO	Se eliminó el grupo de seguridad [nombre del grupo] del clúster.
Seguridad	REDSHIFT-EVENT-4004	INFO	Se cambió el grupo de seguridad [nombre del grupo] del clúster. Los cambios se aplicarán automáticamente a todos los clústeres asociados.

En la siguiente tabla, se muestra la categoría de eventos y una lista de los eventos correspondiente a una snapshot como tipo de origen.

Categorías y eventos de una instantánea como tipo de origen

Categoría de Amazon Redsh	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2009	INFO	Se inició la instantánea [nombre de la instantánea] de un usuario para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora]. Para supervisar el progreso de la snapshot, revise la AWS Management Console.
Administración	REDSHIFT-EVENT-2010	INFO	Se canceló la instantánea [nombre de la instantánea] del usuario para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].

Categoría de Amazon Redsh	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2011	INFO	Se eliminó la instantánea [nombre de la instantánea] del usuario para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Administración	REDSHIFT-EVENT-2012	INFO	Se inició la instantánea final [nombre de la instantánea] para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3004	INFO	Se completó correctamente la instantánea [nombre de la instantánea] del usuario para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3005	INFO	Se completó correctamente la instantánea final [nombre] para el clúster [nombre] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3006	INFO	Se canceló la instantánea final [nombre de la instantánea] para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora].
Supervisión	REDSHIFT-EVENT-3502	ERROR	Se produjo un error en la instantánea final [nombre de la instantánea] para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora]. El equipo está investigando el problema. Revise la AWS Management Console para volver a ejecutar la operación.

Categoría de Amazon Redsh	ID de evento	Gravedad del evento	Descripción
Supervisión	REDSHIFT-EVENT-3503	ERROR	Se produjo un error en la instantánea [nombre de la instantánea] del usuario para el clúster [nombre del clúster] de Amazon Redshift a la(s) [hora]. El equipo está investigando el problema. Revise la AWS Management Console para volver a ejecutar la operación.

Notificaciones de eventos de Amazon Redshift sin servidor con Amazon EventBridge

Amazon Redshift Serverless utiliza Amazon EventBridge para administrar las notificaciones de eventos y mantenerle actualizado sobre los cambios en el almacenamiento de datos. Amazon EventBridge es un servicio de bus de eventos sin servidor que se puede utilizar para conectar las aplicaciones con datos de varios orígenes. En este caso, el origen de eventos es Amazon Redshift. Los eventos, que son cambios monitoreados en un entorno, se envían a EventBridge desde el almacenamiento de datos de Amazon Redshift automáticamente. Los eventos se envían casi en tiempo real.

Las capacidades de EventBridge incluyen proporcionar un entorno para escribir reglas de eventos, que pueden especificar las acciones que se deben realizar para eventos específicos. También puede configurar destinos, que son recursos a los que EventBridge puede enviar un evento. Un objetivo puede incluir un destino de API, un grupo de registro de Amazon CloudWatch, etc. Para obtener más información sobre reglas, consulte Reglas de Amazon EventBridge. Para obtener más información sobre destinos, consulte Destinos de Amazon EventBridge.

Los eventos se pueden clasificar según la gravedad y por categorías. Están disponibles los siguientes filtros:

- Filtrado de recursos: reciba mensajes en función del recurso al que estén asociados los eventos. Los recursos incluyen un grupo de trabajo, una instantánea, etc.
- Filtro de intervalo de tiempo: analice los eventos en un periodo de tiempo específico.

- Filtrado por categorías: reciba notificaciones de eventos de todos los eventos de las categorías especificadas.

En la tabla siguiente se incluyen los eventos de Amazon Redshift Serverless, con metadatos adicionales:

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
RateChange	REDSHIFT-SERVERLESS-EVENT-1001	INFO	El cambio de RPU base del grupo de trabajo se completó correctamente a la hora <time in UTC>.
RateChange	REDSHIFT-SERVERLESS-EVENT-1002	ERROR	No se pudo completar el cambio de RPU base del grupo de trabajo a la hora <time in UTC>.
Supervisión	REDSHIFT-SERVERLESS-EVENT-1003	INFO	El software se actualizó en el almacenamiento de datos de Amazon Redshift <endpoint name> a la hora <time in UTC>.
Configuración	REDSHIFT-SERVERLESS-EVENT-1011	ERROR	Amazon Redshift sin servidor no ha podido crear el grupo de trabajo [nombre del grupo de trabajo] porque no se puede acceder al rol

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
			vinculado al servicio (SLR) necesario para esta operación . Intente crearlo de nuevo en la consola de Amazon Redshift. Amazon Redshift creará el SLR automátic amente.
Supervisión	REDSHIFT-SERVERLESS-EVENT-1500	ERROR	No se puede crear ni actualizar el grupo de trabajo <workgroup name> porque superó el límite de direccion es IP elásticas de su cuenta. Elimine las direcciones IP elásticas no utilizadas o solicite un aumento del límite a Amazon EC2.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-SERVERLESS-EVENT-1501	ERROR	La subred <subnet id> no tiene direccion es IP disponibles. Esto evitará que los siguientes tipos de consultas se ejecuten correctamente en el grupo de trabajo <workgroup name>: EMR, consultas federadas y COPY/ UNLOAD de Amazon EC2. Para corregir el problema, libere las IP de la subred eliminando las ENI.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-SERVERLESS-EVENT-1502	ERROR	La subred <subnet id> no tiene direccion es IP disponibles. Esto evitará que los tipos de consultas de Amazon EMR, las consultas federadas de Redshift, COPY/ UNLOAD de Redshift y Redshift ML se ejecuten correctam ente en el grupo de trabajo <workgrou p name>. Para corregir el problema, libere las IP de la subred eliminando las interfaces de red elástica (ENI) que no se utilizan.
Administr ación	REDSHIFT-SERVERLESS-EVENT-1008	INFO	Se ha creado el grupo de trabajo <workgroup name> de Amazon Redshift y está listo para usarse.
Administr ación	REDSHIFT-SERVERLESS-EVENT-1009	INFO	El grupo de trabajo <workgroup name> de Amazon Redshift se eliminó a la hora <time in UTC>.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-SERVERLESS-EVENT-1000	INFO	La instantánea <snapshot name> se completó correctamente a la hora <time in UTC>.
Administración	REDSHIFT-SERVERLESS-EVENT-1004	INFO	La restauración desde una instantánea en el espacio de nombres <namespace name> se completó correctamente a la hora <time in UTC>.
Administración	REDSHIFT-SERVERLESS-EVENT-1005	ERROR	Se produjo un error en la restauración desde una instantánea en el espacio de nombres <namespace name> a la hora <time in UTC>.
Administración	REDSHIFT-SERVERLESS-EVENT-1006	INFO	La restauración desde un punto de recuperación en el espacio de nombres <namespace name> se completó correctamente a la hora <time in UTC>.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Administración	REDSHIFT-SERVERLESS-EVENT-1007	INFO	Se produjo un error en la restauración desde un punto de recuperación en el espacio de nombres <namespace name> a la hora <time in UTC>.
Seguridad	REDSHIFT-SERVERLESS-EVENT-1012	ERROR	Amazon Redshift no puede acceder al secreto de su espacio de nombres <nombre del espacio de nombres>.
Seguridad	REDSHIFT-SERVERLESS-EVENT-1013	ERROR	Amazon Redshift no puede acceder a la clave de KMS que se ha utilizado para cifrar el secreto de las credenciales de administrador para el espacio de nombres [nombre del espacio de nombres].

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Seguridad	REDSHIFT-SERVERLESS-EVENT-1014	ERROR	Amazon Redshift no puede rotar el secreto del espacio de nombres <nombre del espacio de nombres> porque hay una operación en curso en el grupo de trabajo.
Seguridad	REDSHIFT-SERVERLESS-EVENT-1015	ERROR	Su espacio de nombres <nombre del espacio de nombres> no tiene ningún grupo de trabajo adjunto. Amazon Redshift solo puede rotar los secretos de los espacios de nombres que tengan grupos de trabajo asociados.
Seguridad	REDSHIFT-SERVERLESS-EVENT-1016	INFO	Credenciales de administrador actualizadas para su espacio de nombres <nombre del espacio de nombres> a las <hora en UTC>.

Notificaciones de eventos de integración sin ETL con Amazon EventBridge

La integración sin ETL utiliza Amazon EventBridge para administrar las notificaciones de eventos y ofrecerle actualizaciones sobre los cambios en las integraciones. Amazon EventBridge es un servicio de bus de eventos sin servidor que se puede utilizar para conectar las aplicaciones con datos de varios orígenes. En este caso, el origen de eventos es Amazon Redshift. Los eventos, que son cambios monitoreados en un entorno, se envían a EventBridge desde el almacenamiento de datos de Amazon Redshift automáticamente. Los eventos se envían casi en tiempo real.

EventBridge proporciona un entorno para escribir reglas de eventos, que pueden especificar las acciones que se deben realizar para eventos específicos. También puede configurar destinos, que son recursos a los que EventBridge puede enviar un evento. Un objetivo puede incluir un destino de API, un grupo de registro de Amazon CloudWatch, etc. Para obtener más información sobre reglas, consulte Reglas de Amazon EventBridge. Para obtener más información sobre destinos, consulte Destinos de Amazon EventBridge.

Los eventos se pueden clasificar según la gravedad y por categorías. Están disponibles los siguientes filtros:

- Filtrado de recursos: reciba mensajes en función del recurso al que estén asociados los eventos. Los recursos incluyen un grupo de trabajo o una instantánea.
- Filtro de intervalo de tiempo: analice los eventos en un periodo de tiempo específico.
- Filtrado por categorías: reciba notificaciones de eventos de todos los eventos de las categorías especificadas.

En la siguiente tabla se incluyen eventos de integración sin ETL con metadatos adicionales:

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-INTEGRATION-EVENT-0000	INFO	La integración sin ETL <nombre de la integración> se ha

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
			creado y ahora está ACTIVE.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0001	INFO	La integración sin ETL <nombre de la integración> se ha eliminado a las <hora en UTC>.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0002	INFO	La eliminación de la integración sin ETL <nombre de la integración> se ha iniciado a las <hora en UTC>.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0003	INFO	La integración sin ETL <nombre de la integración> está sincronizando datos de transacción en el almacenamiento de datos de destino.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-INTEGRATION-EVENT-0004	WARNING	Una o varias de las tablas no tienen clave principal y no se pueden sincroniz ar. Realice una copia de seguridad en Amazon RDS, elimine estas tablas y vuelva a crearlas siguiendo las prácticas recomenda das de Amazon Redshift para el diseño de tablas.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0005	WARNING	No se pueden sincronizar una o más tablas porque contienen longitude s o tipos de datos no compatibles. Corrija las tablas e inténtelo de nuevo. Para saber más sobre los tipos de datos no compatibl es, consulte Tipos de datos no admitidos.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-INTEGRATION-EVENT-0006	ERROR	No se ha podido crear la integración. Hay que eliminar y volver a crear la integración.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0007	ERROR	No se ha podido cargar los datos debido a un error interno. Hay que eliminar y volver a crear la integración.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0008	ERROR	La autorización ha fallado porque se han denegado los permisos del clúster de la base de datos de Aurora de origen. Hay que eliminar y volver a crear la integración.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0009	ERROR	No se pueden enviar datos a Amazon Redshift porque el número de tablas y esquemas supera el límite de Amazon Redshift. Hay que eliminar y volver a crear la integración.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Supervisión	REDSHIFT-INTEGRATION-EVENT-0012	ERROR	Se ha invocado una restauración desde el punto de recuperación en el espacio de nombres sin servidor de destino. Hay que eliminar y volver a crear la integración.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0013	INFO	La integración sin ETL <nombre de la integración> ahora está ACTIVE.
Supervisión	REDSHIFT-INTEGRATION-EVENT-0014	ERROR	La integración <nombre de la integración> ha fallado porque no se ha podido modificar debido a un error interno. Hay que eliminar y volver a crear la integración. Si el error persiste, póngase en contacto con AWS Support.
Operación	REDSHIFT-INTEGRATION-EVENT-0015	INFO	Se ha aplicado un cambio de DDL <cambio de DDL> a la tabla <esquema.nombre>.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Operación	REDSHIFT-INTEGRATION-EVENT-0016	INFO	Su integración sin ETL <nombre de la integración> está procesando una solicitud de modificación con los siguientes argumentos: <copia de los argumentos de la solicitud>.
Operación	REDSHIFT-INTEGRATION-EVENT-0017	INFO	Se ha aplicado la modificación a la integración sin ETL <nombre de la integración>.
Operación	REDSHIFT-INTEGRATION-EVENT-0018	WARNING	Se ha pausado el clúster de Amazon Redshift de destino. Espere a que el clúster esté pausado y, a continuación, reanúdelo para continuar con la transmisión de datos.
Operación	REDSHIFT-INTEGRATION-EVENT-0019	WARNING	Se ha pausado el clúster de Amazon Redshift de destino. Reanude el clúster para continuar con la transmisión de datos.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Operación	REDSHIFT-INTEGRATION-EVENT-0020	WARNING	Se ha reanudado el clúster de Amazon Redshift de destino. Espere a que el clúster esté activo para continuar con la transmisión de datos.
Configuración	REDSHIFT-INTEGRATION-EVENT-1000	ERROR	Uno o varios parámetros del clúster de base de datos de Aurora de origen están mal configurados. Corrija el grupo de parámetros y reinicie el clúster para aplicar los cambios y, a continuación, vuelva a crear la integración.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Configuración	REDSHIFT-INTEGRATION-EVENT-1001	ERROR	La integración ha fallado porque el valor del parámetro enable_case_sensitive_identifier es incorrecto. Establezca el valor en true para el clúster de base de datos de Aurora de origen y, a continuación, elimine y vuelva a crear la integración.
Configuración	REDSHIFT-INTEGRATION-EVENT-1002	ERROR	La integración ha fallado porque el valor del parámetro cdc_insert_enabled es incorrecto. Establezca el valor en true para el clúster de base de datos de Aurora de origen y, a continuación, elimine y vuelva a crear la integración.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Configuración	REDSHIFT-INTEGRATION-EVENT-1003	ERROR	El parámetro binlog_format del grupo de parámetros del clúster de base de datos de origen debe establecerse en ROW. Corrija el grupo de parámetros y reinicie el clúster para aplicar el cambio y, a continuación, vuelva a crear la integración.
Configuración	REDSHIFT-INTEGRATION-EVENT-1004	ERROR	No se han podido cargar los datos porque el parámetro del clúster binlog_transaction_compression está activado. Establezca el valor del parámetro en OFF y reinicie la instancia de escritura para aplicar el cambio y, a continuación, vuelva a crear la integración.

Categoría de Amazon Redshift	ID de evento externo	Gravedad del evento	Descripción del mensaje
Configuración	REDSHIFT-INTEGRATION-EVENT-1005	ERROR	No se han podido cargar los datos porque el parámetro del clúster binlog_row_value_options está establecido en PARTIAL_JSON, lo cual no es compatible. Corrija el grupo de parámetros y reinicie la instancia de escritura para aplicar el cambio y, a continuación, vuelva a crear la integración.
Configuración	REDSHIFT-INTEGRATION-EVENT-1006	WARNING	No se ha podido analizar el filtro de integración. Corrija la sintaxis del filtro.

Cuotas y límites de Amazon Redshift

Amazon Redshift tiene cuotas que limitan el uso de varios recursos en su cuenta de AWS en función de cada región de AWS. Existe un valor predeterminado para cada cuota, y algunas cuotas se pueden ajustar. En el caso de las cuotas ajustables, puede solicitar un aumento para su cuenta de AWS en una región de AWS mediante el envío de un Formulario de aumento de límites de Amazon Redshift.

Cuotas para objetos de Amazon Redshift

Amazon Redshift tiene cuotas que limitan el uso de varios tipos de objetos. Hay un valor predeterminado para cada uno.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Cuentas de AWS que puede autorizar para que restauren una instantánea por instantánea	20	No	Número máximo de cuentas de AWS que puede autorizar para realizar una restauración de instantánea por instantánea.
Cuentas de AWS que puede autorizar para que restauren	100	No	El número máximo de cuentas de AWS que puede autorizar para que restauren una instantánea por cada clave de KMS. Es decir, si tiene 10 instantáneas que están cifradas con una sola clave de KMS, puede autorizar a 10 cuentas de AWS a restaurar cada instantánea u otras combinaciones que sumen

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
una instantánea por cada AWS KMS key			hasta 100 cuentas y no excedan las 20 cuentas por cada instantánea.
Roles de IAM del clúster que permiten a Amazon Red acceder a otros servicios de AWS	50[1]	No	Número máximo de roles de IAM que puede asociar a un clúster para permitir que Amazon Redshift acceda a otros servicios de AWS del usuario propietario del clúster y los roles de IAM. [1] La cuota es 10 en las siguientes Regiones de AWS: us-iso-east-1, us-iso-west-1, us-isob-east-1.
Nivel de simultaneidad (slots de consulta) de todas las colas de WLM manuales definidas por el usuario	50	No	Máximo número de slots de consulta en todas las colas definidas por el usuario a través de la administración manual de cargas de trabajo.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Clústeres de escalado de simultaneidad	10	Sí	Número máximo de clústeres de escalado de simultaneidad.
Nodos DC2 de un clúster	128	Sí	Número máximo de nodos DC2 que se pueden asignar a un clúster. Para obtener más información sobre los límites de cada tipo de nodo, consulte Clústeres y nodos de Amazon Redshift.
Nodos DS2 de un clúster	128	Sí	Número máximo de nodos DS2 que se pueden asignar a un clúster. Para obtener más información sobre los límites de cada tipo de nodo, consulte Clústeres y nodos de Amazon Redshift.
Suscripciones de eventos	20	Sí	Número máximo de suscripciones a eventos para esta cuenta en la región de AWS actual.
Nodos	200	Sí	Número máximo de nodos entre todas las instancias de base de datos para esta cuenta en la región de AWS actual.
Grupos de parámetros	20	No	Número máximo de grupos de parámetros para esta cuenta en la región de AWS actual.
Nodos RA3 de un clúster	128	Sí	Número máximo de nodos RA3 que se pueden asignar a un clúster. Para obtener más información sobre los límites de cada tipo de nodo, consulte Clústeres y nodos de Amazon Redshift.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Puntos de enlace de la VPC administrados por Redshift que se conectan a un clúster	30	Sí	Número máximo de puntos de enlace de la VPC administrados por Redshift que puede conectar a un clúster. Para obtener más información acerca de los puntos de enlace de la VPC administrados por Redshift, consulte Uso de puntos de enlace de la VPC administrados por Redshift.
Los beneficiarios del clúster al cual se accede a través de un punto de enlace de la VPC administrado por Redshift	5	Sí	Número máximo de beneficiarios que el propietario de un clúster puede autorizar para crear un punto de enlace de la VPC administrado por Redshift para un clúster. Para obtener más información acerca de los puntos de enlace de la VPC administrados por Redshift, consulte Uso de puntos de enlace de la VPC administrados por Redshift.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Puntos de enlaces de la VPC administrados por Redshift por cada autorización	5	Sí	Número máximo de puntos de enlace de la VPC administrados por Redshift que puede crear por cada autorización. Para obtener más información acerca de los puntos de enlace de la VPC administrados por Redshift, consulte Uso de puntos de enlace de la VPC administrados por Redshift.
Nodos reservados	200	Sí	Número máximo de nodos reservados para esta cuenta en la región de AWS actual.
Esquemas de cada base de datos por clúster	9900	No	Número máximo de esquemas que se pueden crear en cada base de datos y cada clúster. No obstante, los esquemas `pg_temp_*` no se tienen cuentan para calcular esta cuota.
Grupos de seguridad	20	Sí	Número máximo de grupos de seguridad para esta cuenta en la región de AWS actual.
Tamaño de fila única cuando carga se realiza mediante COPY	4	No	Tamaño máximo (en MB) de una sola fila cuando la carga se realiza mediante el comando COPY.
Instantáneas	20	Sí	Número máximo de instantáneas del usuario para esta cuenta en la región de AWS actual.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Grupos de subredes	20	Sí	Número máximo de grupos de subredes para esta cuenta en la región de AWS actual.
Subredes de un grupo de subredes	20	Sí	Número máximo de subredes de un grupo de subredes.
Tablas de nodos de clúster de tipo `large`	9900	No	Número máximo de tablas en los nodos de clúster de tipo large. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.
Tablas de nodos de clúster de tipo `xlarge`	9900	No	Número máximo de tablas en los nodos de clúster de tipo `xlarge`. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Tablas para el tipo de nodo de clúster `xlplus` con un clúster de un solo nodo.	9900	No	Número máximo de tablas para el tipo de nodo de clúster `xlplus` con un clúster de un solo nodo. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.
Tablas para el tipo de nodo de clúster `xlplus` con un clúster de varios nodos.	20 000	No	Número máximo de tablas para el tipo de nodo de clúster `xlplus` con un clúster de varios nodos. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Tablas de nodos de clúster de tipo `4xlarge`	200.000	No	Número máximo de tablas en los nodos de clúster de tipo `4xlarge`. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.
Tablas de nodos de clúster de tipo `8xlarge`	200.000	No	Número máximo de tablas en los nodos de clúster de tipo `8xlarge`. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Tablas de nodos de clúster de tipo `16xlarge`	200.000	No	Número máximo de tablas en los nodos de clúster de tipo `16xlarge`. Este límite incluye tablas permanentes, tablas temporales, tablas de recursos para compartir datos y vistas materializadas. Las tablas externas se cuentan como tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de las consultas o el mantenimiento del sistema. Las vistas y las tablas de sistema no se incluyen en este límite.
Número de bases de datos	60	No	El número máximo permitido de bases de datos en un clúster de Amazon Redshift. Esto excluye las bases de datos creadas a partir de recursos compartidos de datos.
Tiempo de espera para sesiones en reposo o inactivas	4 horas	No	Este ajuste se aplica al clúster. Para obtener más información sobre cómo configurar el valor del tiempo de espera de la sesión en reposo de un usuario, consulte ALTER USER en la Guía para desarrolladores de bases de datos de Amazon Redshift. El ajuste del usuario tiene prioridad sobre el ajuste del clúster.
Tiempo de espera para las transacciones inactivas	6 horas	No	El período máximo de inactividad de una transacción abierta antes de que Amazon Redshift finalice la sesión asociada a la transacción. Esta configuración tiene prioridad sobre la relativa al tiempo de inactividad definida por el usuario. Se aplica al clúster.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Procedimientos almacenados en una base de datos	10 000	No	Número máximo de procedimientos almacenados. Consulte Límites y diferencias para procedimientos almacenados compatibles si desea conocer más límites.
Número máximo de conexiones para nodos RA3	2,000	No	El número máximo de conexiones a un clúster RA3. (Se aplica de manera específica a los tipos de nodos ra3.xlplus, ra3.4xlarge y ra3.16xlarge). El número máximo de conexiones permitidas varía según el tipo de nodo.
Número máximo de conexiones para nodos DC2 y DS2	Varía	No	El número máximo de conexiones a un clúster dc2.large o ds2.large es 500. El número máximo de colecciones en un clúster dc2.8xlarge o ds2.8xlarge es 2000.
Número de roles de Amazon Redshift en un clúster	1 000	Sí	Número máximo de roles de Amazon Redshift que puede crear por clúster. Para obtener más información sobre los roles del control de acceso basado en roles (RBAC), consulte Control de acceso basado en roles (RBAC) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Cuotas de objetos de Amazon Redshift Serverless

Amazon Redshift tiene cuotas que limitan el uso de varios tipos de objetos en la instancia de Amazon Redshift Serverless. Hay un valor predeterminado para cada uno.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Número de bases de datos	100	No	El número máximo permitido de bases de datos en un espacio de nombres de Amazon Redshift sin servidor. Esto excluye las bases de datos creadas a partir de recursos compartidos de datos.
Número de esquemas	9900	No	El número máximo permitido de esquemas en una instancia de Amazon Redshift Serverless.
Número de tablas	200.000	No	El número máximo permitido de tablas en una instancia de Amazon Redshift Serverless.
Tiempo de espera para sesiones en reposo o inactivas	1 hora	No	Para obtener más información sobre cómo configurar el valor del tiempo de espera de la sesión en reposo de un usuario, consulte ALTER USER en la Guía para desarrolladores de bases de datos de Amazon Redshift. La configuración del usuario tiene prioridad.
Se ha agotado el tiempo de espera de una consulta en ejecución	86 399 segundos (24 horas)	No	Tiempo máximo de ejecución de una consulta antes de que Amazon Redshift la finalice.
Tiempo de espera para las transacciones inactivas	6 horas	No	El período máximo de inactividad de una transacción abierta antes de que Amazon Redshift Serverless finalice la sesión asociada a la transacción. Esta configuración tiene prioridad sobre la relativa al tiempo de inactividad definida por el usuario.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Número máximo de conexiones	2000	No	El número máximo de conexiones permitidas para conectarse a un grupo de trabajo.
Número de grupos de trabajo	25	Sí	Número de grupos de trabajo admitidos.
Número de espacios de nombres	25	Sí	Número de espacios de nombres admitidos.
Número de roles de Amazon Redshift en un grupo de trabajo	1 000	Sí	Número máximo de roles de Amazon Redshift que puede crear por grupo de trabajo. Para obtener más información sobre los roles del control de acceso basado en roles (RBAC), consulte Control de acceso basado en roles (RBAC) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para obtener más información acerca de la forma en que la configuración del tiempo de espera afecta a la facturación de Amazon Redshift Serverless, consulte Facturación para Amazon Redshift Serverless.

Cuotas para la API de datos de Amazon Redshift

Amazon Redshift tiene cuotas que limitan el uso de la API de datos de Redshift. Hay un valor predeterminado para cada uno. Para obtener más información acerca de la API de datos de Amazon Redshift, consulte Uso de la API de datos de Amazon Redshift.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Transacciones por segundo (TPS) para la API `BatchExecuteStatement`	20	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `CancelStatement`	3	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `DescribeStatement`	100	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `DescribeTable`	3	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Transacciones por segundo (TPS) para la API `ExecuteStatement`	30	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `GetStatementResult`	20	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `ListDatabases`	3	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `ListSchemas`	3	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Transacciones por segundo (TPS) para la API `ListStatements`	3	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.
Transacciones por segundo (TPS) para la API `ListTables`	3	No	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación.

Cuotas para objetos del editor de consultas v2

Amazon Redshift tiene cuotas que limitan el uso de varios tipos de objetos en el editor de consultas de Amazon Redshift v2. Hay un valor predeterminado para cada uno.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Conexiones	500	Sí	El número máximo de conexiones que puede crear en esta cuenta y en la región actual utilizando el editor de consultas v2.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Entidades principales activas por cuenta	50	Sí	Número máximo de entidades principales simultáneas que pueden usar el editor de consultas v2 en esta cuenta en la región actual.
Consultas guardadas	2.500	Sí	El número máximo de consultas guardadas que puede crear en esta cuenta y en la región actual utilizando el editor de consultas v2.
Versiones de consultas	20	Sí	El número máximo de versiones por consulta que puede crear en esta cuenta y en la región actual utilizando el editor de consultas v2.
Gráficos guardados	500	Sí	El número máximo de gráficos guardados que puede crear en esta cuenta y en la región actual utilizando el editor de consultas v2.
Filas recuperadas por consulta	100 000	No	El número máximo de filas recuperadas por consulta por el editor de consultas v2 en esta cuenta y en la región actual.
Tamaño de los datos recuperados por consulta	5	No	Tamaño máximo, en megabytes, de los datos recuperados por consulta por el editor de consultas v2 en esta cuenta y en la región actual.

Nombre de la cuota	Valor predeterminado de AWS	Ajustable	Descripción
Conexiones de socket simultáneas por entidad principal	10	Sí	Número máximo de conexiones de socket simultáneas al editor de consultas v2 que puede establecer una sola entidad principal en la región actual. Evalúe si debe aumentar esta cuota en caso de que reciba errores que le indiquen que sus conexiones de socket están por encima del límite.
Conexiones de socket simultáneas por cuenta	250	Sí	Número máximo de conexiones de socket simultáneas al editor de consultas v2 que pueden establecer todas las entidades principales de la cuenta en la región actual. Evalúe si debe aumentar esta cuota en caso de que reciba errores que le indiquen que sus conexiones de socket están por encima del límite.
Máximo de conexiones simultáneas	3	No	Número máximo de conexiones a bases de datos por usuario (incluye sesiones aisladas). El administrador del editor de consultas v2 puede establecer este valor del 1 al 10 en la Account settings (Configuración de la cuenta). Si alcanza el límite establecido por el administrador, considere la posibilidad de utilizar sesiones compartidas en lugar de sesiones aisladas al ejecutar el SQL. Para obtener más información acerca de las conexiones, consulte Apertura del editor de consultas v2. Para obtener más información sobre cómo configurar el límite, consulte Modificación de la configuración de la cuenta.

Cuotas y límites de objetos de Amazon Redshift Spectrum

Amazon Redshift Spectrum dispone de los siguientes límites y cuotas:

- Número máximo de bases de datos por cada cuenta de AWS cuando se utiliza AWS Glue Data Catalog. Para ver este valor, consulte Cuotas de servicio de AWS Glue en la Referencia general de Amazon Web Services.
- Número máximo de tablas por cada base de datos cuando se utiliza AWS Glue Data Catalog. Para ver este valor, consulte Cuotas de servicio de AWS Glue en la Referencia general de Amazon Web Services.
- Número máximo de particiones por cada tabla cuando se utiliza AWS Glue Data Catalog. Para ver este valor, consulte Cuotas de servicio de AWS Glue en la Referencia general de Amazon Web Services.
- Número máximo de particiones por cada cuenta de AWS cuando se utiliza AWS Glue Data Catalog. Para ver este valor, consulte Cuotas de servicio de AWS Glue en la Referencia general de Amazon Web Services.
- El número máximo de columnas de tablas externas cuando se utiliza AWS Glue Data Catalog es de 1597 cuando las pseudocolumnas están habilitadas y de 1600 cuando no lo están.
- El tamaño máximo de un valor de cadena de un archivo ION o JSON cuando se utiliza AWS Glue Data Catalog es 16 KB. La cadena se puede truncar si se alcanza este límite.
- Puede añadir un máximo de 100 particiones en una única instrucción ALTER TABLE.
- Todos los datos de S3 deben estar en la misma región de AWS que el clúster de Amazon Redshift.
- Las marcas temporales de ION y JSON deben usar el formato ISO8601.
- No se admite la compresión externa de archivos ORC.
- Los SERDE de Text, OpenCSV y Regex no admiten delimitadores octales mayores que `\177`
- Debe especificar un predicado en la columna de partición para evitar que se lean datos de todas las particiones.

  Por ejemplo, el predicado siguiente filtrará la columna `ship_dtm`, pero no aplicará el filtro en la columna de partición `ship_yyyymm`:

  ```
  WHERE ship_dtm > '2018-04-01'.
  ```

  Para omitir las particiones innecesarias, tiene que añadir un predicado `WHERE ship_yyyymm = '201804'`. Este predicado limitará las operaciones de lectura a la partición `\ship_yyyymm=201804\`.

Estos límites no se aplican a un metaalmacén Apache Hive.

Restricciones en la nomenclatura

En la siguiente tabla, se describen las restricciones en la nomenclatura de Amazon Redshift.

Identificador de clúster	• Un identificador de clúster debe contener caracteres en minúscula únicamente. • Debe incluir entre 1 y 63 caracteres alfanuméricos o guiones. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos. • Debe ser único para todos los clústeres de una cuenta de AWS.
Nombre de base de datos	• El nombre de base de datos debe contener entre 1 y 64 caracteres alfanuméricos. • Debe contener letras en minúscula únicamente. • No puede ser una palabra reservada. Para obtener una lista de palabras reservadas, consulte Palabras reservadas en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Nombre del punto de enlace de la VPC administrado por Redshift	• El nombre de un punto de enlace debe contener entre 1 y 30 caracteres. • Los caracteres válidos son A-Z, a-z, 0-9 y guion (-). • El primer carácter debe ser una letra. •

	El nombre no puede contener dos guiones consecutivos ni finalizar con guion.
Nombre de usuario administrador	• Un nombre de usuario administrador debe contener solo caracteres en minúsculas. • Debe tener entre 1 y 128 caracteres alfanuméricos. • El primer carácter debe ser una letra. • No puede ser una palabra reservada. Para obtener una lista de palabras reservadas, consulte Palabras reservadas en la Guía para desarrolladores de bases de datos de Amazon Redshift.
Contraseña de administrador	• Una contraseña de administrador debe contener entre 8 y 64 caracteres. • Debe contener una letra mayúscula como mínimo. • Debe contener una letra minúscula como mínimo. • Debe contener un número. • Puede usar cualquier carácter ASCII con códigos ASCII del rango de 33 a 126, excepto ' (comilla simple), " (comilla doble), \, / o @.

Nombre del grupo de parámetros	• El nombre de un grupo de parámetros debe contener entre 1 y 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos.
Nombre del grupo de seguridad de clúster	• El nombre de un grupo de seguridad de clúster no debe contener más de 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • No debe ser **`Default`**. • Debe ser único para todos los grupos de seguridad creados por la cuenta de AWS.
Nombre del grupo de subred	• El nombre de un grupo de subred no debe contener más de 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • No debe ser **`Default`**. • Debe ser único para todos los grupos de subred creados por la cuenta de AWS.

Identificador de instantánea de clúster	• Un identificador de instantánea de clúster no debe contener más de 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • No debe ser **`Default`**. • Debe ser único para todos los identificadores de instantáneas creados por la cuenta de AWS.

Etiquetado de recursos en Amazon Redshift

Temas

- Información general del proceso de etiquetado
- Administración de etiquetas de recursos mediante la consola
- Administración de etiquetas mediante la API de Amazon Redshift

Información general del proceso de etiquetado

En AWS, el usuario define las etiquetas, que se componen de pares de clave-valor. Amazon Redshift admite el uso de etiquetas para proporcionar metadatos sobre los recursos a simple vista y para categorizar los informes de facturación en función de la asignación de costos. Para utilizar etiquetas para la asignación de costos, primero debe activar esas etiquetas en el servicio AWS Billing and Cost Management. Si desea obtener más información acerca de la configuración y el uso de etiquetas para la facturación, consulte Uso de etiquetas de asignación de costos y Configuración de un informe mensual de asignación de costos.

Las etiquetas no son obligatorias para los recursos de Amazon Redshift, pero ayudan a proporcionar contexto. Es posible que desee etiquetar recursos con metadatos en relación con los centros de costos, nombres de proyectos y otra información relevante relacionada con el recurso. Por ejemplo, suponga que desea hacer un seguimiento de qué recursos pertenecen a un entorno de prueba y a un entorno de producción. Puede crear una clave denominada `environment` y proporcionar el valor de `test` o de `production` para identificar los recursos que se utilizan en cada entorno. Si utiliza etiquetas en otros servicios de AWS o si tiene categorías estándar en su negocio, le recomendamos crear los mismos pares de clave-valor en los recursos de Amazon Redshift para mantener la consistencia.

Después de que cambia el tamaño de un clúster y después de que restaura una snapshot de un clúster dentro de la misma región, se conservan las etiquetas para los recursos. Sin embargo, no se conservan las etiquetas si copia una snapshot a otra región, por lo que deberá volver a crear las etiquetas en la nueva región. Si elimina un recurso, se eliminarán todas las etiquetas asociadas.

Cada recurso tiene un conjunto de etiquetas, que es una colección de una o varias etiquetas asignadas al recurso. Cada recurso puede tener hasta 50 etiquetas por cada conjunto de etiquetas. Puede añadir etiquetas al crear un recurso y después de que se haya creado. Puede agregar etiquetas a los siguientes tipos de recursos de Amazon Redshift:

- CIDR/IP
- Clúster
- Grupo de seguridad de clúster
- Regla de entrada del grupo de seguridad de clúster
- Grupo de seguridad de Amazon EC2
- Conexión de un módulo de seguridad de hardware (HSM)
- Certificado de cliente del HSM
- Grupo de parámetros
- Instantánea
- Subnet group (Grupo de subredes)

Para utilizar el etiquetado desde la consola de Amazon Redshift, el usuario de IAM puede adjuntar la política administrada de AWS `AmazonRedshiftFullAccess`. Para obtener un ejemplo de política de IAM con permisos de etiquetado limitados que puede adjuntar a un usuario de la consola de Amazon Redshift, consulte Ejemplo 7: Permitir a un usuario etiquetar recursos con la consola de Amazon Redshift. Para obtener más información acerca del etiquetado, consulte ¿Qué es AWS Resource Groups?

Requisitos de etiquetado

Las etiquetas tienen los siguientes requisitos:

- Las claves no pueden tener el prefijo `aws:`.
- Las claves deben ser únicas dentro de un conjunto de etiquetas.
- Una clave debe tener entre 1 y 128 caracteres permitidos.
- Un valor debe tener entre 0 y 256 caracteres permitidos.
- No es necesario que los valores sean únicos dentro de un conjunto de etiquetas.
- Los caracteres permitidos para las claves y los valores son letras y dígitos Unicode, espacios en blanco y cualquiera de estos símbolos: _ . : / = + - @.
- Las claves y los valores distinguen entre mayúsculas y minúsculas.

Administración de etiquetas de recursos mediante la consola

Para administrar etiquetas en los recursos de Amazon Redshift

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en https://console.aws.amazon.com/redshiftv2/.
2. En el menú de navegación, elija Configurations (Configuraciones) y, a continuación, elija Manage tags (Administrar etiquetas).
3. Introduzca sus elecciones para los recursos y seleccione qué etiquetas añadir, modificar o eliminar. A continuación seleccione Manage tags of the resources that you choose (Administrar las etiquetas de los recursos que elija).

   Los recursos que puede etiquetar incluyen clústeres, grupos de parámetros, grupos de subredes, certificados de clientes HSM, conexiones HSM e instantáneas.
4. En la página de navegación Manage tags (Administrar etiquetas), elija Review and apply tag changes (Revisar y aplicar los cambios de etiqueta) y, a continuación, seleccione Apply (Aplicar) para guardar los cambios.

Administración de etiquetas mediante la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la AWS CLI para administrar etiquetas en Amazon Redshift.

- create-tags
- delete-tags
- describe-tags

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar etiquetas:

- CreateTags
- DeleteTags
- DescribeTags
- Etiqueta
- TaggedResource

Además, puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar y ver las etiquetas de un recurso determinado:

- CreateCluster
- CreateClusterParameterGroup
- CreateClusterSecurityGroup
- CreateClusterSnapshot
- CreateClusterSubnetGroup
- CreateHsmClientCertificate
- CreateHsmConfiguration
- DescribeClusters
- DescribeClusterParameterGroups
- DescribeClusterSecurityGroups
- DescribeClusterSnapshots
- DescribeClusterSubnetGroups
- DescribeHsmClientCertificates
- DescribeHsmConfigurations

Versiones de clúster para Amazon Redshift

Amazon Redshift publica regularmente versiones de clúster. Los clústeres de Amazon Redshift se revisan durante el periodo de mantenimiento del sistema. El momento de la revisión depende de la Región de AWS y configuración del periodo de mantenimiento. Puede ver o cambiar la configuración del periodo de mantenimiento desde la consola de Amazon Redshift. Para obtener más información sobre mantenimiento, consulte Mantenimiento de clústeres.

Puede consultar la versión de su clúster en la consola de Amazon Redshift en la pestaña Maintenance (Mantenimiento) de los detalles del clúster. O puede ver la versión del clúster en el resultado del comando SQL:

```
SELECT version();
```

Temas

- Parche 180 de Amazon Redshift
- Parche 179 de Amazon Redshift
- Revisión 178 de Amazon Redshift
- Revisión 177 de Amazon Redshift
- Parche 176 de Amazon Redshift
- Parche 175 de Amazon Redshift
- Revisión 174 de Amazon Redshift
- Parche 173 de Amazon Redshift
- Parche 172 de Amazon Redshift
- Parche 171 de Amazon Redshift
- Parche 170 de Amazon Redshift
- Parche 169 de Amazon Redshift
- Parche 168 de Amazon Redshift

Parche 180 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.63590 - Versión actual de la pista: publicada el 19 de febrero de 2024
- 1.0.63567 - Versión de Amazon Redshift sin servidor: publicada el 16 de febrero de 2024
- 1.0.63282 - Versión de Amazon Redshift sin servidor: publicada el 13 de febrero de 2024
- 1.0.63269 - Versión actual de la pista: publicada el 13 de febrero de 2024
- 1.0.63215 - Versión de Amazon Redshift sin servidor: publicada el 12 de febrero de 2024
- 1.0.63205 - Versión actual de la pista: publicada el 12 de febrero de 2024
- 1.0.63030 - Versión de Amazon Redshift sin servidor: publicada el 7 de febrero de 2024
- 1.0.62913 - Versión actual de la pista: publicada el 7 de febrero de 2024
- 1.0.62922 - Versión de Amazon Redshift sin servidor: publicada el 5 de febrero de 2024
- 1.0.62878 - Versión actual de la pista: publicada el 5 de febrero de 2024
- 1.0.62698 - Versión de Amazon Redshift sin servidor: publicada el 31 de enero de 2024
- 1.0.62614 - Versión actual de la pista: publicada el 31 de enero de 2024
- 1.0.61687 - Versión de Amazon Redshift sin servidor: publicada el 5 de enero de 2024
- 1.0.61678 - Versión actual de la pista: publicada el 5 de enero de 2024
- 1.0.61567 - Versión de Amazon Redshift sin servidor: publicada el 31 de diciembre de 2023
- 1.0.61559 - Versión actual de la pista: publicada el 31 de diciembre de 2023
- 1.0.61430 - Versión de Amazon Redshift sin servidor: publicada el 29 de diciembre de 2023
- 1.0.61395 - Versión actual de la pista: publicada el 29 de diciembre de 2023

Nuevas características y mejoras en este parche

- Cambia CURRENT_USER para que deje de truncar el nombre de usuario devuelto en 64 caracteres.
- Añade la posibilidad de aplicar políticas de enmascaramiento de datos en las vistas estándar y en las vistas de enlace tardío.
- Añade la posibilidad de aplicar el enmascaramiento dinámico de datos (DDM) a los atributos escalares de las columnas de tipos de datos SUPER.
- Añade la función SQL OBJECT_TRANSFORM. Para obtener más información, consulte Función OBJECT_TRANSFORM en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Añade la posibilidad de aplicar un control de acceso detallado de AWS Lake Formation a sus datos anidados y realizar consultas con el análisis de lagos de datos de Amazon Redshift.

- Añade el tipo de datos INTERVAL.
- Añade CONTINUE_HANDLER, que es un tipo de controlador de excepciones que controla el flujo de un procedimiento almacenado. Al usarlo, puedes atrapar y administrar excepciones sin finalizar el bloque de instrucciones existente.
- Añade la posibilidad de definir permisos para un ámbito (esquema o base de datos) además de los objetos individuales. De este modo, se puede otorgar un permiso a los usuarios y roles en todos los objetos actuales y futuros del ámbito.
- Añade la posibilidad de crear una base de datos a partir de un recurso compartido de datos con permisos que permitan a los administradores del lado del consumidor otorgar permisos individuales sobre los objetos compartidos de la base de datos a los usuarios y roles del lado del consumidor.
- Añade compatibilidad con el tipo de datos de retorno SUPER de los modelos BYOM remotos. Esto amplía la gama de modelos de SageMaker aceptados para incluir aquellos con formatos de devolución más complejos.
- Cambia las funciones externas para convertir ahora implícitamente números con o sin partes fraccionarias en el tipo de datos numéricos de la columna. En las columnas int2, int4 e int8, se aceptan números con dígitos fraccionarios truncándolos, a menos que el número esté fuera del rango. En las columnas float4 y float8, se aceptan números sin dígitos fraccionarios.
- Agrega tres funciones espaciales que funcionan con el sistema de cuadrícula de indexación geoespacial jerárquico H3: H3_FromLongLat, H3_FromPoint, and H3_Polyfill.

Parche 179 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.62317 - Versión de Amazon Redshift sin servidor: publicada el 29 de enero de 2024
- 1.0.62312 - Versión final de la pista: publicada el 29 de enero de 2024
- 1.0.61631 - Versión de Amazon Redshift sin servidor: publicada el 5 de enero de 2024
- 1.0.61626 - Versión actual de la pista: publicada el 5 de enero de 2024
- 1.0.61191 - Versión actual de la pista: publicada el 16 de diciembre de 2023
- 1.0.61150 - Versión de Amazon Redshift sin servidor: publicada el 16 de diciembre de 2023
- 1.0.60982 - Versión de Amazon Redshift sin servidor: publicada el 13 de diciembre de 2023
- 1.0.60854 - Versión actual de la pista: publicada el 10 de diciembre de 2023
- 1.0.60354 - Versión de Amazon Redshift sin servidor: publicada el 22 de noviembre de 2023

- 1.0.60353 - Versión actual de la pista: publicada el 21 de noviembre de 2023
- 1.0.60293 - Versión de Amazon Redshift sin servidor: publicada el 21 de noviembre de 2023
- 1.0.60292 - Versión actual de la pista: publicada el 22 de noviembre de 2023
- 1.0.60161 - Versión de Amazon Redshift sin servidor: publicada el 18 de noviembre de 2023
- 1.0.60140 - Versión actual de la pista: publicada el 18 de noviembre de 2023
- 1.0.60139 - Versión de Amazon Redshift sin servidor: publicada el 18 de noviembre de 2023
- 1.0.59947 - Versión de Amazon Redshift sin servidor: publicada el 16 de noviembre de 2023
- 1.0.59945 - Versión actual de la pista: publicada el 16 de noviembre de 2023
- 1.0.59118 - Versión de Amazon Redshift sin servidor: publicada el 9 de noviembre de 2023
- 1.0.59117 - Versión actual de la pista: publicada el 9 de noviembre de 2023

Nuevas características y mejoras en este parche

- Añade compatibilidad para que los usuarios federados con los permisos adecuados puedan ver las vistas del sistema de enmascaramiento de datos dinámico y de seguridad en el nivel de la fila, que incluyen:
  - SVV_ATTACHED_MASKING_POLICY
  - SVV_MASKING_POLICY
  - SVV_RLS_ATTACHED_POLICY
  - SVV_RLS_POLICY
  - SVV_RLS_RELATION
- Añade una funcionalidad que permite que una consulta que solo contiene funciones escalares en la cláusula FROM ahora genere un error.
- Añade las instrucciones CREATE TABLE AS (CTAS) con la funcionalidad de tablas de destino permanentes a los clústeres de escalado simultáneo. Los clústeres de escalado simultáneo ahora admiten más consultas.
- Añade las siguientes tablas del sistema para realizar un seguimiento del estado de redistribución de las tablas después de ejecutar la versión clásica de redimensionamiento en los clústeres RA3:
  - La tabla del sistema SYS_RESTORE_STATE muestra la evolución de la redistribución en el nivel de tabla.
  - La tabla del sistema SYS_RESTORE_LOG muestra el rendimiento histórico de la redistribución de datos.

- Mejora la minimización de la inclinación de los segmentos en las tablas EVEN después de ejecutar el redimensionamiento clásico en los tipos de nodo RA3. Esto también se aplica a los clústeres del parche 178 que ejecutaban el redimensionamiento clásico.
- Añade compatibilidad con UNLOAD con EXTENSION en los clústeres de escalado simultáneo.
- Mejora el rendimiento de las consultas que contienen UDF de λ en las uniones HashJoins y NestLoop.
- Mejora el rendimiento del redimensionamiento elástico en los tipos de nodo RA3.
- Mejora el rendimiento de las consultas de uso compartido de datos.
- Mejora el rendimiento de las consultas de análisis iniciadas manualmente en grupos de trabajo sin servidor y clústeres aprovisionados redimensionados de forma elástica.
- Mejora el rendimiento de las consultas WLM automáticas con una mejor predicción de los recursos en la administración de cargas de trabajo.
- Elimina la funcionalidad de lanzar clústeres en las VPC de tenencia dedicada. Este cambio no afecta a la tenencia de ninguna instancia de EC2 en la VPC. Puede modificar la tenencia de la VPC de forma predeterminada con el comando `modify-vpc-tenancy` de la AWS CLI.
- Ahora se admite la actualización manual de la vista materializada en los clústeres de escalado simultáneo aprovisionados y en la computación con escalado automático sin servidor.
- Añade compatibilidad con los literales INTERVAL a la función EXTRACT. Por ejemplo, `EXTRACT('hours' from Interval '50 hours')` devuelve 2 porque 50 horas se interpretan como 2 días y 2 horas, y se extrae el componente de hora de 2.

Revisión 178 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.63327 - Versión actual de la pista: publicada el 9 de febrero de 2024
- 1.0.63313 - Versión final de la pista: publicada el 9 de febrero de 2024
- 1.0.60977 - Versión actual de la pista: publicada el 15 de diciembre de 2023
- 1.0.59596 - Versión actual de la pista: publicada el 9 de noviembre de 2023
- 1.0.58593 - Versión de Amazon Redshift sin servidor: publicada el 23 de octubre de 2023
- 1.0.58558 - Versión actual de la pista: publicada el 23 de octubre de 2023
- 1.0.57864 - Versión actual de la pista: publicada el 12 de octubre de 2023

- 1.0.57850 - Versión de Amazon Redshift sin servidor: publicada el 12 de octubre de 2023
- 1.0.56952 - Versión actual de la pista: publicada el 25 de septiembre de 2023
- 1.0.56970 - Versión de Amazon Redshift sin servidor: publicada el 25 de septiembre de 2023

Nuevas características y mejoras en este parche

- Amazon Redshift ha mejorado ahora el rendimiento de las consultas de uso compartido de datos al acelerar la actualización de metadatos en las instancias consumidoras mientras se producen cambios simultáneos de datos en la instancia productora.
- Agrega compatibilidad con la actualización automática e incremental de vistas materializadas en instancias consumidoras de uso compartido de datos de Amazon Redshift cuando las tablas base de la vista materializada hacen referencia a los datos compartidos.
- Agrega compatibilidad para almacenar objetos grandes de hasta 16 MB de tamaño en el tipo de datos SUPER. Al ingesta desde archivos de origen JSON, PARQUET, TEXTO y CSV, puede cargar datos semiestructurados o documentos como valores en el tipo de datos SUPER, de hasta 16 MB.
- Agrega compatibilidad con el cambio de tamaño elástico para escalar hacia y desde un clúster de Amazon Redshift RA3 de un solo nodo.
- Los clústeres RA3 de un solo nodo de Amazon Redshift ya pueden beneficiarse de las mejoras de cifrado, que reducen el tiempo total de cifrado y mejoran la disponibilidad del almacenamiento de datos durante el proceso de cifrado.
- Mejora la compatibilidad con las consultas al anular la anidación y anular la rotación de los datos almacenados en el tipo de datos SUPER.
- Mejora el rendimiento de la actualización de vistas materializadas con tipos de datos SUPER.
- Agrega soporte para agregar literales INTERVAL con la función ANY_VALUE.
- La ingesta de streaming ahora admite el siguiente nuevo comando SQL para purgar datos de flujo: `DELETE FROM streaming_materialized_views WHERE <where filter clause>`.
- La función DECODE reemplaza un valor específico por otro valor específico o por un valor predeterminado, según el resultado de una condición de igualdad. DECODE ahora requiere los tres parámetros siguientes:
  - expresión
  - buscar
  - resultado

- Agrega funcionalidad a los procedimientos almacenados para permitir la captura de errores de conversión de tipo de datos por desbordamiento de datos y el manejo dentro de un bloque de manejo de excepciones.
- Ahora recibirá un error al consultar la seguridad de nivel de fila o las relaciones protegidas por enmascaramiento de datos dinámico si cambia enable_case_sensitive_identifier para que sea diferente de la configuración predeterminada de la sesión. Además, la siguiente configuración se bloquea cuando se aplican políticas de seguridad de nivel de fila o de enmascaramiento de datos dinámicos en su clúster aprovisionado o espacio de nombres sin servidor:

  ```
  ALTER USER <current_user> SET case-sensitive identifier.
  ```
- El comando MERGE admite ahora una sintaxis simplificada que solo requiere la tabla de destino y origen. Para obtener más información, consulte MERGE en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Agrega soporte para asociar políticas de enmascaramiento de datos dinámicas idénticas a varios usuarios o roles con la misma prioridad, o sin especificar la prioridad.
- Ahora puede especificar COLLATION al agregar una nueva columna mediante ALTER TABLE ADD COLUMN.
- Soluciona un problema que retrasa la aplicación de las reglas de QMR en clústeres con escalado de simultaneidad y Amazon Redshift sin servidor.
- La consulta federada de Amazon Redshift ha ampliado la compatibilidad de la inserción de la zona horaria con la marca temporal en Amazon RDS para PostgreSQL y Amazon Aurora PostgreSQL.
- Ahora puede utilizar nombres de bases de datos de Amazon RDS para MySQL y Aurora MySQL que empiecen por dígitos con consultas federadas.
- Agrega la vista SYS_ANALYZE_HISTORY, que contiene los detalles de registro de las operaciones ANALYZE.
- Agrega la vista SYS_ANALYZE_COMPRESSION_HISTORY, que contiene detalles de registro para las operaciones de análisis de compresión durante los comandos COPY o ANALYZE COMPRESSION.
- Agrega la vista SYS_SESSION_HISTORY, que contiene detalles de registro relacionados con las sesiones activas, históricas y reiniciadas.
- Agrega la vista SYS_TRANSACTION_HISTORY, que contiene detalles de registro relacionados con el análisis del nivel de transacción que proporciona el tiempo empleado en la confirmación, el número datasha de bloques confirmados y el nivel de aislamiento.

- Agrega la vista SVV_REDSHIFT_SCHEMA_QUOTA, que contiene registros relacionados con las cuotas y la utilización actual del disco para cada esquema de una base de datos.
- Agrega la vista SYS_PROCEDURE_CALL, que contiene registros relacionados con las llamadas a procedimientos almacenados, incluida la hora de inicio, la hora de finalización, el estado de la llamada al procedimiento almacenado y la jerarquía de llamadas para las llamadas a procedimientos almacenados anidados.
- Agrega la vista SYS_CROSS_REGION_DATASHARING_USAGE, que contiene registros relacionados con el seguimiento del uso compartido de datos entre regiones.
- Agrega la vista SYS_PROCEDURE_MESSAGES, que contiene registros relacionados con el seguimiento de la información sobre los mensajes de procedimientos almacenados registrados.
- Agrega la vista SYS_UDF_LOG, que contiene registros relacionados con el seguimiento de los mensajes de registro del sistema procedentes de llamadas a funciones definidas por el usuario, errores, advertencias o trazas, según corresponda.
- Agrega las nuevas columnas IS_RECURSIVE, IS_NESTED, S3LIST_TIME y GET_PARTITION_TIME a SYS_EXTERNAL_QUERY_DETAIL.
- Añade MaxRPU, una nueva configuración de control de costos de computación para Redshift sin servidor. Con MaxRPU, puede especificar un umbral de computación superior para controlar los costos del almacenamiento de datos en diferentes momentos seleccionando el nivel de computación máximo que puede escalar Redshift sin servidor por grupo de trabajo.
- Corrige el resultado del literal INTERVAL con cadenas de intervalos numéricos. Por ejemplo, un intervalo que especifique `INTERVAL '1' YEAR` ahora devuelve `1 YEAR` en lugar de `"00:00:00`. Además, el resultado del literal INTERVAL se trunca al componente INTERVAL más pequeño especificado. Por ejemplo, `INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE` se trunca en `1 day 01:01:00`.

Revisión 177 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.57922 - Versión actual de la pista: publicada el 12 de octubre de 2023
- 1.0.57799 - Versión de Amazon Redshift sin servidor: publicada el 10 de octubre de 2023
- 1.0.57798 - Versión actual de la pista: publicada el 10 de octubre de 2023
- 1.0.57085 - Versión final de la pista: publicada el 26 de septiembre de 2023
- 1.0.56899 - Versión de Amazon Redshift sin servidor: publicada el 21 de septiembre de 2023

- 1.0.56754 - Versión actual de la pista: publicada el 21 de septiembre de 2023
- 1.0.56242 - Versión actual de la pista: publicada el 11 de septiembre de 2023
- 1.0.55539 - Versión de Amazon Redshift sin servidor: publicada el 28 de agosto de 2023
- 1.0.55524 - Versión actual de la pista: publicada el 28 de agosto de 2023
- 1.0.54899 - Versión actual de la pista: publicada el 15 de agosto de 2023
- 1.0.54899 - Versión actual de la pista: publicada el 14 de agosto de 2023
- 1.0.54899 - Versión actual de la pista: publicada el 15 de agosto de 2023
- 1.0.54239 - Versión actual de la pista: publicada el 3 de agosto de 2023
- 1.0.54321 - Versión de Amazon Redshift sin servidor: publicada el 3 de agosto de 2023

Nuevas características y mejoras en este parche

- Agrega la vista SYS_MV_STATE, que contiene una fila para cada transición de estado de una vista materializada. SYS_MV_STATE puede utilizarse para monitorear la actualización de la máquina para instancias aprovisionadas de Amazon Redshift sin servidor y Amazon Redshift.
- Agrega la vista SYS_USERLOG, que registra los detalles de los cambios realizados en un usuario de la base de datos para Crear usuario, Eliminar usuario, Modificar usuario (cambiar nombre), Modificar usuario (modificar propiedades).
- Agrega la vista SYS_COPY_REPLACEMENTS, que muestra un registro de los momentos en que se reemplazaron caracteres UTF-8 no válidos por el comando COPY con la opción ACCEPTINVCHARS.
- Agrega la vista SYS_SPATIAL_SIMPLIFY, que contiene información sobre objetos de geometría espacial simplificada mediante el comando COPY.
- Agrega la vista SYS_VACUUM_HISTORY, que puede utilizar para ver los detalles y resultados de las operaciones de VACUUM.
- Agrega la vista SYS_SCHEMA_QUOTA_VIOLATIONS para registrar la incidencia, marca temporal, XID y otra información útil cuando se excede una cuota de esquema.
- Agrega la vista SYS_RESTORE_STATE, que puede utilizar para monitorear el progreso de la redistribución de cada tabla del clúster durante el cambio de tamaño clásico asíncrono.
- Agrega la vista SYS_EXTERNAL_QUERY_ERROR, que devuelve información sobre los errores de análisis de Redshift Spectrum.

- Agrega el parámetro de etiqueta al comando CREATE MODEL, por lo que ahora puede hacer un seguimiento de los costos de entrenamiento con los trabajos de entrenamiento de piloto automático.
- Agrega nombres de dominio personalizados (CNAME) para los clústeres de Amazon Redshift.
- Agrega compatibilidad previa con Apache Iceberg, lo que permite a los clientes ejecutar consultas analíticas en tablas de Apache Iceberg en Amazon Redshift.
- Agrega compatibilidad para utilizar roles de usuario con grupos de parámetros en la administración de la carga de trabajo (WLM).
- Agrega soporte para el montaje automático de AWS Glue Data Catalog, lo que facilita a los clientes la ejecución de consultas en sus lagos de datos.
- Agrega una funcionalidad por la que utilizar funciones de agrupación sin una cláusula GROUP BY o utilizar operaciones de agrupación en una cláusula WHERE provoca un error.
- Agrega funcionalidad a los procedimientos almacenados para permitir la captura de errores de división por cero y su control dentro de un bloque de control de excepciones.
- Corrige un error que impedía que las consultas utilizaran el escalado de simultaneidad para escribir datos en las tablas cuando la tabla de origen es una tabla de recursos compartidos de datos.
- Corrige el identificador que distingue entre mayúsculas y minúsculas documentado en enable_case_sensitive_identifier para que ahora funcione con las instrucciones MERGE.
- Corrige el error por el que una consulta de la función pg_get_late_binding_view_cols() podía ser omitida ocasionalmente. Ahora siempre puede cancelar este tipo de consultas.
- Mejora el rendimiento de las consultas de uso compartido de datos que se ejecutan en los consumidores cuando se ejecutan trabajos de limpieza en el productor.
- Mejora el rendimiento de las consultas de compartición de datos y escalado de simultaneidad, especialmente con cambios de datos simultáneos en el productor o cuando se descarga en una instancia de escalado de simultaneidad adjunta al consumidor.

Parche 176 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.56738 - Versión final de la pista: publicada el 21 de septiembre de 2023
- 1.0.55837 - Versión final de la pista: publicada el 11 de septiembre de 2023

- 1.0.54776 - Versión actual de la pista: publicada el 15 de agosto de 2023
- 1.0.54052 - Versión actual de la pista: publicada el 26 de julio de 2023
- 1.0.53642 - Versión de Amazon Redshift sin servidor: publicada el 20 de julio de 2023
- 1.0.53301 - Versión actual de la pista: publicada el 20 de julio de 2023
- 1.0.52943 - Versión de Amazon Redshift sin servidor: publicada el 7 de julio de 2023
- 1.0.52931 - Versión actual de la pista: publicada el 7 de julio de 2023
- 1.0.52194 - Versión de Amazon Redshift sin servidor: publicada el 21 de junio de 2023
- 1.0.51986 - Versión actual de la pista: publicada el 16 de junio de 2023
- 1.0.51594 - Versión actual de la pista: publicada el 9 de junio de 2023

Nuevas características y mejoras en este parche

- Se ha mejorado el manejo de errores al escribir GROUP BY () para un conjunto de agrupaciones vacío. Esto se ignoró anteriormente y ahora devuelve un error del analizador.
- Mejoras de rendimiento para actualizar de forma incremental las vistas materializadas con columnas SUPER.
- ALTER TABLE <target_tbl> APPEND FROM <streaming_mv> - (ATA) El comando SQL ahora permite mover todos los registros de una vista materializada (MV) de streaming como origen, además de las tablas como origen, a una tabla de destino. La compatibilidad con ATA en las máquinas virtuales de streaming permite a los usuarios purgar rápidamente todos los registros de una máquina virtual de transmisión moviéndolos a otra tabla para gestionar el crecimiento de los datos.
- TRUNCATE <streaming_mv> - El comando SQL ahora admite truncar todos los registros en una vista materializada (MV) de streaming, además de con las tablas. TRUNCATE elimina todos los registros de la máquina virtual de streaming, mientras deja intacta la estructura de la máquina virtual de streaming. La ejecución de TRUNCATE en las máquinas virtuales de streaming permite a los clientes purgar rápidamente todos los registros de una máquina virtual de streaming para administrar el crecimiento de los datos.
- Se ha agregado la funcionalidad de la cláusula QUALIFY al comando SELECT.
- Compatibilidad de machine learning de Redshift para la previsión de series temporales mediante la integración con Amazon Forecast.
- Se admite el montaje automático de AWS Glue Data Catalog para simplificar la consulta de un lago de datos sin pasos adicionales para crear referencias de esquemas externas.

- Ahora se admite la modificación de una política de RLS. Consulte la documentación para obtener más información en ALTER RLS POLICY.
- Las UDF de Lambda ahora admiten el parámetro de volatilidad de la función STABLE en la instrucción CREATE FUNCTION. Cuando se utiliza el parámetro STABLE en la instrucción CREATE FUNCTION y se llama a la UDF de Lambda varias veces con los mismos argumentos, se reduce el número esperado de invocaciones de la función de UDF de Lambda. La categoría de volatilidad de la función STABLE se explica con más detalle en los parámetros CREATE FUNCTION.
- Múltiples mejoras en el rendimiento de la UDF de Lambda. En concreto, se ha mejorado la compatibilidad con el procesamiento por lotes de registros al consultar una tabla protegida por una política de seguridad a nivel de fila (RLS).
- Reducción del tiempo total de cifrado de los clústeres RA3 de Amazon Redshift y mejora de la disponibilidad del almacenamiento de datos durante el cifrado. Para obtener más información, consulte Cifrado de base de datos de Amazon Redshift.
- Se ha agregado una nueva vista del sistema SYS_MV_REFRESH_HISTORY a Redshift. La vista SYS_MV_REFRESH_HISTORY contiene una fila para la actividad de actualización de las vistas materializadas. Con SYS_MV_REFRESH_HISTORY, puede comprobar el historial de actualizaciones de las vistas materializadas. SYS_MV_REFRESH_HISTORY está visible para todos los usuarios. Los superusuarios pueden ver todas las filas; los usuarios normales solo pueden ver sus datos.

  Se ha agregado una nueva columna SPILLED_BLOCK_LOCAL_DISK a la vista del sistema SYS_QUERY_DETAIL. La nueva columna SPILLED_BLOCK_LOCAL_DISK ayuda a los clientes a determinar los bloques vertidos en el disco local. Puede utilizar SYS_QUERY_DETAIL para visualizar los detalles de las consultas en el nivel de paso. SYS_QUERY_DETAIL es visible para todos los usuarios. Los superusuarios pueden ver todas las filas; los usuarios normales solo pueden ver los metadatos a los que tienen acceso.
- Se ha agregado una nueva vista del sistema, SYS_QUERY_TEXT, a Amazon Redshift sin servidor y se ha aprovisionado Amazon Redshift. La vista SYS_QUERY_TEXT es similar a SVL_STATEMENTTEXT para los clústeres aprovisionados. Utilice la columna `sequence` de la vista SYS_QUERY_TEXT para obtener el texto completo de la instrucción SQL.

Parche 175 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.53064 - Versión actual de la pista: publicada el 7 de julio de 2023
- 1.0.51973 - Versión actual de la pista: publicada el 16 de junio de 2023
- 1.0.51781 - Versión actual de la pista: publicada el 10 de junio de 2023
- 1.0.51314 - Versión de Amazon Redshift sin servidor: publicada el 3 de junio de 2023
- 1.0.51304 - Versión actual de la pista: publicada el 2 de junio de 2023
- 1.0.50708 - Versión actual de la pista: publicada el 19 de mayo de 2023
- 1.0.50300 - Versión actual de la pista: publicada el 8 de mayo de 2023
- 1.0.49710 - Versión de Amazon Redshift sin servidor: publicada el 28 de abril 2023
- 1.0.49676 - Versión actual de la pista: publicada el 28 de abril de 2023

Nuevas características y mejoras en este parche

- Correcciones de errores menores.
- La ingesta de streaming de Amazon Redshift ahora admite la ingesta de streaming entre regiones, donde el tema de origen Amazon Kinesis Data Streams (KDS) o Amazon Managed Streaming for Apache Kafka (MSK) puede estar ubicado en una región de AWS distinta de la región de AWS en la que se encuentra su almacenamiento de datos de Amazon Redshift. Se ha revisado la documentación de Introducción a la ingesta de streaming de Amazon Kinesis Data Streams donde se explica cómo se utiliza la palabra clave REGION.
- Ajuste del horario de verano de Egipto.
- Se han mejorado los horarios generales de cifrado de los clústeres RA3.

Revisión 174 de Amazon Redshift

1.0.51296: publicado el 2 de junio de 2023

Liberar para la pista de seguimiento. Sin notas de la versión.

1.0.50468: publicada el 12 de mayo de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.49780, 1.0.49868 y 1.0.49997: publicadas el 28 de abril de 2023

Notas de la versión de esta versión:

- Se ha mejorado la compatibilidad con la agrupación en lotes para Lambda UDF.
- Agrupación en lotes incremental para Lambda UDF.
- Nuevo comando MERGE SQL para aplicar cambios en los datos de origen a las tablas de Amazon Redshift.
- Nueva función de enmascaramiento dinámico de datos para simplificar el proceso de protección de datos confidenciales en un almacenamiento de datos de Amazon Redshift.
- Nuevo control de acceso centralizado para compartir datos con Lake Formation que permite gestionar las concesiones de permisos, ver los controles de acceso y auditar los permisos en las tablas y vistas de los recursos compartidos de datos de Amazon Redshift mediante las API de Lake Formation y la consola de AWS.
- Ajuste del horario de verano de Egipto.

1.0.49087: publicado el 12 de abril de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.48805: publicado el 5 de abril de 2023

Notas de la versión de esta versión:

- Amazon Redshift incorporó mejoras adicionales en el rendimiento de las consultas que usan muchas cadenas con BYTEDICT, una nueva codificación de compresión en Amazon Redshift que acelera entre 5 y 63 veces el procesamiento de datos basados en cadenas en comparación con codificaciones de compresión alternativas como LZO o ZSTD. Para obtener más información sobre esta característica, consulte Codificación por diccionario de bytes en la Guía para desarrolladores de bases de datos de Amazon Redshift.

1.0.48004: publicado el 17 de marzo de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.47470: publicado el 11 de marzo de 2023

Notas de la versión de esta versión:

- Mejora el rendimiento de consultas en `pg_catalog.svv_table_info`. También agrega una nueva columna `create_time`. Al crear una tabla, esta columna almacena la marca de fecha/hora en UTC.
- Agrega compatibilidad para especificar el tiempo de espera de nivel de sesión en la consulta federada.

Parche 173 de Amazon Redshift

1.0.49788: publicada el 28 de abril de 2023

Notas de la versión de esta versión:

- Ajuste del horario de verano de Egipto.

1.0.49074: publicado el 12 de abril de 2023

Notas de la versión de esta versión:

- Configuración de la zona horaria actualizada a la versión 2022g de la biblioteca IANA.

1.0.48766: publicado el 5 de abril de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.48714: publicado el 5 de abril de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.48022: publicado el 17 de marzo de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.47357: publicado el 7 de marzo de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.46987: publicado el 24 de febrero de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.46806: publicado el 18 de febrero de 2023

Versión de mantenimiento. Sin notas de la versión.

1.0.46607: publicado el 13 de febrero de 2023

Notas de la versión de esta versión:

- Ahora convertimos automáticamente las tablas con claves de clasificación intercaladas establecidas manualmente en claves de clasificación compuestas si su estilo de distribución se ha establecido a DISTSTYLE KEY, para mejorar el rendimiento de estas tablas. Esto se realiza en el momento de restaurar una instantánea en Amazon Redshift sin servidor.

1.0.45698: publicado el 20 de enero de 2023

Notas de la versión de esta versión:

- Agrega un parámetro de extensión de archivo al comando UNLOAD para que las extensiones de archivo se agreguen automáticamente a los nombres de archivo.
- Admite la protección de objetos protegidos por RLS de forma predeterminada al agregarlos a un recurso compartido de datos o si ya forman parte de un recurso compartido de datos. Los administradores ahora pueden desactivar el RLS para los recursos compartidos de datos a fin de permitir a los consumidores acceder al objeto protegido.
- Agrega nuevas tablas de sistema para el monitoreo: `SVV_ML_MODEL_INFO`, `SVV_MV_DEPENDENCY` y `SYS_LOAD_DETAIL`. También agrega las columnas `data_skewness` y `time_skewness` a la tabla del sistema `SYS_QUERY_DETAIL`.

Parche 172 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.46534: publicado el 18 de febrero de 2023
- 1.0.46523: publicado el 13 de febrero de 2023
- 1.0.46206: publicado el 1 de febrero de 2023
- 1.0.45603: publicado el 20 de enero de 2023
- 1.0.44924: publicado el 19 de diciembre de 2022

- 1.0.44903: publicado el 18 de diciembre de 2022
- 1.0.44540: publicado el 13 de diciembre de 2022
- 1.0.44126: publicado el 23 de noviembre de 2022
- 1,0.43980: publicado el 17 de noviembre de 2022

Nuevas características y mejoras en este parche

- Las tablas creadas por CTAS son AUTO de forma predeterminada.
- Agrega compatibilidad con la seguridad a nivel de fila (RLS) en las vistas materializadas.
- Aumenta el tiempo de espera de S3 para mejorar el uso compartido de datos entre regiones.
- Agrega la nueva función espacial `ST_GeomFromGeohash`.
- Mejora la selección automática de la clave de distribución a partir de claves primarias compuestas para mejorar el rendimiento inmediato.
- Agrega la clave principal automática a la clave de distribución para tablas con claves primarias compuestas, lo que mejora el rendimiento inmediato.
- Mejora el escalado de simultaneidad para permitir que se escalen más consultas, incluso cuando los datos cambian.
- Mejora el rendimiento de las consultas de uso compartido de datos.
- Agrega métricas de probabilidad de machine learning para modelos de clasificación.
- Agrega nuevas tablas de sistema para la supervisión: `SVV_USER_INFO`, `SVV_MV_INFO`, `SYS_CONNECTION_LOG`, `SYS_DATASHARE_USAGE_PRODUCER`, `SYS_DATASHARE_USAGE_CONSUMER` y `SYS_DATASHARE_CHANGE_LOG`.
- Agrega soporte para consultar columnas VARBYTE en tablas externas para los tipos de archivos Parquet y ORC.

Parche 171 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.43931: publicado el 16 de noviembre de 2022
- 1.0.43551: publicado el 5 de noviembre de 2022
- 1.0.43331: publicado el 29 de septiembre de 2022

- 1.0.43029: publicado el 26 de septiembre de 2022

Nuevas características y mejoras en este parche

- Compatibilidad con CONNECT BY: agrega compatibilidad con el constructo CONNECT BY de SQL, lo que le permite consultar de forma recursiva los datos jerárquicos de su almacenamiento de datos basándose en la relación principal-secundario en ese conjunto de datos.

Parche 170 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.43922: publicado el 21 de noviembre de 2022
- 1.0.43573: publicado el 7 de noviembre de 2022
- 1.0.41881: publicado el 20 de septiembre de 2022
- 1.0.41465: publicado el 7 de septiembre de 2022
- 1.0.40083: publicado el 27 de julio de 2022

Nuevas características y mejoras en este parche

- ST_GeomFromGeojSON: construye un objeto de geometría espacial de Amazon Redshift a partir de VARCHAR en la representación de GeoJSON.

Parche 169 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.41050: publicado el 7 de septiembre de 2022
- 1.0.40083: publicado el 16 de julio de 2022
- 1.0.39734: publicado el 7 de julio de 2022
- 1.0.39380: publicado el 23 de junio de 2022
- 1.0.39251: publicado el 15 de junio de 2022
- 1.0.39009: publicado el 8 de junio de 2022

Nuevas características y mejoras en este parche

- Agrega un rol como parámetro del comando Alter Default Privileges para admitir el control de acceso basado en roles.
- Agrega el parámetro ACCEPTINVCHARS para admitir el reemplazo de caracteres UTF-8 no válidos al copiar desde archivos Parquet y ORC.
- Agrega la función OBJECT(k,v) para crear objetos SUPER a partir de pares clave y valor.

Parche 168 de Amazon Redshift

Versiones de clúster de este parche:

- 1.0.38698: publicado el 25 de mayo de 2022
- 1.0.38551: publicado el 20 de mayo de 2022
- 1.0.38463: publicado el 18 de mayo de 2022
- 1.0.38361: publicado el 13 de mayo de 2022
- 1.0.38199: publicado el 9 de mayo de 2022
- 1.0.38112: publicado el 6 de mayo de 2022
- 1.0.37684: publicado el 20 de abril de 2022

Nuevas características y mejoras en este parche

- Agrega compatibilidad con el tipo de modelo Linear Learner en Amazon Redshift ML.
- Agrega la opción SNAPSHOT para el nivel de aislamiento de transacciones SQL.
- Agrega `farmhashFingerprint64` como nuevo algoritmo de hash para datos `VARBYTE` y `VARCHAR`.
- Admite la función AVG en la actualización progresiva de las vistas materializadas.
- Admite subconsultas correlacionadas en tablas externas de Redshift Spectrum.
- Para mejorar el rendimiento de las consultas listas para usar, Amazon Redshift elige automáticamente una única clave principal de columna para tablas específicas como clave de distribución.

Ejemplos de código de Amazon Redshift usando SDK de AWS

En los siguientes ejemplos de código, se muestra cómo utilizar Amazon Redshift con un kit de desarrollo de software (SDK) de AWS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica llamando a varias funciones dentro del mismo servicio.

Los ejemplos entre servicios son aplicaciones de muestra que funcionan en varios Servicios de AWS.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Introducción

Hello Amazon Redshift

En el siguiente ejemplo de código se muestra cómo empezar a utilizar Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import
 software.amazon.awssdk.services.redshift.paginators.DescribeClustersIterable;
```

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class HelloRedshift {

    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        RedshiftClient redshiftClient = RedshiftClient.builder()
            .region(region)
            .build();

        listClustersPaginator(redshiftClient);
    }

    public static void listClustersPaginator(RedshiftClient redshiftClient) {
        DescribeClustersIterable clustersIterable =
 redshiftClient.describeClustersPaginator();
        clustersIterable.stream()
            .flatMap(r -> r.clusters().stream())
            .forEach(cluster -> System.out
                .println(" Cluster identifier: " + cluster.clusterIdentifier() +
 " status = " + cluster.clusterStatus()));
    }
}
```

- Para obtener más información sobre la API, consulte describeClusters en la Referencia de la API de AWS SDK for Java 2.x.

Ejemplos de código

- Acciones de Amazon Redshift usando SDK de AWS
  - Cree un clúster de Amazon Redshift usando un SDK de AWS.
  - Creación de un clúster de Amazon Redshift mediante un SDK de AWS
  - Eliminar un clúster de Amazon Redshift usando un SDK de AWS.

- Descripción de una instrucción de consulta de Amazon Redshift mediante un SDK de AWS
- Descripción de clústeres mediante un SDK de AWS
- Obtención del resultado de la instrucción de Amazon Redshift mediante un SDK de AWS
- Inserción de datos en una tabla de Amazon Redshift mediante un SDK de AWS
- Modificar un clúster de Amazon Redshift usando un SDK de AWS
- Consulta de una tabla de Amazon Redshift mediante un SDK de AWS

- Escenarios de Amazon Redshift con SDK de AWS
  - Introducción a tablas, elementos y consultas de Amazon Redshift
- Ejemplos en diversos servicios de Amazon Redshift usando SDK de AWS
  - Crear un rastreador de artículos de Amazon Redshift

Acciones de Amazon Redshift usando SDK de AWS

Los siguientes ejemplos de código muestran cómo llevar a cabo acciones individuales de Amazon Redshift con los SDK de AWS. En estos fragmentos, se llama a la API de Amazon Redshift. Se trata de fragmentos de código de programas más grandes que se deben ejecutar en contexto. En cada ejemplo se incluye un enlace a GitHub, con instrucciones de configuración y ejecución del código.

Los ejemplos siguientes incluyen solo las acciones que se utilizan con mayor frecuencia. Para ver una lista completa, consulte la Referencia de la API de Amazon Redshift .

Ejemplos

- Cree un clúster de Amazon Redshift usando un SDK de AWS.
- Creación de un clúster de Amazon Redshift mediante un SDK de AWS
- Eliminar un clúster de Amazon Redshift usando un SDK de AWS.
- Descripción de una instrucción de consulta de Amazon Redshift mediante un SDK de AWS
- Descripción de clústeres mediante un SDK de AWS
- Obtención del resultado de la instrucción de Amazon Redshift mediante un SDK de AWS
- Inserción de datos en una tabla de Amazon Redshift mediante un SDK de AWS
- Modificar un clúster de Amazon Redshift usando un SDK de AWS
- Consulta de una tabla de Amazon Redshift mediante un SDK de AWS

Cree un clúster de Amazon Redshift usando un SDK de AWS.

Los siguientes ejemplos de código muestran cómo crear un clúster de Amazon Redshift.

CLI

AWS CLI

Crear un clúster con parámetros mínimos En este ejemplo, se crea un clúster con el conjunto mínimo de parámetros. De forma predeterminada, la salida es en JSON format.Command:

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
 mycluster
```

Resultado:

```
{
   "Cluster": {
      "NodeType": "dw.hs1.xlarge",
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
         {
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "default.redshift-1.0"
         } ],
      "ClusterSecurityGroups": [
         {
            "Status": "active",
            "ClusterSecurityGroupName": "default"
         } ],
      "AllowVersionUpgrade": true,
      "VpcSecurityGroups": \[],
      "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
      "AutomatedSnapshotRetentionPeriod": 1,
      "ClusterStatus": "creating",
      "ClusterIdentifier": "mycluster",
      "DBName": "dev",
      "NumberOfNodes": 2,
      "PendingModifiedValues": {
         "MasterUserPassword": "\****"
```

```
      }
   },
   "ResponseMetadata": {
      "RequestId": "7cf4bcfc-64dd-11e2-bea9-49e0ce183f07"
   }
}
```

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree el clúster.

```
   public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                    String masterUserPassword) {
       try {
           CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
               .clusterIdentifier(clusterId)
               .masterUsername(masterUsername)
               .masterUserPassword(masterUserPassword)
               .nodeType("ra3.4xlarge")
               .publiclyAccessible(true)
               .numberOfNodes(2)
               .build();

           CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
           System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

       } catch (RedshiftException e) {
```

```
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de la API de AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree el cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Cree el clúster.

```
// Import required AWS SDK clients and commands for Node.js
import { CreateClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME", // Required
  NodeType: "NODE_TYPE", //Required
  MasterUsername: "MASTER_USER_NAME", // Required - must be lowercase
  MasterUserPassword: "MASTER_USER_PASSWORD", // Required - must contain at least
 one uppercase letter, and one number
```

```
  ClusterType: "CLUSTER_TYPE", // Required
  IAMRoleARN: "IAM_ROLE_ARN", // Optional - the ARN of an IAM role with
 permissions your cluster needs to access other AWS services on your behalf, such
 as Amazon S3.
  ClusterSubnetGroupName: "CLUSTER_SUBNET_GROUPNAME", //Optional - the name of a
 cluster subnet group to be associated with this cluster. Defaults to 'default'
 if not specified.
  DBName: "DATABASE_NAME", // Optional - defaults to 'dev' if not specified
  Port: "PORT_NUMBER", // Optional - defaults to '5439' if not specified
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new CreateClusterCommand(params));
    console.log(
      "Cluster " + data.Cluster.ClusterIdentifier + " successfully created",
    );
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de la API de AWS SDK for JavaScript.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree el clúster.

```
suspend fun createCluster(clusterId: String?, masterUsernameVal: String?,
 masterUserPasswordVal: String?) {
```

```
    val clusterRequest = CreateClusterRequest {
        clusterIdentifier = clusterId
        masterUsername = masterUsernameVal
        masterUserPassword = masterUserPasswordVal
        nodeType = "ds2.xlarge"
        publiclyAccessible = true
        numberOfNodes = 2
    }

    RedshiftClient { region = "us-east-1" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.createCluster(clusterRequest)
        println("Created cluster ${clusterResponse.cluster?.clusterIdentifier}")
    }
}
```

- Para obtener información sobre la API, consulte CreateCluster en la Referencia de la API del SDK de AWS para Kotlin.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Creación de un clúster de Amazon Redshift mediante un SDK de AWS

En los siguientes ejemplos de código, se muestra cómo crear una tabla de Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
        try {
```

```
            ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .dbUser(userName)
                .database(databaseName)
                .sql("CREATE TABLE Movies ("
                    + "id INT PRIMARY KEY, "
                    + "title VARCHAR(100), "
                    + "year INT)")
                .build();

            redshiftDataClient.executeStatement(createTableRequest);
            System.out.println("Table created: Movies");

        } catch (RedshiftDataException e) {
            System.err.println("Error creating table: " + e.getMessage());
            System.exit(1);
        }
    }
```

- Para obtener información acerca de la API, consulte CreateTable en la referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Eliminar un clúster de Amazon Redshift usando un SDK de AWS.

Los siguientes ejemplos de código muestran cómo eliminar un clúster de Amazon Redshift.

CLI

AWS CLI

Eliminación de un clúster sin una instantánea final del clúster En este ejemplo, se elimina un clúster y se fuerza la eliminación de los datos, por lo que no se crea una instantánea final del clúster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-
snapshot
```

Eliminación de un clúster, lo que permite obtener una instantánea final del clúster En este ejemplo se elimina un clúster, pero especifica una instantánea final del clúster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-
snapshot-identifier myfinalsnapshot
```

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Eliminar el clúster.

```
   public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
       try {
           DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
                   .clusterIdentifier(clusterId)
                   .skipFinalClusterSnapshot(true)
                   .build();

           DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
           System.out.println("The status is " +
response.cluster().clusterStatus());

       } catch (RedshiftException e) {
           System.err.println(e.getMessage());
```

```
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de la API de AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree el cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Cree el clúster.

```
// Import required AWS SDK clients and commands for Node.js
import { DeleteClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  SkipFinalClusterSnapshot: false,
  FinalClusterSnapshotIdentifier: "CLUSTER_SNAPSHOT_ID",
};
```

```
const run = async () => {
  try {
    const data = await redshiftClient.send(new DeleteClusterCommand(params));
    console.log("Success, cluster deleted. ", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de la API de AWS SDK for JavaScript.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Eliminar el clúster.

```
suspend fun deleteRedshiftCluster(clusterId: String?) {

    val request = DeleteClusterRequest {
        clusterIdentifier = clusterId
        skipFinalClusterSnapshot = true
    }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val response = redshiftClient.deleteCluster(request)
        println("The status is ${response.cluster?.clusterStatus}")
    }
}
```

- Para obtener información sobre la API, consulte DeleteCluster en la Referencia de la API del SDK de AWS para Kotlin.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Descripción de una instrucción de consulta de Amazon Redshift mediante un SDK de AWS

En los siguientes ejemplos de código, se muestra cómo describir una instrucción de consulta de Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
       try {
           DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
                   .id(sqlId)
                   .build();

           String status;
           while (true) {
               DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
               status = response.statusAsString();
               System.out.println("..." + status);

               if (status.compareTo("FAILED") == 0 ) {
                   System.out.println("The Query Failed. Ending program");
```

```
                    System.exit(1);

                } else if (status.compareTo("FINISHED") == 0) {
                    break;
                }
                TimeUnit.SECONDS.sleep(1);
            }

            System.out.println("The statement is finished!");

        } catch (RedshiftDataException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte DescribeStatement en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Descripción de clústeres mediante un SDK de AWS

En los siguientes ejemplos de código se muestra cómo describir clústeres de Amazon Redshift.

CLI

AWS CLI

Obtención de una descripción de todos los clústeres En este ejemplo se devuelve una descripción de todos los clústeres de la cuenta. De forma predeterminada, la salida es en JSON format.Command:

```
aws redshift describe-clusters
```

Resultado:

```
{
```

```
    "Clusters": [
    {
       "NodeType": "dw.hs1.xlarge",
       "Endpoint": {
          "Port": 5439,
          "Address": "mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com"
       },
       "ClusterVersion": "1.0",
       "PubliclyAccessible": "true",
       "MasterUsername": "adminuser",
       "ClusterParameterGroups": [
          {
             "ParameterApplyStatus": "in-sync",
             "ParameterGroupName": "default.redshift-1.0"
          } ],
       "ClusterSecurityGroups": [
          {
             "Status": "active",
             "ClusterSecurityGroupName": "default"
          } ],
       "AllowVersionUpgrade": true,
       "VpcSecurityGroups": \[],
       "AvailabilityZone": "us-east-1a",
       "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
       "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
       "AutomatedSnapshotRetentionPeriod": 1,
       "ClusterStatus": "available",
       "ClusterIdentifier": "mycluster",
       "DBName": "dev",
       "NumberOfNodes": 2,
       "PendingModifiedValues": {}
    } ],
    "ResponseMetadata": {
       "RequestId": "65b71cac-64df-11e2-8f5b-e90bd6c77476"
    }
}
```

También puede obtener la misma información en formato de texto mediante la opción `--output text`. Comando:

`--output text` option.Command:

option.Command:

```
aws redshift describe-clusters --output text
```

Resultado:

```
dw.hs1.xlarge       1.0     true    adminuser       True    us-east-1a
 2013-01-22T21:59:29.559Z        sat:03:30-sat:04:00     1       available
 mycluster       dev     2
ENDPOINT    5439    mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com
in-sync     default.redshift-1.0
active      default
PENDINGMODIFIEDVALUES
RESPONSEMETADATA    934281a8-64df-11e2-b07c-f7fbdd006c67
```

- Para obtener información sobre la API, consulte DescribeClusters en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Describir el clúster.

```
   public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
       boolean clusterReady = false;
       String clusterReadyStr;
       System.out.println("Waiting for cluster to become available. This may
take a few mins.");
       try {
           DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
               .clusterIdentifier(clusterId)
               .build();
           long startTime = System.currentTimeMillis();
```

```
            // Loop until the cluster is ready.
            while (!clusterReady) {
                DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
                List<Cluster> clusterList = clusterResponse.clusters();
                for (Cluster cluster : clusterList) {
                    clusterReadyStr = cluster.clusterStatus();
                    if (clusterReadyStr.contains("available"))
                        clusterReady = true;
                    else {
                        long elapsedTimeMillis = System.currentTimeMillis() -
startTime;
                        long elapsedSeconds = elapsedTimeMillis / 1000;
                        long minutes = elapsedSeconds / 60;
                        long seconds = elapsedSeconds % 60;

                        System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
                        TimeUnit.SECONDS.sleep(5);
                    }
                }
            }

            long elapsedTimeMillis = System.currentTimeMillis() - startTime;
            long elapsedSeconds = elapsedTimeMillis / 1000;
            long minutes = elapsedSeconds / 60;
            long seconds = elapsedSeconds % 60;

            System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

        } catch (RedshiftException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte AWS SDK for Java 2.xDescribeClusters en la referencia de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree el cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Describir sus clústeres.

```
// Import required AWS SDK clients and commands for Node.js
import { DescribeClustersCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DescribeClustersCommand(params));
    console.log("Success", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Para obtener información sobre la API, consulte AWS SDK for JavaScriptDescribeClusters en la referencia de la API.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Describir el clúster.

```
suspend fun describeRedshiftClusters() {

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse =
 redshiftClient.describeClusters(DescribeClustersRequest {})
        val clusterList = clusterResponse.clusters

        if (clusterList != null) {
            for (cluster in clusterList) {
                println("Cluster database name is ${cluster.dbName}")
                println("Cluster status is ${cluster.clusterStatus}")
            }
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeClusters en la Referencia de la API del SDK de AWS para Kotlin.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Obtención del resultado de la instrucción de Amazon Redshift mediante un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo obtener el resultado de la instrucción.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Compruebe el resultado de la instrucción.

```
   public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
       try {
           GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
               .id(statementId)
               .build();

           // Extract and print the field values using streams.
           GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
           response.records().stream()
               .flatMap(List::stream)
               .map(Field::stringValue)
               .filter(value -> value != null)
               .forEach(value -> System.out.println("The Movie title field is "
+ value));

       } catch (RedshiftDataException e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Para ver la información de la API, consulte GetStatementResult en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Inserción de datos en una tabla de Amazon Redshift mediante un SDK de AWS

En los siguientes ejemplos de código, se muestra cómo insertar datos en una tabla de Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
       JsonParser parser = new JsonFactory().createParser(new File(fileName));
       com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
       Iterator<JsonNode> iter = rootNode.iterator();
       ObjectNode currentNode;
       int t = 0;
       while (iter.hasNext()) {
           if (t == number)
               break;
           currentNode = (ObjectNode) iter.next();
           int year = currentNode.get("year").asInt();
           String title = currentNode.get("title").asText();

           // Use SqlParameter to avoid SQL injection.
```

```
            List<SqlParameter> parameterList = new ArrayList<>();
            String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year);";

            // Create the parameters.
            SqlParameter idParam = SqlParameter.builder()
                .name("id")
                .value(String.valueOf(t))
                .build();

            SqlParameter titleParam= SqlParameter.builder()
                .name("title")
                .value(title)
                .build();

            SqlParameter yearParam = SqlParameter.builder()
                .name("year")
                .value(String.valueOf(year))
                .build();
            parameterList.add(idParam);
            parameterList.add(titleParam);
            parameterList.add(yearParam);

            try {
                ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                    .clusterIdentifier(clusterId)
                    .sql(sqlStatement)
                    .database(databaseName)
                    .dbUser(userName)
                    .parameters(parameterList)
                    .build();

                redshiftDataClient.executeStatement(insertStatementRequest);
                System.out.println("Inserted: " + title + " (" + year + ")");
                t++;

            } catch (RedshiftDataException e) {
                System.err.println("Error inserting data: " + e.getMessage());
                System.exit(1);
            }
        }
        System.out.println(t + " records were added to the Movies table. ");
    }
```

- Para obtener más información acerca de la API, consulte Insert en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Modificar un clúster de Amazon Redshift usando un SDK de AWS

En los siguientes ejemplos de código se muestra cómo modificar un clúster de Amazon Redshift.

CLI

AWS CLI

Asociación de un grupo de seguridad a un clúster En este ejemplo se muestra cómo asociar un grupo de seguridad de clúster al clúster especificado. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-
groups mysecuritygroup
```

Modificación del período de mantenimiento de un clúster Aquí se muestra cómo cambiar el período de mantenimiento semanal preferido de un clúster para que sea el período mínimo de cuatro horas, que comience los domingos a las 23:15 y termine los lunes a las 3:15. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-
maintenance-window Sun:23:15-Mon:03:15
```

Cambio de la contraseña maestra del clúster En este ejemplo se muestra cómo cambiar la contraseña maestra de un clúster. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password
 A1b2c3d4
```

- Para obtener información sobre la API, consulte ModifyCluster en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Modificar un clúster

```
   public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
       try {
           ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
                .clusterIdentifier(clusterId)
                .preferredMaintenanceWindow("wed:07:30-wed:08:00")
                .build();

           ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
           System.out.println("The modified cluster was successfully modified
and has "
                + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

       } catch (RedshiftException e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
   }
```

- Para obtener información sobre la API, consulte ModifyCluster en la referencia de la API de AWS SDK for Java 2.x.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree el cliente.

```
const { RedshiftClient } = require("@aws-sdk/client-redshift");
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Modificar un clúster

```
// Import required AWS SDK clients and commands for Node.js
import { ModifyClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

// Set the parameters
const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  MasterUserPassword: "NEW_MASTER_USER_PASSWORD",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new ModifyClusterCommand(params));
    console.log("Success was modified.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Para obtener información sobre la API, consulte ModifyCluster en la referencia de la API de AWS SDK for JavaScript.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Modificar un clúster

```
suspend fun modifyCluster(clusterId: String?) {
    val modifyClusterRequest = ModifyClusterRequest {
        clusterIdentifier = clusterId
        preferredMaintenanceWindow = "wed:07:30-wed:08:00"
    }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.modifyCluster(modifyClusterRequest)
        println("The modified cluster was successfully modified and has
 ${clusterResponse.cluster?.preferredMaintenanceWindow} as the maintenance
 window")
    }
}
```

- Para obtener información sobre la API, consulte ModifyCluster en la Referencia de la API de un SDK de AWS para Kotlin.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Consulta de una tabla de Amazon Redshift mediante un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo consultar una tabla de Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Consulte una tabla.

```
    public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                           String database,
                                           String dbUser,
                                           int year,
                                           String clusterId) {

        try {
            String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
            SqlParameter yearParam= SqlParameter.builder()
                .name("year")
                .value(String.valueOf(year))
                .build();

            ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .database(database)
                .dbUser(dbUser)
                .parameters(yearParam)
                .sql(sqlStatement)
                .build();

            ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
            return response.id();
```

```
        } catch (RedshiftDataException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }
```

- Para obtener detalles de la API, consulte Query en la Referencia de la API de AWS SDK for JavaScript.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Escenarios de Amazon Redshift con SDK de AWS

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes en Amazon Redshift con SDK de AWS. Estos escenarios muestran cómo llevar a cabo tareas específicas llamando a varias funciones dentro de Amazon Redshift. En cada escenario se incluye un enlace a GitHub, con instrucciones de configuración y ejecución del código.

Ejemplos

- Introducción a tablas, elementos y consultas de Amazon Redshift

Introducción a tablas, elementos y consultas de Amazon Redshift

En el siguiente ejemplo de código, se muestra cómo trabajar con tablas, elementos y consultas de Amazon Redshift.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import com.fasterxml.jackson.core.JsonFactory;
import com.fasterxml.jackson.databind.JsonNode;
import com.fasterxml.jackson.databind.ObjectMapper;
import com.fasterxml.jackson.databind.node.ObjectNode;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import software.amazon.awssdk.services.redshift.model.Cluster;
import software.amazon.awssdk.services.redshift.model.CreateClusterRequest;
import software.amazon.awssdk.services.redshift.model.CreateClusterResponse;
import software.amazon.awssdk.services.redshift.model.DeleteClusterRequest;
import software.amazon.awssdk.services.redshift.model.DeleteClusterResponse;
import software.amazon.awssdk.services.redshift.model.DescribeClustersRequest;
import software.amazon.awssdk.services.redshift.model.DescribeClustersResponse;
import software.amazon.awssdk.services.redshift.model.ModifyClusterRequest;
import software.amazon.awssdk.services.redshift.model.ModifyClusterResponse;
import software.amazon.awssdk.services.redshift.model.RedshiftException;
import software.amazon.awssdk.services.redshiftdata.RedshiftDataClient;
import
 software.amazon.awssdk.services.redshiftdata.model.DescribeStatementRequest;
import
 software.amazon.awssdk.services.redshiftdata.model.DescribeStatementResponse;
import
 software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementRequest;
import
 software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.redshiftdata.model.Field;
import
 software.amazon.awssdk.services.redshiftdata.model.GetStatementResultRequest;
import
 software.amazon.awssdk.services.redshiftdata.model.GetStatementResultResponse;
import software.amazon.awssdk.services.redshiftdata.model.ListDatabasesRequest;
import software.amazon.awssdk.services.redshiftdata.model.RedshiftDataException;
import software.amazon.awssdk.services.redshiftdata.model.SqlParameter;
import
 software.amazon.awssdk.services.redshiftdata.paginators.ListDatabasesIterable;
import com.fasterxml.jackson.core.JsonParser;
import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Iterator;
import java.util.List;
import java.util.Scanner;
import java.util.concurrent.TimeUnit;
```

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 *
 This Java example performs these tasks:
 *
 * 1. Prompts the user for a unique cluster ID or use the default value.
 * 2. Creates a Redshift cluster with the specified or default cluster Id value.
 * 3. Waits until the Redshift cluster is available for use.
 * 4. Lists all databases using a pagination API call.
 * 5. Creates a table named "Movies" with fields ID, title, and year.
 * 6. Inserts a specified number of records into the "Movies" table by reading
 the Movies JSON file.
 * 7. Prompts the user for a movie release year.
 * 8. Runs a SQL query to retrieve movies released in the specified year.
 * 9. Modifies the Redshift cluster.
 * 10. Prompts the user for confirmation to delete the Redshift cluster.
 * 11. If confirmed, deletes the specified Redshift cluster.
 */

public class RedshiftScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");
    public static void main(String[] args) throws Exception {
        final String usage = """

            Usage:
                <jsonFilePath>\s

            Where:
                jsonFilePath - The path to the Movies JSON file (you can locate
 that file in ../../../resources/sample_files/movies.json)
            """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
```

```
        }

        String jsonFilePath = args[0];
        String userName;
        String userPassword;
        String databaseName = "dev" ;
        Scanner scanner = new Scanner(System.in);

        Region region = Region.US_EAST_1;
        RedshiftClient redshiftClient = RedshiftClient.builder()
            .region(region)
            .build();

        RedshiftDataClient redshiftDataClient = RedshiftDataClient.builder()
            .region(region)
            .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon Redshift SDK Getting Started
scenario.");
        System.out.println("""
        This Java program demonstrates how to interact with Amazon Redshift by
using the AWS SDK for Java (v2).\s
        Amazon Redshift is a fully managed, petabyte-scale data warehouse service
hosted in the cloud.

        The program's primary functionalities include cluster creation,
verification of cluster readiness,\s
        list databases, table creation, data population within the table, and
execution of SQL statements.
        Furthermore, it demonstrates the process of querying data from the Movie
table.\s

        Upon completion of the program, all AWS resources are cleaned up.
        """);

        System.out.println("Lets get started...");
        System.out.println("Please enter your user name (default is awsuser)");
        String user = scanner.nextLine();
        userName = user.isEmpty() ? "awsuser" : user;
        System.out.println(DASHES);
        System.out.println("Please enter your user password (default is
AwsUser1000)");
        String userpass = scanner.nextLine();
```

```
        userPassword = userpass.isEmpty() ? "AwsUser1000" : userpass;
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("A Redshift cluster refers to the collection of
 computing resources and storage that work together to process and analyze large
 volumes of data.");
        System.out.println("Enter a cluster id value (default is redshift-
cluster-movies): ");
        String userClusterId = scanner.nextLine();
        String clusterId = userClusterId.isEmpty() ? "redshift-cluster-movies" :
 userClusterId;
        createCluster(redshiftClient, clusterId, userName, userPassword);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("Wait until "+clusterId +" is available.");
        System.out.print("Press Enter to continue...");
        scanner.nextLine();
        waitForClusterReady(redshiftClient, clusterId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        String databaseInfo = """
            When you created $clusteridD, the dev database is created by default
 and used in this scenario.\s

            To create a custom database, you need to have a CREATEDB privilege.\s
            For more information, see the documentation here: https://
docs.aws.amazon.com/redshift/latest/dg/r_CREATE_DATABASE.html.
           """.replace("$clusteridD", clusterId);

        System.out.println(databaseInfo);
        System.out.print("Press Enter to continue...");
        scanner.nextLine();
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("List databases in "+clusterId);
        System.out.print("Press Enter to continue...");
        scanner.nextLine();
        listAllDatabases(redshiftDataClient, clusterId, userName, databaseName);
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("Now you will create a table named Movies.");
        System.out.print("Press Enter to continue...");
        scanner.nextLine();
        createTable(redshiftDataClient, clusterId, databaseName, userName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("Populate the Movies table using the Movies.json
file.");
        System.out.println("Specify the number of records you would like to add
to the Movies Table.");
        System.out.println("Please enter a value between 50 and 200.");
        int numRecords;
        do {
            System.out.print("Enter a value: ");
            while (!scanner.hasNextInt()) {
                System.out.println("Invalid input. Please enter a value between
50 and 200.");
                System.out.print("Enter a year: ");
                scanner.next();
            }
            numRecords = scanner.nextInt();
        } while (numRecords < 50 || numRecords > 200);
        popTable(redshiftDataClient, clusterId, databaseName, userName,
jsonFilePath, numRecords);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("Query the Movies table by year. Enter a value between
2012-2014.");
        int movieYear;
        do {
            System.out.print("Enter a year: ");
            while (!scanner.hasNextInt()) {
                System.out.println("Invalid input. Please enter a valid year
between 2012 and 2014.");
                System.out.print("Enter a year: ");
                scanner.next();
            }
            movieYear = scanner.nextInt();
            scanner.nextLine();
        } while (movieYear < 2012 || movieYear > 2014);
```

```
        String id = queryMoviesByYear(redshiftDataClient, databaseName, userName,
movieYear, clusterId);
        System.out.println("The identifier of the statement is " + id);
        checkStatement(redshiftDataClient, id);
        getResults(redshiftDataClient, id);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("Now you will modify the Redshift cluster.");
        System.out.print("Press Enter to continue...");
        scanner.nextLine();
        modifyCluster(redshiftClient, clusterId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("Would you like to delete the Amazon Redshift cluster?
(y/n)");
        String delAns = scanner.nextLine().trim();
        if (delAns.equalsIgnoreCase("y")) {
            System.out.println("You selected to delete " +clusterId);
            System.out.print("Press Enter to continue...");
            scanner.nextLine();
            deleteRedshiftCluster(redshiftClient, clusterId);
        } else {
            System.out.println("The "+clusterId +" was not deleted");
        }
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("This concludes the Amazon Redshift SDK Getting
Started scenario.");
        System.out.println(DASHES);
    }

    public static void listAllDatabases(RedshiftDataClient redshiftDataClient,
String clusterId, String dbUser, String database) {
        try {
            ListDatabasesRequest databasesRequest =
ListDatabasesRequest.builder()
                .clusterIdentifier(clusterId)
                .dbUser(dbUser)
                .database(database)
                .build();
```

```
            ListDatabasesIterable listDatabasesIterable =
redshiftDataClient.listDatabasesPaginator(databasesRequest);
            listDatabasesIterable.stream()
                .flatMap(r -> r.databases().stream())
                .forEach(db -> System.out
                    .println("The database name is : " + db));

        } catch (RedshiftDataException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
        try {
            DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
                .clusterIdentifier(clusterId)
                .skipFinalClusterSnapshot(true)
                .build();

            DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
            System.out.println("The status is " +
response.cluster().clusterStatus());

        } catch (RedshiftException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
        JsonParser parser = new JsonFactory().createParser(new File(fileName));
        com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
        Iterator<JsonNode> iter = rootNode.iterator();
        ObjectNode currentNode;
        int t = 0;
        while (iter.hasNext()) {
            if (t == number)
```

```
                break;
            currentNode = (ObjectNode) iter.next();
            int year = currentNode.get("year").asInt();
            String title = currentNode.get("title").asText();

            // Use SqlParameter to avoid SQL injection.
            List<SqlParameter> parameterList = new ArrayList<>();
            String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year);";

            // Create the parameters.
            SqlParameter idParam = SqlParameter.builder()
                .name("id")
                .value(String.valueOf(t))
                .build();

            SqlParameter titleParam= SqlParameter.builder()
                .name("title")
                .value(title)
                .build();

            SqlParameter yearParam = SqlParameter.builder()
                .name("year")
                .value(String.valueOf(year))
                .build();
            parameterList.add(idParam);
            parameterList.add(titleParam);
            parameterList.add(yearParam);

            try {
                ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                    .clusterIdentifier(clusterId)
                    .sql(sqlStatement)
                    .database(databaseName)
                    .dbUser(userName)
                    .parameters(parameterList)
                    .build();

                redshiftDataClient.executeStatement(insertStatementRequest);
                System.out.println("Inserted: " + title + " (" + year + ")");
                t++;

            } catch (RedshiftDataException e) {
```

```
                System.err.println("Error inserting data: " + e.getMessage());
                System.exit(1);
            }
        }
        System.out.println(t + " records were added to the Movies table. ");
    }

    public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
        try {
            DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
                .id(sqlId)
                .build();

            String status;
            while (true) {
                DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
                status = response.statusAsString();
                System.out.println("..." + status);

                if (status.compareTo("FAILED") == 0 ) {
                    System.out.println("The Query Failed. Ending program");
                    System.exit(1);

                } else if (status.compareTo("FINISHED") == 0) {
                    break;
                }
                TimeUnit.SECONDS.sleep(1);
            }

            System.out.println("The statement is finished!");

        } catch (RedshiftDataException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
        try {
```

```
            ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
                .clusterIdentifier(clusterId)
                .preferredMaintenanceWindow("wed:07:30-wed:08:00")
                .build();

            ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
            System.out.println("The modified cluster was successfully modified
and has "
                + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

        } catch (RedshiftException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                           String database,
                                           String dbUser,
                                           int year,
                                           String clusterId) {

        try {
            String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
            SqlParameter yearParam= SqlParameter.builder()
                .name("year")
                .value(String.valueOf(year))
                .build();

            ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .database(database)
                .dbUser(dbUser)
                .parameters(yearParam)
                .sql(sqlStatement)
                .build();

            ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
            return response.id();
```

```
        } catch (RedshiftDataException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
        try {
            GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
                .id(statementId)
                .build();

            // Extract and print the field values using streams.
            GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
            response.records().stream()
                .flatMap(List::stream)
                .map(Field::stringValue)
                .filter(value -> value != null)
                .forEach(value -> System.out.println("The Movie title field is "
+ value));

        } catch (RedshiftDataException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
        boolean clusterReady = false;
        String clusterReadyStr;
        System.out.println("Waiting for cluster to become available. This may
take a few mins.");
        try {
            DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
                .clusterIdentifier(clusterId)
                .build();
            long startTime = System.currentTimeMillis();
```

```
            // Loop until the cluster is ready.
            while (!clusterReady) {
                DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
                List<Cluster> clusterList = clusterResponse.clusters();
                for (Cluster cluster : clusterList) {
                    clusterReadyStr = cluster.clusterStatus();
                    if (clusterReadyStr.contains("available"))
                        clusterReady = true;
                    else {
                        long elapsedTimeMillis = System.currentTimeMillis() -
startTime;
                        long elapsedSeconds = elapsedTimeMillis / 1000;
                        long minutes = elapsedSeconds / 60;
                        long seconds = elapsedSeconds % 60;

                        System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
                        TimeUnit.SECONDS.sleep(5);
                    }
                }
            }

            long elapsedTimeMillis = System.currentTimeMillis() - startTime;
            long elapsedSeconds = elapsedTimeMillis / 1000;
            long minutes = elapsedSeconds / 60;
            long seconds = elapsedSeconds % 60;

            System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

        } catch (RedshiftException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
        try {
            ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
```

```
                .dbUser(userName)
                .database(databaseName)
                .sql("CREATE TABLE Movies ("
                    + "id INT PRIMARY KEY, "
                    + "title VARCHAR(100), "
                    + "year INT)")
                .build();

            redshiftDataClient.executeStatement(createTableRequest);
            System.out.println("Table created: Movies");

        } catch (RedshiftDataException e) {
            System.err.println("Error creating table: " + e.getMessage());
            System.exit(1);
        }
    }

    public static void createCluster(RedshiftClient redshiftClient, String
 clusterId, String masterUsername,
                                     String masterUserPassword) {
        try {
            CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
                .clusterIdentifier(clusterId)
                .masterUsername(masterUsername)
                .masterUserPassword(masterUserPassword)
                .nodeType("ra3.4xlarge")
                .publiclyAccessible(true)
                .numberOfNodes(2)
                .build();

            CreateClusterResponse clusterResponse =
 redshiftClient.createCluster(clusterRequest);
            System.out.println("Created cluster " +
 clusterResponse.cluster().clusterIdentifier());

        } catch (RedshiftException e) {

            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener detalles de la API, consulte los siguientes temas en la Referencia de la API de AWS SDK for Java 2.x.
  - createCluster
  - describeClusters
  - describeStatement
  - executeStatement
  - getStatementResult
  - listDatabasesPaginator
  - modifyCluster

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos en diversos servicios de Amazon Redshift usando SDK de AWS

Las siguientes aplicaciones de ejemplo utilizan SDK de AWS para combinar Amazon Redshift con otros Servicios de AWS. Cada ejemplo incluye un enlace a GitHub, con instrucciones de configuración y ejecución de la aplicación.

Ejemplos

- Crear un rastreador de artículos de Amazon Redshift

Crear un rastreador de artículos de Amazon Redshift

Los siguientes ejemplos de código muestran cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo e informe al respecto con una base de datos de Amazon Redshift.

Java

SDK para Java 2.x

Muestra cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon Redshift e informe al respecto.

Para obtener el código fuente completo e instrucciones sobre cómo configurar una API de REST de Spring que consulta datos de Amazon Redshift y para su uso por parte de una aplicación React, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Redshift
- Amazon SES

Kotlin

SDK para Kotlin

Muestra cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon Redshift e informe al respecto.

Para obtener el código fuente completo e instrucciones sobre cómo configurar una API de REST de Spring que consulta datos de Amazon Redshift y para su uso por parte de una aplicación React, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Redshift
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de este servicio con un SDK de AWS. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Historial del documento

> **Note**
>
> Para obtener una descripción de las nuevas características de Amazon Redshift, consulte Novedades.

La siguiente tabla describe los cambios importantes en la documentación en la Guía de administración de Amazon Redshift a partir de junio de 2018. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Versión de API: 2012-12-01

Para obtener una lista con los cambios realizados a la Guía para desarrolladores de bases de datos de Amazon Redshift, consulte el Historial de revisión de la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para obtener más información acerca de las nuevas características, incluida una lista de correcciones y los números de versión del clúster asociado, consulte el historial de versiones del clúster.

Cambio	Descripción	Fecha
Actualizar políticas administradas del editor de consultas v2	Actualizaciones de políticas administradas `AmazonRedshiftQueryEditorV2FullAccess`, `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` y `AmazonRedshiftQueryEditorV2ReadWriteSharing` con permisos `redshift-serverles`	21 de febrero de 2024

	`s:ListNamespaces` y `redshift-serverless:ListWorkgroups`.	
Actualizar la política administrada de acceso de solo lectura de Amazon Redshift	Actualizaciones de la política administrada de `AmazonRedshiftReadOnlyAccess` con permiso `redshift:ListRecommendations` para mostrar las recomendaciones de Amazon Redshift Advisor.	7 de febrero de 2024
Lanzamiento del parche 180 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 180 de Amazon Redshift.	29 de diciembre de 2023
Lanzamiento del parche 179 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 179 de Amazon Redshift.	9 de noviembre de 2023

Actualizar las políticas administradas de Amazon Redshift	Actualizaciones de la política administrada `AmazonRedshiftServiceLinkedRolePolicy` con los permisos `ec2:AssignIpv6Addresses` y `ec2:UnassignIpv6Addresses` .	31 de octubre de 2023
Lanzamiento de la revisión 178 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Revisión 178 de Amazon Redshift.	25 de septiembre de 2023
Actualizar políticas administradas del editor de consultas v2	Actualiza políticas administradas `AmazonRedshiftQueryEditorV2NoSharing` , `AmazonRedshiftQueryEditorV2ReadSharing` y `AmazonRedshiftQueryEditorV2ReadWriteSharing` con permisos `sqlworkbench:GetAutocompletionMetadata` y `sqlworkbench:GetAutocompletionResource` .	16 de agosto de 2023

Actualizar la política administrada de Amazon Redshift	Actualizaciones de la política administrada `AmazonRedshiftServiceLinkedRolePolicy` para conceder permisos en AWS Secrets Manager para crear y administrar los secretos de las credenciales de administrador.	14 de agosto de 2023
Lanzamiento de la revisión 177 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Revisión 177 de Amazon Redshift.	3 de agosto de 2023
Lanzamiento del parche 176 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 176 de Amazon Redshift.	8 de junio de 2023

Lanzamiento del parche 175 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 175 de Amazon Redshift.	28 de abril de 2023
Actualizar la política administrada de Amazon Redshift	Actualizaciones de la política administrada de `AmazonRedshiftServiceLinkedRolePolicy` para eliminar los permisos para las acciones relacionadas con la red ec2. Estos se asociaban específicamente con la etiqueta de recurso Purpose:RedshiftMigrateToVpc.	27 de abril de 2023
Actualizar la política administrada de la API de datos de Amazon Redshift	Actualizaciones de la política administrada por `AmazonRedshiftDataFullAccess` con el permiso `redshift:GetClusterCredentialsWithIAM` .	7 de abril de 2023

Actualizar políticas administradas del editor de consultas v2	Actualiza políticas administradas `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` y `AmazonRedshiftQueryEditorV2ReadWriteSharing` con permiso `sqlworkbench:GetSchemaInference`.	21 de marzo de 2023
Se lanzó la revisión 174 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Revisión 174 de Amazon Redshift.	11 de marzo de 2023
Actualizar políticas administradas del editor de consultas v2	Actualiza políticas administradas `AmazonRedshiftQueryEditorV2NoSharing`, `AmazonRedshiftQueryEditorV2ReadSharing` y `AmazonRedshiftQueryEditorV2ReadWriteSharing` con permiso `sqlworkbench:AssociateNotebookWithTab`.	2 de febrero de 2023

Se lanzó el parche 173 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 173 de Amazon Redshift.	20 de enero de 2023
Se lanzó el parche 172 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 172 de Amazon Redshift.	17 de noviembre de 2022
Se lanzó el parche 171 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 171 de Amazon Redshift.	9 de noviembre de 2022

Se lanzó el parche 170 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 170 de Amazon Redshift.	20 de julio de 2022
Se lanzó el parche 169 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte Parche 169 de Amazon Redshift.	8 de junio de 2022
Se ha lanzado el parche 168 de Amazon Redshift.	Se está implementando un nuevo parche de Amazon Redshift. Una nueva versión tarda varias semanas en estar disponible en todas las Regiones de AWS compatibles con Amazon Redshift. Para obtener más información sobre esta versión, consulte parche 168 de Amazon Redshift.	19 de abril de 2022

Compatibilidad con perfiles de autenticación de los controladores de Amazon Redshift	Ahora puede conectarse a Amazon Redshift con un perfil de autenticación.	2 de agosto de 2021
Compatibilidad con puntos de conexión entre VPC para Amazon Redshift con tecnología AWS PrivateLink	Ahora puede utilizar puntos de conexión de la VPC administrados por Redshift con Amazon Redshift	1 de abril de 2021
Compatibilidad con las mejoras del editor de consultas de Amazon Redshift	Ahora puede utilizar el editor de consultas con enrutamiento de la VPC mejorado, tiempos de ejecución de consultas más largos y más tipos de nodos de clúster.	17 de febrero de 2021
Compatibilidad con la integración de la consola con socios	Puede integrarse a socios usando la consola de Amazon Redshift.	9 de diciembre de 2020
Compatibilidad con la capacidad de mover clústeres entre zonas de disponibilidad	Ahora, puede mover clústeres RA3 entre zonas de disponibilidad.	9 de diciembre de 2020
Compatibilidad con los tipos de nodo ra3.xlplus	Ahora, puede crear tipos de nodo ra3.xlplus.	9 de diciembre de 2020
Compatibilidad con el controlador JDBC en la versión 2.0	Ahora, puede configurar el controlador JDBC en la versión 2.0.	5 de noviembre de 2020
Compatibilidad con la tokenización y las UDF de Lambda	Ahora, puede escribir las UDF de Lambda para habilitar la tokenización externa de datos.	26 de octubre de 2020
Compatibilidad para programar la ejecución de una instrucción SQL	Ahora, puede programar una consulta en la consola de Amazon Redshift.	22 de octubre de 2020

Compatibilidad con la API de datos para Amazon Redshift	Ahora, se puede acceder a Amazon Redshift con la API de datos integrada. Las actualizaciones de la documentación incluyen una Referencia de la API de datos de Amazon Redshift.	10 de septiembre de 2020
Compatibilidad con la supervisión de consultas de la consola de Amazon Redshift	Actualizamos la guía para describir los nuevos gráficos de monitoreo de consultas.	7 de mayo de 2020
Compatibilidad con los límites de uso	Se ha actualizado la guía con una descripción de los límites de uso.	23 de abril de 2020
Autenticación multifactor	Actualizamos la guía para describir la compatibilidad con la autenticación multifactor.	20 de abril de 2020
La función de cambio de tamaño elástico ahora permite modificar el tipo de nodo	Se ha actualizado la descripción del cambio de tamaño elástico.	6 de abril de 2020
Compatibilidad de tipos de nodos ra3.4xlarge con almacenamiento administrado	Se ha actualizado la guía para incluir los tipos de nodos ra3.4xlarge.	2 de abril de 2020
Soporte para pausa y reanudación	Se ha actualizado la guía para describir las operaciones de pausa y reanudación del clúster.	11 de marzo de 2020
Compatibilidad con Microsoft Azure AD como proveedor de identidades	Se actualizó la guía para describir los pasos para usar Microsoft Azure AD como proveedor de identidades.	10 de febrero de 2020

Compatibilidad con el tipo de nodo RA3	Se ha actualizado la guía para describir el nuevo tipo de nodo RA3.	3 de diciembre de 2019
Soporte para la nueva consola	Actualizamos la guía para describir la nueva consola de Amazon Redshift.	11 de noviembre de 2019
Actualizaciones de la información de seguridad	Actualizaciones a la documentación de información de seguridad.	24 de junio de 2019
Mejoras de las instantáneas	Ahora, Amazon Redshift admite varias mejoras para administrar y programar instantáneas.	4 de abril de 2019
Escalado de simultaneidad	Puede configurar la administración de cargas de trabajo (WLM) para habilitar el modo de escalado de simultaneidad. Para obtener más información, consulte Configuración de la carga de trabajo.	21 de marzo de 2019
Controladores JDBC y ODBC actualizados	Ahora, Amazon Redshift admite nuevas versiones de los controladores JDBC y ODBC. Para obtener más información, consulte Configuración de una conexión JDBC y Configuración de una conexión ODBC.	4 de febrero de 2019

Mantenimiento pospuesto	Si necesita volver a programar el período de mantenimiento de su clúster, tiene la opción de posponer el mantenimiento hasta 14 días. Si necesitamos actualizar el hardware o realizar alguna otra actualización obligatoria durante el periodo de postergación, le notificaremos y realizaremos los cambios necesarios. Su clúster no está disponible durante estas actualizaciones. Para obtener más información, consulte Mantenimiento diferido.	20 de noviembre de 2018
Notificación avanzada	Amazon Redshift proporciona una notificación con antelación para algunos eventos. Estos eventos tienen una categoría de evento de `pending`. Por ejemplo, enviamos una notificación con antelación si se requiere una actualización de hardware para alguno de los nodos de su clúster. Puede suscribirse a los eventos pendientes de la misma forma que a otros eventos de Amazon Redshift. Para obtener más información, consulte Suscripción a notificaciones de eventos de Amazon Redshift.	20 de noviembre de 2018

Elastic resize (Cambio de tamaño elástico)	El cambio de tamaño elástico es el método más rápido de cambiar el tamaño de un clúster. El cambio de tamaño elástico agrega o quita nodos de un clúster existente y, a continuación, redistribuye automáticamente los datos a los nuevos nodos. Como no crea un nuevo clúster, la operación de cambio de tamaño elástico se completa rápidamente, normalmente en unos pocos minutos. Para obtener más información, consulte Cambio de tamaño de clústeres.	15 de noviembre de 2018
Nuevos controladores ODBC	Los controladores ODBC de Amazon Redshift se actualizaron a la versión 1.4.3.1000. Para obtener más información, consulte Configuración de una conexión ODBC.	8 de noviembre de 2018
Cancelación de la operación de cambio de tamaño	Ahora puede cancelar una operación de cambio de tamaño mientras aún está en curso. Para obtener más información, consulte Información general de la operación de cambio de tamaño.	2 de noviembre de 2018

Modificación del clúster para cambiar el cifrado	Puede modificar un clúster no cifrado para que use el cifrado de AWS Key Management Service (AWS KMS), mediante una clave administrada por AWS o una clave administr ada por el cliente. Cuando modifica su clúster para habilitar el cifrado de KMS, Amazon Redshift migra sus datos de manera automátic a a un nuevo clúster cifrado. También puede migrar un clúster no cifrado a un clúster cifrado modificando el clúster.	16 de octubre de 2018
Amazon Redshift Spectrum admite el enrutamiento de VPC mejorado	Ahora puede utilizar Redshift Spectrum con Enhanced VPC Routing habilitado para su clúster. Es posible que deba realizar algún paso de configuración adicional. Para obtener más información, consulte Uso de Amazon Redshift Spectrum con el enrutamiento de VPC mejorado.	10 de octubre de 2018
Editor de consultas	Ahora, puede ejecutar consultas SQL desde la consola de administración de Amazon Redshift.	4 de octubre de 2018

Gráfico de desglose de ejecuciones de cargas de trabajo	Ahora es posible obtener una vista detallada del rendimiento de las cargas de trabajo consultando el gráfico de desglose de ejecuciones de cargas de trabajo en la consola. Para obtener más información, consulte Análisis del rendimiento de las cargas de trabajo.	30 de julio de 2018
Pistas de mantenimiento	Ahora, puede determinar si su clúster se actualizará siempre a la última versión de Amazon Redshift o a una versión anterior seleccionando una pista de mantenimiento. Para obtener más información, consulte Elección de pistas de mantenimiento del clúster.	26 de julio de 2018

En la siguiente tabla, se describen los cambios importantes en la Guía de administración de Amazon Redshift anteriores a julio de 2018.

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nuevas métricas de CloudWatch	Se han agregado nuevas métricas de CloudWatch para monitorear el rendimiento de las consultas. Para obtener más información, consulte Monitoreo de Amazon Redshift mediante las métricas de CloudWatch	17 de mayo de 2018
Cifrado de HSM	Amazon Redshift solo admite AWS CloudHSM para la administración de claves del módulo de	6 de marzo de 2018

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
	seguridad de hardware (HSM). Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift.	
Encadenamiento de roles de IAM	Si un rol de IAM adjunto a su clúster no tiene acceso a los recursos necesarios, puede encadenar otro rol, que posiblemente pertenezca a otra cuenta. El clúster asumirá de forma temporal el rol encadenado para obtener acceso a los datos. También puede conceder acceso entre cuentas mediante el encadenamiento de roles. Cada uno de los roles de la cadena asume el rol siguiente, hasta que el clúster asume el rol situado al final de la cadena. Puede encadenar un máximo de 10 roles. Para obtener más información, consulte Encadenamiento de roles de IAM en Amazon Redshift.	23 de febrero de 2018
Nuevos tipos de nodos DC2	La nueva generación de tipos de nodos de Dense Compute (DC, computación de alta densidad) ofrece un rendimiento mucho mejor al mismo precio que DC1. Para aprovechar las mejoras del rendimien to, puede migrar su clúster DC1 a los más recientes tipos de nodos DC2. Para obtener más información, consulte Clústeres y nodos de Amazon Redshift.	17 de octubre de 2017

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Certificados de ACM	Amazon Redshift está sustituyendo los certificados SSL en sus clústeres con certificados emitidos por AWS Certificate Manager (ACM). ACM en una entidad de certificación (CA) pública de confianza en la que confían la mayoría de los sistemas actuales. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte Migración a certificados de ACM para las conexiones SSL.	18 de septiembre de 2017
Roles vinculados al servicio	Un rol vinculado a un servicio es un tipo único de rol de IAM que está conectado de forma directa a Amazon Redshift. Los roles vinculados a servicio están predefinidos por Amazon Redshift e incluyen todos los permisos que el servicio requiere para llamar a servicios de AWS en nombre de su clúster de Amazon Redshift. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Redshift.	18 de septiembre de 2017
Autenticación de usuarios de base de datos de IAM	Puede configurar el sistema para permitir que los usuarios creen credenciales de usuario e inicien sesión en la base de datos en función de sus credenciales de IAM. También puede configurar el sistema para permitir que los usuarios inicien sesión mediante el inicio de sesión único federado a través de un proveedor de identidad compatible con SAML 2.0. Para obtener más información, consulte Uso de la autenticación de IAM para generar credenciales de usuario de base de datos.	11 de agosto de 2017

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
La restauración de nivel de tabla admite Enhanced VPC Routing (enrutamiento VPC mejorado)	La restauración de nivel de tabla ahora se admite en clústeres que utilizan Enhanced VPC Routing. Para obtener más información, consulte Restauración de una tabla a partir de una instantánea.	19 de julio de 2017
Reglas de monitorización de consultas	A través de las reglas de monitoreo de consultas de la WLM, puede definir los límites de rendimiento basados en métricas para las colas de WLM y especificar la acción que se debe realizar cuando una consulta supera esos límites: registro, salto y anulación. Puede definir las reglas de monitorización de consultas como parte de la configuración de la administración de cargas de trabajo (WLM). Para obtener más informaci ón, consulte Configuración de la administración de cargas de trabajo.	21 de abril de 2017
Enhanced VPC Routing	Cuando utiliza el enrutamiento de VPC mejorado de Amazon Redshift, este servicio fuerza todo el tráfico COPY y UNLOAD entre el clúster y los repositorios de datos a que pase por su VPC de Amazon VPC. Para obtener más información, consulte Enrutamiento de VPC mejorado en Amazon Redshift.	15 de septiembre de 2016
Nuevos campos de registro de conexión	El registro de auditoría Registro de conexión tiene dos campos nuevos para realizar un seguimiento de las conexiones SSL. Si habitualmente carga registros de auditoría a una tabla de Amazon Redshift, necesitar á añadir las siguientes columnas nuevas a la tabla de destino: sslcompression y sslexpansion.	5 de mayo de 2016

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nuevos controladores ODBC	Los controladores ODBC de Amazon Redshift se actualizaron a la versión 1.2.7.1007. Para obtener más información, consulte Configuración de una conexión ODBC.	30 de marzo de 2016
Roles de IAM para COPY y UNLOAD	Ahora, puede especificar uno o más roles de AWS Identity and Access Management (IAM) que su clúster puede utilizar en la autenticación para obtener acceso a otros servicios de AWS. Los roles de IAM ofrecen una alternativa más segura para proporcionar la autenticación con los comandos COPY, UNLOAD o CREATE LIBRARY. Para obtener más información, consulte Autorización a Amazon Redshift para obtener acceso a otros servicios de AWS en su nombre y Autorización de las operaciones COPY, UNLOAD, CREATE EXTERNAL FUNCTION y CREATE EXTERNAL SCHEMA mediante roles de IAM.	29 de marzo de 2016
Restaurar desde la tabla	Puede restaurar una tabla desde una instantánea de clúster a una tabla nueva en un clúster activo. Para obtener más información, consulte Restauración de una tabla a partir de una instantánea.	10 de marzo de 2016
Uso de la condición IAM en las políticas	Puede restringir aún más el acceso a recursos mediante el elemento Condición en las políticas de IAM. Para obtener más información, consulte Usar condiciones de las políticas de IAM para control de acceso preciso.	10 de diciembre de 2015
Modificación a acceso público	Puede modificar un clúster existente en una VPC para cambiar si es de acceso público o no. Para obtener más información, consulte Modificación de un clúster.	20 de noviembre de 2015

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	28 de agosto de 2015
Actualización de la documentación	Se actualizó la guía para la solución de problemas sobre la configuración de opciones de red para asegurar que los hosts con diferentes tamaños de maximum transmission unit (MTU, unidad de transmisión máxima) puedan determinar el tamaño de un paquete para una conexión. Para obtener más información, consulte Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster.	25 de agosto de 2015
Actualización de la documentación	Se revisó toda la sección sobre los grupos de parámetros para una mejor organización y claridad. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift.	17 de agosto de 2015
Propiedades dinámicas de WLM	El parámetro de configuración de WLM ahora admite la aplicación de algunas propiedades de manera dinámica. Otras propiedades son cambios estáticos y requieren que los clústeres asociados se reinicien para que se apliquen los cambios de la configuración. Para obtener más información, consulte Propiedades dinámicas y estáticas de WLM y Grupos de parámetros de Amazon Redshift.	3 de agosto de 2015
Copia de clústeres cifrados con KMS a otra región de AWS	Agregamos contenido sobre la configuración de concesiones de copias de instantáneas para habilitar la copia de los clústeres con cifrado de AWS KMS a otra región de AWS. Para obtener más información, consulte Copia de instantáneas cifradas por AWS KMS en otra región de AWS.	28 de julio de 2015

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Actualización de la documentación	Actualizamos la sección de cifrado de bases de datos para explicar mejor cómo Amazon Redshift utiliza AWS KMS o HSM para administrar las claves, y cómo funciona el proceso de cifrado con cada una de estas opciones. Para obtener más información, consulte Cifrado de la base de datos de Amazon Redshift.	28 de julio de 2015
Nuevo tipo de nodo	Ahora, Amazon Redshift ofrece un nuevo tipo de nodo: DS2. Se actualizaron las referencias a los tipos de nodos existentes en la documentación para utilizar los nuevos nombres introducidos en esta publicación. También se revisó la sección para una mejor explicación sobre las combinaciones de tipos de nodos y aclaración de los límites de cuota predeterminados. Para obtener más información, consulte Clústeres y nodos de Amazon Redshift.	9 de junio de 2015
Ofertas de nodos reservados	Se añadió contenido sobre las nuevas ofertas de nodos reservados. También se revisó la sección para brindar una mejor explicación y comparación de las ofertas disponibles y proporcionar ejemplos para demostrar cómo los precios de los nodos reservados y bajo demanda afectan la facturación. Para obtener más información, consulte Información general.	9 de junio de 2015
Nuevos controladores ODBC	Se actualizaron los controladores ODBC de Amazon Redshift. Se añadió una sección sobre las versiones anteriores de estos controladores y un enlace a las notas de la versión de los controladores. Para obtener más información, consulte Configuración de una conexión ODBC.	5 de junio de 2015

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	30 de abril de 2015
Nueva característica	Esta versión de Amazon Redshift presenta nuevos controladores JDBC y ODBC optimizados para su uso con Amazon Redshift. Para obtener más información, consulte Conexión a un almacenamiento de datos de Amazon Redshift mediante herramientas de cliente SQL.	26 de febrero de 2015
Nueva característica	Esta versión de Amazon Redshift presenta las métricas de rendimiento del clúster que le permiten ver y analizar los detalles de ejecución de la consulta. Para obtener más información, consulte Visualización de consultas y cargas.	26 de febrero de 2015
Actualización de la documentación	Agregamos una nueva política de ejemplo en la que se muestra la concesión de permisos para los recursos y las acciones comunes de los servicios de AWS en los que se basa Amazon Redshift. Para obtener más información, consulte Ejemplos de políticas administradas por el cliente.	16 de enero de 2015
Actualización de la documentación	Se actualizó la guía sobre la configuración de la maximum transmission unit (MTU, unidad de transmisión máxima) para deshabilitar tramas gigantes TCP/IP. Para obtener más información, consulte Usar EC2-VPC al crear el clúster y Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster.	16 de enero de 2015

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Actualización de la documentación	Se ha revisado el contenido sobre el parámetro `wlm_json_configuration` y se ha proporcionado una sintaxis de ejemplo para configurar este parámetro utilizando la AWS CLI en los sistemas operativos Microsoft Windows, Mac OS X y Linux. Para obtener más información, consulte Configuración de la administración de cargas de trabajo.	13 de enero de 2015
Actualización de la documentación	Se añadieron notificaciones y descripciones faltantes de eventos. Para obtener más información, consulte Categorías y mensajes de eventos de Amazon Redshift.	8 de enero de 2015
Actualización de la documentación	Actualizamos las directrices sobre las políticas de IAM para las acciones y los recursos de Amazon Redshift. Se revisó la sección para mejorar la organización y la claridad. Para obtener más información, consulte Seguridad en Amazon Redshift.	21 de noviembre de 2014
Nueva característica	Esta versión de Amazon Redshift presenta la capacidad para cifrar clústeres con claves de cifrado de AWS Key Management Service (AWS KMS). AWS KMS combina hardware y software seguro y con alta disponibilidad para proporcionar un sistema de administración de claves escalado para la nube. Para obtener más información acerca de AWS KMS y las opciones de cifrado para Amazon Redshift, consulte Cifrado de la base de datos de Amazon Redshift y Administración de clústeres a través de la consola.	12 de noviembre de 2014

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nueva característica	Esta versión de Amazon Redshift presenta la capacidad para etiquetar los recursos, como clústeres e instantáneas. Las etiquetas le permiten proporcionar metadatos definidos por el usuario para categorizar los informes de facturación basados en la asignación de costos y ayudar a identificar mejor los recursos de inmediato. Para obtener más información, consulte Etiquetado de recursos en Amazon Redshift.	4 de noviembre de 2014
Nueva característica	Se aumentó el límite de nodos máximo a 128 para los tamaños de nodo dw1.8xlarge y dw2.8xlarge. Para obtener más información, consulte Clústeres y nodos de Amazon Redshift.	30 de octubre de 2014
Actualización de la documentación	Agregamos enlaces a los paquetes Microsoft Visual C++ 2010 Redistributable que se requieren para que Amazon Redshift utilice los controladores PostgreSQL ODBC. Para obtener más información, consulte Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows.	30 de octubre de 2014
Nueva característica	Agregamos la capacidad para terminar consultas y cargas desde la consola de Amazon Redshift. Para obtener más información, consulte Visualización de consultas y cargas y Visualización de métricas de clúster durante las operaciones de carga.	28 de octubre de 2014
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	17 de octubre de 2014
Nuevo contenido	Se añadió contenido sobre el cierre y la eliminación de clústeres. Para obtener más información, consulte Cierre y eliminación de clústeres y Eliminación de un clúster.	14 de agosto de 2014

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Actualización de la documentación	Se ha clarificado el comportamiento de la opción Allow Version Upgrade (Permitir actualización de versions) en los clústeres. Para obtener más información, consulte Información general de Amazon Redshift.	14 de agosto de 2014
Actualización de la documentación	Revisamos los procedimientos, las capturas de pantalla y la organización del trabajo con clústeres en la consola de Amazon Redshift. Para obtener más información, consulte Administración de clústeres a través de la consola.	11 de julio de 2014
Nuevo contenido	Agregamos un nuevo tutorial sobre la modificación del tamaño de los clústeres de Amazon Redshift, que incluyen cómo cambiar el tamaño de un clúster mientras se acorta la cantidad de tiempo que el clúster está en modo de solo lectura. Para obtener más información, consulte Cambio de tamaño de clústeres.	27 de junio de 2014
Nueva característica	Se añadió la función para cambiar el nombre de los clústeres. Para obtener más información, consulte Cambio de nombre de los clústeres y Modificación de un clúster.	2 de junio de 2014
Actualización de la documentación	Se actualizó el ejemplo de código .NET para utilizar el proveedor de datos ODBC cuando se conecta a un clúster mediante programación utilizando .NET. Para obtener más información, consulte Conexión a un almacenamiento de datos mediante programación.	15 de mayo de 2014
Nueva característica	Se añadieron las opciones para seleccionar un grupo de parámetros y un grupo de seguridad diferentes cuando restaura un clúster a partir de una instantánea. Para obtener más información, consulte Restauración de un clúster desde una instantánea.	12 de mayo de 2014

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nueva característica	Agregamos una nueva sección en la que se describe cómo configurar una alarma predeterminada de Amazon CloudWatch para monitorear el porcentaje de espacio utilizado en el disco en un clúster de Amazon Redshift. Esta alarma es una nueva opción en el proceso de creación de clúster. Para obtener más información, consulte Alarma predeterminada de espacio en disco.	28 de abril de 2014
Actualización de la documentación	Aclaramos la información acerca de la compatibilidad con Elliptic Curve Diffie-Hellman Exchange (ECDHE) con Amazon Redshift. Para obtener más información, consulte Conexión mediante una SSL.	22 de abril de 2014
Nueva característica	Agregamos una instrucción sobre la compatibilidad de Amazon Redshift con el protocolo de acuerdo de claves Elliptic Curve Diffie-Hellman (ECDH). Para obtener más información, consulte Conexión mediante una SSL.	18 de abril de 2014
Actualización de la documentación	Se revisaron y reorganizaron los temas en la sección Conexión a un almacenamiento de datos de Amazon Redshift mediante herramientas de cliente SQL. Se añadió más información acerca de las conexiones ODBC y JDBC y se agregó una nueva sección para solucionar problemas de conexión.	15 de abril de 2014
Actualización de la documentación	Se añadió una versión en los ejemplos de la política de IAM a lo largo de la guía.	3 de abril de 2014
Actualización de la documentación	Se añadió información acerca del funcionamiento de los precios cuando cambia el tamaño de un clúster. Para obtener más información, consulte Adquisición de nodos reservados de Amazon Redshift.	2 de abril de 2014

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nueva característica	Se añadió una sección sobre un nuevo parámetro, `max_cursor_result_set_size`, que establece el tamaño máximo de conjuntos de resultados, en megabytes, que pueden almacenarse por cursor individual. El valor del parámetro también afecta el número de cursores activos simultáneamente para el clúster. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift.	28 de marzo de 2014
Nueva característica	Se ha añadido una explicación sobre el campo Cluster Version (Versión del clúster), que ahora incluye la versión del motor del clúster y el número de revisión de la base de datos. Para obtener más información, consulte Clústeres aprovisionados de Amazon Redshift.	21 de marzo de 2014
Nueva característica	Se ha actualizado el procedimiento de cambio de tamaño para mostrar información nueva sobre el progreso del cambio de tamaño en la pestaña Status (Estado) del clúster. Para obtener más información, consulte Redimensionamiento de un clúster.	21 de marzo de 2014
Actualización de la documentación	Se reorganizó y actualizó ¿Qué es Amazon Redshift? y se revisó Información general de los clústeres de Amazon Redshift aprovisionados. Se publicaron varias correcciones de la documentación.	21 de febrero de 2014

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nueva característica	Agregamos nuevos tipos y tamaños de nodos para los clústeres de Amazon Redshift. Además, reescribimos el tema relacionado de información general del clúster para tener una mejor organización y más claridad a partir de los comentarios. Para obtener más información, consulte Clústeres aprovisionados de Amazon Redshift.	23 de enero de 2014
Nueva característica	Agregamos información sobre el uso de direcciones IP elásticas (EIP) para los clústeres accesibles públicamente de Amazon Redshift en las nubes virtuales privadas. Para obtener más información acerca de las EIP en Amazon Redshift, consulte Administración de clústeres en una VPC y Creación de un clúster en una VPC.	20 de diciembre de 2013
Nueva característica	Agregamos información sobre los registros de AWS CloudTrail para Amazon Redshift. Para obtener más información acerca de la compatibilidad de Amazon Redshift con CloudTrail, consulte Registro con CloudTrail.	13 de diciembre de 2013
Nueva característica	Agregamos información sobre el nuevo registro de la actividad del usuario y el parámetro de la base de datos `enable_user_activity_logging` para la característica de registro de auditoría de la base de datos de Amazon Redshift. Para obtener más información acerca del registro de auditoría de la base de datos, consulte Registro de auditoría de bases de datos. Para obtener más información acerca de los parámetros de la base de datos, consulte Grupos de parámetros de Amazon Redshift.	6 de diciembre de 2013

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nueva característica	Realizamos una actualización para describir la configuración de Amazon Redshift para copiar automáticamente las instantáneas automatizadas y manuales en una región de AWS secundaria. Para obtener más información acerca de la configuración para copiar instantáneas entre regiones, consulte Copia de instantáneas a otra región de AWS.	14 de noviembre de 2013
Nueva característica	Agregamos una sección para describir el registro de auditoría de Amazon Redshift de la actividad de conexión y la actividad del usuario, así como describir el almacenamiento de estos registros en Amazon S3. Para obtener más información acerca del registro de auditoría de la base de datos, consulte Registro de auditoría de bases de datos.	11 de noviembre de 2013
Nueva característica	Agregamos una sección para describir el cifrado de Amazon Redshift con nuevas características para administrar claves de cifrado en un módulo de seguridad de hardware (HSM) y para rotar las claves de cifrado. Para obtener más información acerca del cifrado, el HSM; y la rotación de claves, consulte Cifrado de la base de datos de Amazon Redshift, Cifrado de Amazon Redshift con módulos de seguridad de hardware y Rotación de claves de cifrado en Amazon Redshift.	11 de noviembre de 2013
Nueva característica	Realizamos una actualización para describir la publicación de notificaciones de eventos de Amazon Redshift a través de Amazon SNS. Para obtener más información sobre las notificaciones de eventos de Amazon Redshift, consulte Notificaciones de eventos de Amazon Redshift.	11 de noviembre de 2013

Cambio	Descripción	Fecha de lanzamiento de la nueva versión
Nueva característica	Realizamos una actualización para describir los permisos en el nivel de los recursos de IAM. Para obtener más información sobre los permisos de IAM de Amazon Redshift, consulte Seguridad en Amazon Redshift.	9 de agosto de 2013
Nueva característica	Se realizó una actualización para describir la restauración de las métricas de progreso. Para obtener más información, consulte Restauración de un clúster desde una instantánea.	9 de agosto de 2013
Nueva característica	Se realizó una actualización para describir el uso compartido de instantáneas de clústeres y la creación de métricas de progreso de instantáneas. Para obtener más información, consulte Uso compartido de instantáneas.	17 de julio de 2013
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	8 de julio de 2013
Nuevas pantallas de consolas	Actualizamos la Guía de administración de Amazon Redshift para que coincida con los cambios de la consola de Amazon Redshift.	22 de abril de 2013
Nueva guía	Esta es la primera versión de la Guía de administración de Amazon Redshift.	14 de febrero de 2013