Guía del usuario

AWS CloudTrail

Version 1.0

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

AWS CloudTrail: Guía del usuario

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 AWS CloudTrail? 1
Cómo CloudTrail funciona 3
Historial de eventos 3
CloudTrail Almacenes de datos de lagos y eventos 4
CloudTrail senderos 5
CloudTrail canales 8
Flujo de trabajo 8
Historial de eventos 9
CloudTrail Lake 9
Registros de seguimiento 12
Conceptos 15
¿Qué son los CloudTrail eventos? 16
¿Qué es el historial de CloudTrail eventos? 35
¿Qué son los registros de seguimiento? 35
¿Qué son los registros de seguimiento de organización? 35
¿Cómo se gestiona CloudTrail? 37
¿Cómo se controla el acceso a? CloudTrail 39
¿Cómo registra los eventos de administración o de datos? 39
¿Cómo se registran los eventos de CloudTrail Insights? 40
¿Cómo se ejecutan consultas complejas sobre los eventos registrados por CloudTrail? 40
¿Cómo se realiza la supervisión CloudTrail? 41
¿Cómo se CloudTrail comporta a nivel regional y global? 42
Eventos de servicios globales 44
¿Cómo CloudTrail se relaciona con otros servicios AWS de supervisión? 46
Soluciones de socios 46
Regiones admitidas 46
Ejemplos de archivos de registros de CloudTrail 51
Formato de nombre de archivo de registros de CloudTrail 51
Ejemplos de archivos de registros 52
Servicios e integraciones compatibles 65
AWS integraciones de servicios con registros CloudTrail 65
CloudTrail integración con Amazon EventBridge 67
CloudTrail integración con AWS Organizations 68
AWS temas de servicio para CloudTrail 68

Servicios no admitidos 96
Cuotas en AWS CloudTrail 96
CloudTrail tutoriales 104
Requisitos previos 104
Inscríbase en una Cuenta de AWS 104
Cómo crear un usuario administrativo 105
Otorgue permisos de uso CloudTrail 106
Tutorial: Revisa la actividad AWS de la cuenta en el historial de eventos 108
Tutorial: Crear un registro de seguimiento 111
Tutorial: Ver los archivos de registro 116
Planificar los pasos siguientes 119
Tutoriales para Lake CloudTrail 121
Tutorial: Creación de un almacén de datos de eventos para eventos de administración 122
Tutorial: Creación de un almacén de datos de eventos para eventos de datos de S3 130
Tutorial: Copia los eventos del sendero a CloudTrail Lake 139
Tutorial: Ver los paneles de Lake 151
Tutorial: Ver y ejecutar consultas de ejemplo 157
Tutorial: Guardar los resultados de las consultas en un bucket de Amazon S3 160
Trabajar con el historial de CloudTrail eventos 165
Limitaciones del Historial de eventos 166
Visualización de los eventos de administración recientes en la CloudTrail consola 167
Navegación entre páginas 169
Personalización de la pantalla 169
Filtrar CloudTrail eventos 171
Ver los detalles de un evento 173
Descarga de eventos 173
Ver los recursos a los que se hace referencia AWS Config 174
Visualización de los eventos de gestión recientes con el AWS CLI 175
Requisitos previos 177
Obtener ayuda de la línea de comandos 177
Buscar eventos 178
Especificar el número de eventos que se devuelven 179
Buscar eventos por intervalo de tiempo 179
Buscar eventos por atributo 180
Especificar la siguiente página de resultados 182
Obtener datos de entrada JSON de un archivo 182

Campos de resultados de búsqueda 184
¿Trabajando con CloudTrail Lake 186
CloudTrail Almacena datos de eventos en Lake 186
CloudTrail Integraciones de Lake 187
CloudTrail Consultas de Lake 188
Regiones en las que se admite CloudTrail Lake 189
Conceptos y terminología de CloudTrail Lake 190
Almacenes de datos de eventos 191
Integraciones 193
Consultas 194
Panel de control 194
Almacenes de datos de eventos 196
Cree un banco de datos de CloudTrail eventos para eventos 198
Cree un banco de datos de eventos para los eventos de CloudTrail Insights 206
Creación de un almacén de datos de eventos para los elementos de configuración de AWS Config 216
Cree un almacén de datos de eventos para eventos ajenos a AWS 231
Copiar eventos de registro de seguimiento en un almacén de datos de eventos 235
Administración de los ciclos de vida de los almacenes de datos de eventos 249
Actualización de un almacén de datos de eventos 250
Detener e iniciar la incorporación de eventos 254
Federar un almacén de datos de eventos 255
Cambiar la protección contra la terminación 266
Eliminación de un almacén de datos de eventos 267
Restauración de un almacén de datos de eventos 268
Almacenes de datos de eventos de la organización 269
Integraciones 274
Creación de una integración con un socio de CloudTrail 276
Creación de una integración personalizada 278
Información adicional acerca de los socios de integración 283
Esquema de eventos de integraciones de CloudTrail Lake 284
Ver los paneles de Lake 293
Limitaciones 294
Requisitos previos 294
Elección de un panel 295
Filtrado de un panel por intervalo de fecha u hora 296

Visualización de la consulta de un widget de panel ... 297
Consultas ... 188
Creación o edición de una consulta ... 298
Consultas de ejemplo ... 301
Ejecutar una consulta y guardar los resultados de la consulta ... 308
Visualización de los resultados de la consulta ... 310
Obtener y descargar resultados de consultas guardados ... 312
Validación de los resultados de consultas guardados ... 314
Recursos de aprendizaje ... 329
Administrar CloudTrail Lake mediante la AWS CLI ... 330
Crear un almacén de datos de eventos con la AWS CLI ... 331
Importar eventos de registros de seguimiento a un almacén de datos de eventos con la AWS CLI ... 340
Crear una integración para registrar eventos externos a AWS con la AWS CLI ... 346
Obtener un almacén de datos de eventos con la AWS CLI ... 353
Enumerar todos los almacenes de datos de eventos de una cuenta con la AWS CLI ... 355
Actualizar un almacén de datos de eventos con la AWS CLI ... 355
Detener la incorporación en un almacén de datos de eventos con la AWS CLI ... 360
Iniciar la incorporación en un almacén de datos de eventos con la AWS CLI ... 361
Habilitar la federación en un almacén de datos de eventos ... 361
Deshabilitar la federación en un almacén de datos de eventos ... 362
Eliminar un almacén de datos de eventos con la AWS CLI ... 362
Restaurar un almacén de datos de eventos con la AWS CLI ... 363
Enumerar todos los canales con la AWS CLI ... 363
Actualizar un canal con la AWS CLI ... 363
Eliminar un canal para eliminar una integración con la AWS CLI ... 364
Iniciar una consulta con la AWS CLI ... 364
Obtener metadatos sobre una consulta con la AWS CLI ... 365
Obtener los resultados de consultas con la AWS CLI ... 366
Enumerar todas las consultas en un almacén de datos de eventos con la AWS CLI ... 366
Cancelar una consulta en curso con la AWS CLI ... 367
CloudTrail Restricciones de Lake SQL ... 368
Funciones, condiciones y operadores join compatibles ... 369
Soporte avanzado de consultas en varias tablas ... 370
Esquemas SQL compatibles con los almacenes de datos de eventos ... 371
Esquema compatible para los campos de registro de eventos de CloudTrail ... 371

Esquema compatible para los campos de registro de eventos de CloudTrail Insights 375
Esquema compatible para los campos de registro de elementos de configuración de AWS Config 377
Esquema compatible para los campos de registro de evidencia de AWS Audit Manager 378
Esquema compatible para campos de eventos que no son de AWS 379
Control de los permisos de usuario 381
Gestión de los costos CloudTrail del lago 381
Opciones de precios del almacén de datos de eventos 382
Entendiendo los cargos de CloudTrail Lake 383
Recomendaciones sobre cómo reducir los costos 385
Herramientas para ayudar a administrar los costos 387
Véase también 388
Métricas de CloudWatch compatibles 389
Trabajar con registros de seguimiento de CloudTrail 393
Creación de un registro de seguimiento para su Cuenta de AWS 393
Creación y actualización de un registro de seguimiento con la consola 395
Creación, actualización y gestión de senderos con AWS Command Line Interface 440
Creación de un registro de seguimiento para una organización 472
Historial de eventos y registros de seguimiento de organización 477
Prácticas recomendadas para pasar de los registros de seguimiento de cuentas miembro a los registros de seguimiento de la organización 477
Prepararse a fin de crear un registro de seguimiento para la organización 478
Creación de un registro de seguimiento para la organización en la consola 482
Crear un registro para una organización con AWS Command Line Interface 500
Solución de problemas 508
Visualizar eventos de CloudTrail Insights para registros de seguimiento 510
Visualizar eventos de CloudTrail Insights para registros de seguimiento en la consola de CloudTrail 511
Visualización de eventos de CloudTrail Insights para senderos con el AWS CLI 522
Copiar los eventos del sendero al CloudTrail lago 533
Consideraciones para copiar eventos de registros de seguimiento 535
Permisos necesarios para copiar eventos de registro de seguimiento 537
Copie los eventos de seguimiento a un almacén de datos de eventos existente mediante la consola CloudTrail 541
Obtención y visualización de archivos de registros de CloudTrail 544
Búsqueda de los archivos de CloudTrail registro 545

Descarga de los archivos de registros de CloudTrail ... 547
Configuración de notificaciones de Amazon SNS para CloudTrail ... 548
Configuración de CloudTrail para el envío de notificaciones ... 549
Consejos para la administración de registros de seguimiento ... 551
Gestión de los costes de los CloudTrail senderos ... 551
Requisitos de nomenclatura ... 554
Control de los permisos de usuario ... 556
Puntos de conexión de VPC compatibles ... 557
Disponibilidad ... 558
Cree un punto final de VPC para CloudTrail ... 559
Subredes compartidas ... 559
Cuenta de AWS cierre y senderos ... 559
Archivo de registros de CloudTrail ... 561
Crear varios registros de seguimiento ... 563
Registro de eventos de administración ... 565
Eventos de administración ... 566
Eventos de lectura y escritura ... 568
Registro de eventos con la AWS Command Line Interface ... 569
Registro de eventos con los SDK de AWS ... 580
Envío de eventos a Amazon CloudWatch Logs ... 581
Registro de eventos de datos ... 581
Eventos de datos ... 582
Eventos de solo lectura y de solo escritura ... 628
Registrar eventos de datos con AWS Command Line Interface ... 629
Registrar eventos de datos para la conformidad con AWS Config ... 641
Registrar eventos de datos con los SDK AWS ... 642
Envío de eventos a Amazon CloudWatch Logs ... 642
Registro de eventos de Insights ... 643
Descripción de la entrega de eventos de Insights ... 644
Registro de eventos de Insights con la AWS Management Console ... 645
Registro de eventos de Insights con la AWS Command Line Interface ... 647
Registro de eventos con los SDK de AWS ... 653
Información adicional para registros de seguimiento ... 653
Recepción de archivos de registro de CloudTrail de varias regiones ... 661
Administración de la consistencia de los datos ... 663
Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs ... 664

Envío de eventos a Amazon CloudWatch Logs 664
Creación de alarmas de CloudWatch para eventos de CloudTrail: ejemplos 673
Impedir que CloudTrail envíe eventos a CloudWatch Logs 681
Grupo de registros de CloudWatch y nomenclatura de secuencias de registros para CloudTrail 682
Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear 683
Recibir archivos de CloudTrail registro de varias cuentas 685
Eliminación de los ID de las cuentas de los propietarios de los buckets para eventos de datos llamados por otras cuentas 686
Configuración de la política de bucket para varias cuentas 688
Crea registros de seguimiento en cuentas adicionales 690
Compartir archivos de registro de CloudTrail entre cuentas de AWS 692
Comparta archivos de registros entre cuentas asumiendo un rol 692
Validar la integridad de los archivos de registros de CloudTrail 702
¿Por qué utilizarla? 703
Cómo funciona 703
Habilitación de la validación de la integridad de los archivos de registros de CloudTrail 704
Validación de la integridad de los archivos de registros de CloudTrail con la AWS CLI 705
Estructura de los archivos de resumen de CloudTrail 714
Implementaciones personalizadas de la validación de la integridad de los archivos de CloudTrail registro 722
Uso de la biblioteca de procesamiento de CloudTrail 734
Requisitos mínimos 735
Procesamiento de registros de CloudTrail 735
Temas avanzados 741
Recursos adicionales 746
Configuración 747
Administrador delegado de la organización 747
Permisos necesarios para designar un administrador delegado 751
Agrega un administrador delegado CloudTrail 751
Eliminar un administrador CloudTrail delegado 753
Canales vinculados a servicios 753
Visualización de canales vinculados a servicios con la consola 754
Visualización de canales vinculados a servicios con la AWS CLI 754
Seguridad 758

Protección de los datos ... 759
Identity and Access Management ... 760
Público ... 761
Autenticación con identidades ... 762
Administración de acceso mediante políticas ... 765
Cómo funciona AWS CloudTrail con IAM ... 768
Ejemplos de políticas basadas en identidades ... 778
Ejemplos de políticas basadas en recursos ... 795
Política de bucket de Amazon S3 para CloudTrail ... 797
Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake ... 805
Política temática de Amazon SNS para CloudTrail ... 808
Solución de problemas ... 816
Usar roles vinculados a servicios ... 820
Políticas administradas de AWS ... 823
Validación de conformidad ... 825
Resiliencia ... 827
Seguridad de infraestructuras ... 828
Prevención del suplente confuso entre servicios ... 829
Prácticas recomendadas de seguridad ... 830
CloudTrail prácticas recomendadas de seguridad policial ... 830
CloudTrail prácticas recomendadas de seguridad preventiva ... 832
Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS) ... 836
Activación del cifrado de los archivos de registro ... 837
Conceder permisos para crear una clave de KMS ... 839
Configurar políticas de clave de AWS KMS para CloudTrail ... 839
Actualización de un recurso para que utilice su clave de KMS ... 855
Habilitar y deshabilitar el cifrado de archivos de registros de CloudTrail con la AWS CLI ... 859
Referencia de eventos de registro ... 863
CloudTrail contenido del registro ... 867
Campos de registro de eventos de Insights ... 879
Ejemplo de sharedEventID ... 879
Detalles de los servicios que admiten TLS en CloudTrail ... 881
CloudTrail Elemento UserIdentity ... 889
Ejemplos ... 889
Campos ... 890
Valores para AWS STS las API con SAML y federación de identidades web ... 898

AWS STS identidad de origen 900
Elemento Insights insightDetails 903
Ejemplo de bloque `insightDetails` 909
Eventos no generados por la API capturados por CloudTrail 912
Eventos de servicio de AWS 912
AWS Management Console eventos de inicio de sesión 913
Historial del documento 929
Actualizaciones anteriores 980
Glosario de AWS 1004
..... mv

¿Qué es AWS CloudTrail?

AWS CloudTrail es un servicio de AWS que lo ayuda a habilitar la gobernanza, la conformidad y las auditorías de operaciones y riesgos de su cuenta de AWS. Las acciones que realiza un usuario, rol o servicio de AWS se registran como eventos en CloudTrail. Los eventos incluyen las acciones llevadas a cabo en la AWS Management Console, AWS Command Line Interface y las API y los SDK de AWS.

CloudTrail está activo en la Cuenta de AWS al crearla y no requiere ninguna configuración manual. Cuando se produce actividad en su Cuenta de AWS, esta se registra en un evento de CloudTrail.

CloudTrail ofrece tres formas de registrar eventos:

- Historial de eventos: el Historial de eventos proporciona un registro visible e inmutable, que se puede buscar y descargar, de los últimos 90 días de eventos de administración registrados en una Región de AWS. Puede filtrar en un solo atributo para buscar eventos. Al crear la cuenta, tendrá acceso automáticamente al Historial de eventos. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

  No se cobran cargos de CloudTrail por ver el Historial de eventos.
- CloudTrail Lake: AWS CloudTrail Lake es un lago de datos administrado para capturar, almacenar, acceder y analizar actividad de API y usuarios en AWS con fines de seguridad y auditoría. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato ORC de Apache. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son colecciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción de precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción de precio de retención de siete años. Puede crear un almacén de datos de eventos para una sola Cuenta de AWS o para varias Cuentas de AWS mediante AWS Organizations. Puede importar cualquier registro de CloudTrail existente de sus buckets de S3 a un almacén de datos de eventos nuevo o existente. También puede ver las principales tendencias de eventos de CloudTrail con los paneles de Lake. Para más información, consulte Trabajando con AWS CloudTrail Lake y Creación de un almacén de datos de eventos.

  Los almacenes de datos de eventos de CloudTrail Lake y las consultas conllevan cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La

opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Cuando ejecuta consultas en Lake, paga según la cantidad de datos escaneados. Para obtener información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

- Registros de seguimiento: los registros de seguimiento capturan un registro de las actividades de AWS y distribuyen y almacenan estos eventos en un bucket de Amazon S3, con entrega opcional a Registros de Amazon CloudWatch y Amazon EventBridge. Puede incorporar estos eventos a sus soluciones de supervisión de seguridad. También puede usar sus propias soluciones de terceros o soluciones como Amazon Athena para buscar y analizar sus registros de CloudTrail. Puede crear registros de seguimiento para una sola Cuenta de AWS o para varias Cuentas de AWS mediante AWS Organizations. Puede registrar eventos de Insights para analizar sus eventos de administración para detectar un comportamiento anómalo en los volúmenes de llamadas a las API y las tasas de error. Para obtener más información, consulte Creación de un registro de seguimiento para su Cuenta de AWS.

  Puede crear un registro de seguimiento para enviar una copia de los eventos de administración en curso en su bucket de Amazon S3 sin costo alguno desde CloudTrail; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

La visibilidad de la actividad de su cuenta de AWS es un aspecto clave de la seguridad y de las prácticas recomendadas operativas. Puede utilizar CloudTrail para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en la infraestructura de AWS. Puede identificar quién o qué tuvo que actuar, sobre qué recursos se actuó, cuándo se produjo el evento y otros detalles que lo ayudarán a analizar y responder a una actividad en la cuenta de AWS.

Puede integrar CloudTrail en las aplicaciones mediante la API, automatizar la creación de registros de seguimiento o almacenes de datos de eventos para su organización, verificar el estado de los almacenes de datos de eventos y registros de seguimiento que crea y controlar la forma en que los usuarios ven los eventos de CloudTrail.

Temas

- Cómo CloudTrail funciona
- Flujo de trabajo de CloudTrail

- CloudTrail conceptos
- CloudTrail regiones compatibles
- Ejemplos de archivos de registros de CloudTrail
- CloudTrail servicios e integraciones compatibles
- Cuotas en AWS CloudTrail

Cómo CloudTrail funciona

CloudTrail está activo en tu AWS cuenta cuando la creas. Cuando se produce actividad en tu AWS cuenta, esa actividad se registra en un CloudTrail evento. Para ver los últimos 90 días de actividad de la API registrada (eventos de gestión) y Región de AWS en la CloudTrail consola, accede al Historial de eventos.

Para mantener un registro continuo de los eventos en su Cuenta de AWS, cree un almacén de datos de eventos o un registro de seguimiento. Los senderos pueden registrar eventos para la CloudTrail administración, los datos y los eventos de Insights. Los almacenes de datos de eventos pueden registrar eventos de CloudTrail administración y datos, eventos de CloudTrail Insights, elementos de AWS Config configuración, AWS Audit Managerpruebas y no AWS eventos de las integraciones.

Para empezar CloudTrail, consulteCómo empezar con AWS CloudTrail los tutoriales.

Para CloudTrail conocer los precios, consulta AWS CloudTrailPrecios. Para obtener información sobre los precios de Amazon S3 y Amazon SNS, consulte Precios de Amazon S3 y Precios de Amazon SNS.

Temas

- Historial de eventos
- CloudTrail Almacenes de datos de lagos y eventos
- CloudTrail senderos
- CloudTrail canales

Historial de eventos

El Historial de eventos proporciona un registro visible e inmutable, que se puede buscar y descargar, de los últimos 90 días de eventos de administración registrados en una Región de AWS. Puedes ver fácilmente los eventos de gestión en la CloudTrail consola desde la página del historial de

eventos. También puede ejecutar el comando aws cloudtrail lookup-events o la operación de la API `LookupEvents` para ver el historial de eventos. Puede buscar eventos en el historial de eventos filtrando los eventos en un solo atributo. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

El Historial de eventos no está conectado a ningún registro de seguimiento ni almacén de datos de eventos que exista en su cuenta y no se ve afectado por los cambios de configuración que haga en los registros de seguimiento ni en los almacenes de datos de eventos.

CloudTrail Almacenes de datos de lagos y eventos

Puede crear un almacén de datos de eventos de CloudTrail Lake para archivar, analizar y responder a los cambios en sus AWS recursos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción Precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción Precio de retención de siete años.

Puede crear un banco de datos de eventos para recopilar eventos CloudTrail de administración y datos, eventos de CloudTrail Insights, elementos de AWS Config configuración, AWS Audit Managerpruebas o no eventos. AWS Puede crear almacenes de datos de eventos mediante la consolaAWS CLI, la o la CloudTrail API. Para obtener más información acerca de cómo crear almacenes de datos de eventos mediante la consola, consulte Creación de un almacén de datos de eventos. Para obtener más información acerca de cómo crear almacenes de datos de eventos mediante la AWS CLI, consulte Administrar CloudTrail Lake mediante la AWS CLI.

CloudTrail Lake le permite registrar eventos desde aplicaciones externasAWS, incluso desde cualquier fuente de sus entornos híbridos, como aplicaciones internas o SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores mediante la creación de integraciones. Puede crear integraciones con más de 12 socios para registrar los eventos que se producen fuera de AWS en sus almacenes de datos de eventos. Para crear una integración, primero debe configurar un canal a través del cual se entregan los eventos. Puede usar CloudTrail Lake para almacenar estos datos, acceder a ellos, analizarlos, solucionar problemas y tomar medidas al respecto sin tener que mantener varios agregadores de registros ni herramientas de generación de informes.

Los almacenes de datos de eventos pueden registrar eventos de la Región de AWS actual o de todas las Regiones de AWS de su cuenta de AWS. Los almacenes de datos de eventos que utilice para registrar eventos de Integración externos a AWS deben ser únicamente para una región; no pueden ser almacenes de datos de eventos de varias regiones.

Para cambiar un banco de datos de eventos después de crearlo, puede ejecutar el update-event-data-storecomando o usar la consola de CloudTrail Lake.

Si ha creado una organización en AWS Organizations, puede crear un almacén de datos de eventos de la organización que registra todos los eventos de todas las cuentas de AWS en dicha organización. Los almacenes de datos de eventos de la organización se pueden aplicar a todas las regiones de AWS o a la región actual. Los almacenes de datos de eventos de la organización deben crearse mediante la cuenta de administración o la cuenta del administrador delegado, y, cuando se especifica que se aplican a una organización, se aplican de forma automática a todas las cuentas de miembro de la organización. Las cuentas de miembro no pueden ver el almacén de datos de eventos de la organización, ni pueden modificarlo o eliminarlo. De forma predeterminada, las cuentas de miembro no tienen acceso a los archivos de registro del almacén de datos de eventos de la organización, ni pueden realizar consultas en los almacenes de datos de eventos de la organización. Los almacenes de datos de eventos de la organización no se pueden utilizar para recopilar eventos de fuera de AWS. Para obtener más información, consulte Almacenes de datos de eventos de la organización.

Para obtener más información sobre cómo empezar a CloudTrail usar Lake, consulta Trabajando con AWS CloudTrail Lake esta guía.

CloudTrail senderos

También puede crear un CloudTrail registro para archivar, analizar y responder a los cambios en sus AWS recursos. Los senderos pueden registrar eventos CloudTrail de administración, eventos de datos y eventos de Insights.

Un registro de seguimiento es una configuración que permite la entrega de eventos a un bucket de Amazon S3 que especifique. También puedes publicar y analizar eventos de una ruta con Amazon CloudWatch Logs y Amazon EventBridge. Puede crear rutas con la CloudTrail consolaAWS CLI, la CloudTrail API o la consola.

Puede crear dos tipos de registros de seguimiento para una cuenta de AWS:

Un registro de seguimiento que se aplica a todas las regiones

Cuando crea un registro que se aplica a todas las regiones, CloudTrail registra los eventos en cada región y envía los archivos de registro de CloudTrail eventos a un depósito de S3 que especifique. Si se agrega una región después de crear un registro de seguimiento que se aplica a todas las regiones, la nueva región se incluye automáticamente y también se registran sus eventos. Crear un registro de seguimiento de varias regiones es una práctica recomendada, ya que registra actividad en todas las regiones de su cuenta. Todos los senderos que cree con la CloudTrail consola son multirregionales. Puede actualizar un registro de seguimiento de una sola región para registrar todas las regiones mediante la AWS CLI. Para obtener más información, consulte Creación de un registro de seguimiento en la consola y Conversión de un registro de seguimiento que se aplica a una sola región en uno que se aplique a todas las regiones.

Un registro de seguimiento que se aplica a una región

Al crear un sendero que se aplica a una región, CloudTrail registra solo los eventos de esa región. A continuación, entrega los archivos de registro de CloudTrail eventos a un bucket de Amazon S3 que usted especifique. Solo puede crear un registro de seguimiento de una sola región mediante la AWS CLI. Si crea rutas individuales adicionales, puede hacer que esas rutas entreguen los archivos de registro de CloudTrail eventos en el mismo depósito de Amazon S3 o en depósitos separados. Esta es la opción predeterminada cuando crea una ruta mediante la API AWS CLI o la CloudTrail API. Para obtener más información, consulte Creación, actualización y gestión de senderos con AWS Command Line Interface.

> **Note**
>
> Puede especificar un bucket de Amazon S3 desde cualquier región para ambos tipos de registro de seguimiento.

A partir del 12 de abril de 2019, los registros de seguimiento solo son visibles en las regiones de AWS en las que registren eventos. Si crea un registro de seguimiento que registra eventos en todas las regiones de AWS, aparecerá en la consola en todas las regiones de AWS. Si crea un registro de seguimiento que solo registra los eventos en una región de AWS, solo podrá verlo y administrarlo en esa región de AWS.

Si ha creado una organización en AWS Organizations, puede crear un registro de seguimiento de la organización que registre todos los eventos de todas las cuentas de AWS en dicha organización.

Los registros de seguimiento de la organización se pueden aplicar a todas las regiones de AWS o a la región actual. Los registros de seguimiento de organización deben crearse mediante la cuenta de administración o la cuenta del administrador delegado, y, cuando se especifica que se aplican a una organización, se aplican de forma automática a todas las cuentas miembro de la organización. Las cuentas de miembro pueden ver el registro de seguimiento de la organización, pero no pueden modificarlo ni eliminarlo. De forma predeterminada, las cuentas de miembro no tendrán acceso a los archivos de registros del registro de seguimiento de una organización en el bucket de Amazon S3.

Puede cambiar la configuración de un registro de seguimiento después de crearlo, incluida la opción que indica si registra los eventos de una región o de todas. Para cambiar un registro de seguimiento de una sola región a uno de todas las regiones, o viceversa, debe ejecutar el comando de la AWS CLI update-trail. También puedes cambiar si registra datos o eventos de CloudTrail Insights. El cambio de la opción que indica si el registro de seguimiento registra eventos de una región o de todas afecta a los eventos que se registran. Para obtener más información, consulte Administrar senderos con el AWS CLI (AWS CLI) y Trabajar con archivos de registros de CloudTrail.

De forma predeterminada, los archivos de registro de CloudTrail eventos de las rutas se cifran mediante el cifrado del lado del servidor (SSE) de Amazon S3. También puede optar por cifrar los archivos de registro con una clave AWS Key Management Service (AWS KMS). Puede almacenar sus archivos de registro en el bucket de durante el tiempo que quiera. También puede definir reglas de ciclo de vida de Amazon S3 para archivar o eliminar archivos de registros de forma automática. Si desea recibir notificaciones sobre el envío y la validación de archivos de registros, puede configurar las notificaciones de Amazon SNS.

CloudTrail publica los archivos de registro varias veces por hora, aproximadamente cada 5 minutos. Estos archivos de registro contienen llamadas a la API de servicios en la cuenta que admiten CloudTrail. Para obtener más información, consulte CloudTrail servicios e integraciones compatibles.

> **Note**
>
> CloudTrail normalmente entrega los registros en una media de unos 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el Acuerdo de nivel de servicios de AWS CloudTrail.
> Si configuras mal la ruta (por ejemplo, si no se puede acceder al depósito de S3), CloudTrail intentarás volver a enviar los archivos de registro a tu depósito de S3 durante 30 días. Estos attempted-to-deliver eventos estarán sujetos a los cargos estándar. CloudTrail Para evitar que se le cobre por un registro de seguimiento mal configurado, debe eliminarlo.

CloudTrail captura las acciones realizadas directamente por el usuario o en nombre del usuario por un servicio. AWS Por ejemplo, una llamada a `CreateStack` de AWS CloudFormation puede resultar en llamadas a la API adicionales a Amazon EC2, Amazon RDS, Amazon EBS u otros servicios, según lo requiera la plantilla de AWS CloudFormation. Este comportamiento es normal y previsible. En ese CloudTrail caso, puede identificar si la acción fue realizada por un AWS servicio con el `invokedby` campo.

CloudTrail canales

CloudTrail admite dos tipos de canales:

Canales para la integración de CloudTrail Lake con fuentes de eventos ajenas a AWS

CloudTrail Lake utiliza los canales para llevar a CloudTrail Lake AWS eventos no relacionados con eventos que provienen de socios externos con los que CloudTrail trabajas o de tus propias fuentes. Cuando crea un canal, elige uno o más almacenes de datos de eventos para almacenar los eventos que llegan del origen del canal. Puede cambiar los almacenes de datos de eventos de destino de un canal según sea necesario, siempre que los almacenes de datos de eventos de destino estén configurados para registrar los eventos de actividad de registros. Cuando crea un canal para eventos de un socio externo, proporciona un ARN de canal a la aplicación asociada o de origen. La política de recursos asociada al canal permite que el origen transmita eventos a través del canal. Para obtener más información consulte Creación de una integración con un origen de eventos externo a AWS y `CreateChannel` en la Referencia de la API de AWS CloudTrail.

Canales vinculados a servicios

AWSlos servicios pueden crear un canal vinculado a un servicio para recibir CloudTrail eventos en su nombre. El servicio de AWS que crea el canal vinculado a servicios configura selectores de eventos avanzados para el canal y especifica si este se aplica a todas las regiones o a una sola.

Puedes usar la CloudTrail consola o ver información sobre cualquier canal CloudTrail vinculado AWS CLIa un servicio creado por. Servicios de AWS

Flujo de trabajo de CloudTrail

En esta sección, se proporciona información sobre las características de CloudTrail y las tareas que puede llevar a cabo para estas funciones.

Historial de eventos

Ver el historial de eventos de su cuenta de AWS

Puede ver y buscar los últimos 90 días de eventos registrados por CloudTrail en la consola de CloudTrail o mediante la AWS CLI. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Descargar eventos

Puede descargar un archivo JSON o CSV que contenga hasta los últimos 90 días de eventos de CloudTrail para su cuenta de AWS. Para obtener más información, consulte Descarga de eventos.

CloudTrail Lake

Habilitar CloudTrail Lake

CloudTrail Lake le permite ejecutar consultas precisas basadas en SQL sobre eventos de orígenes de AWS y orígenes externos a AWS. Los eventos se agregan en almacenes de datos de eventos, que son colecciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción de precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción de precio de retención de siete años. CloudTrail Lake forma parte de una solución de auditoría que le ayuda a realizar investigaciones de seguridad y a solucionar problemas. Para obtener más información, consulte Trabajando con AWS CloudTrail Lake.

Creación de un almacén de datos de eventos

Cuando crea un almacén de datos de eventos en CloudTrail Lake, elige el tipo de eventos que desea incluir en él. Para obtener más información, consulte Creación de un almacén de datos de eventos.

Ver los paneles de Lake

Puede utilizar los paneles de CloudTrail Lake para ver los eventos de un almacén de datos de eventos. Puede seleccionar entre varios tipos de paneles. Para obtener más información, consulte Ver los paneles de Lake.

Administración de registro y eventos de datos

Configure sus registros de datos de eventos para que registren eventos de solo lectura, solo escritura o todos los eventos de administración y datos. De forma predeterminada, los almacenes de datos de eventos registran eventos de administración de registros. Para más información, consulte Cree un banco de datos de CloudTrail eventos para eventos, Registro de eventos de administración y Registro de eventos de datos.

Registrar eventos de Insights

Configure sus almacenes de datos de eventos para registrar eventos de Insights y poder identificar y responder a actividades inusuales asociadas a las llamadas a la API de administración. Para más información, consulte Cree un banco de datos de eventos para los eventos de CloudTrail Insights y Registro de eventos de Insights.

Se aplican cargos adicionales por los eventos de Insights. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para más información, consulte Precios de AWS CloudTrail.

Copiar eventos de registro de seguimiento en CloudTrail Lake

Puede copiar los eventos de registro de seguimiento existentes en un almacén de datos de eventos de CloudTrail Lake para crear una instantánea puntual de los eventos del registro de seguimiento. Para obtener más información, consulte Copiar eventos de registro de seguimiento en un almacén de datos de eventos.

Habilitar la federación en un almacén de datos de eventos

Puede federar un almacén de datos de eventos para ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL sobre los datos de eventos con Amazon Athena. Los metadatos de la tabla almacenados en el Catálogo de datos de AWS Glue permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

Detener o iniciar la ingesta de eventos en un almacén de datos de eventos

Puede detener e iniciar la ingesta de eventos en los almacenes de datos de eventos que recopilan eventos de datos y administración de CloudTrail o elementos de configuración de AWS Config. Para obtener más información acerca de cómo detener la ingesta de eventos en la consola de CloudTrail, consulte Detener e iniciar la incorporación de eventos. Para obtener

más información acerca de cómo detener la ingesta de eventos mediante la AWS CLI, consulte Detener la incorporación en un almacén de datos de eventos con la AWS CLI.

Creación de una integración con un origen de eventos externo a AWS

Puede utilizar las integraciones de CloudTrail Lake para registrar y almacenar datos de actividad de los usuarios externos a AWS, desde cualquier origen en sus entornos híbridos, como aplicaciones internas o de SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores. Para obtener información acerca de la creación de una integración en la consola de CloudTrail Lake, consulte Creación de una integración con un origen de eventos externo a AWS. Para obtener información acerca de la creación de una integración mediante la AWS CLI, consulte Crear una integración para registrar eventos externos a AWS con la AWS CLI.

Ver de consultas de ejemplo de Lake en la consola de CloudTrail

La consola de CloudTrail brinda una serie de consultas de ejemplo que pueden ayudarlo a empezar a escribir sus propias consultas. Para obtener más información, consulte Visualización de consultas de ejemplo en la consola de CloudTrail.

Creación o edición de una consulta

Las consultas en CloudTrail se crean en SQL. Puede crear una consulta en la pestaña Editor de CloudTrail Lake escribiendo la consulta en SQL desde cero o abriendo una consulta guardada o de muestra y editándola. Para más información, consulte Creación o edición de una consulta y CloudTrail Restricciones de Lake SQL.

Guardar los resultados de consultas de CloudTrail Lake en un bucket de Amazon S3

Al ejecutar una consulta, puede guardar los resultados de la consulta en un bucket de S3. Para obtener más información, consulte Ejecutar una consulta y guardar los resultados de la consulta.

Descarga de los resultados de consultas guardados

Puede descargar un archivo CSV que contenga los resultados de las consultas de CloudTrail Lake guardados. Para obtener más información, consulte Descargar los resultados de consultas guardados de CloudTrail Lake.

Validación de los resultados de consultas guardados

Puede usar la validación de integridad de los resultados de las consultas de CloudTrail para determinar si los resultados de la consulta se han modificado, eliminado o continúan igual después de que CloudTrail los envió al bucket al S3. Para obtener más información, consulte Validación de los resultados de consultas guardados.

Administración de los permisos de usuario

Utilice AWS Identity and Access Management (IAM) para administrar qué usuarios tienen permisos para crear, configurar o eliminar canales y almacenes de datos de eventos, iniciar y detener la ingesta de eventos y copiar los eventos de registros de seguimiento en un almacén de datos de eventos. Para obtener más información, consulte Otorgar permisos de CloudTrail administración.

Registrar a un administrador delegado para que se encargue de los recursos de CloudTrail de su organización

Puede registrar un administrador delegado para que administre los almacenes de datos de eventos de CloudTrail de su organización. Para obtener más información, consulte Administrador delegado de la organización.

Trabajar con soluciones de los socios

Analice su resultado de CloudTrail con una solución de los socios que se integra con CloudTrail. Las soluciones de los socios ofrecen un amplio conjunto de capacidades, como el seguimiento de cambios, la solución de problemas y el análisis de seguridad. Para obtener más información, consulte la página de socios de AWS CloudTrail.

Registros de seguimiento

Crear un registro de seguimiento

Un registro de seguimiento habilita a CloudTrail a enviar archivos de registros a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de . 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 S3 especificado. Para obtener más información, consulte Creación de un registro de seguimiento para su Cuenta de AWS.

Administración de registro y eventos de datos

Configure sus registros de seguimiento para que registren eventos de solo lectura y solo escritura o todos los eventos de administración y datos. De forma predeterminada, los registros de seguimiento registran eventos de administración. Para más información, consulte Registro de eventos de administración y Registro de eventos de datos.

Registrar eventos de Insights

Configure sus registros de seguimiento para registrar eventos de Insights y poder identificar y responder a actividades inusuales asociadas a las llamadas a la API de administración . Para obtener más información, consulte Registro de eventos de Insights.

Se aplican cargos adicionales por los eventos de Insights. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para más información, consulte Precios de AWS CloudTrail.

Ver eventos de Insights

Después de habilitar CloudTrail Insights en un registro de seguimiento, puede ver hasta 90 días de eventos de Insights mediante la consola de CloudTrail o la AWS CLI. Para obtener más información, consulte Visualizar eventos de CloudTrail Insights para registros de seguimiento.

Descargar eventos de Insights

Después de habilitar CloudTrail Insights en un registro de seguimiento, puede descargar un archivo JSON o CSV que contenga hasta los últimos 90 días de eventos de Insights para su registro de seguimiento. Para obtener más información, consulte Descarga de eventos de Insights.

Copiar eventos de registro de seguimiento en CloudTrail Lake

Puede copiar los eventos de registro de seguimiento existentes en un almacén de datos de eventos de CloudTrail Lake para crear una instantánea puntual de los eventos del registro de seguimiento. Para obtener más información, consulte Copiar los eventos del sendero al CloudTrail lago.

Crear un tema de Amazon SNS y suscribirse a él

Suscríbase a un tema para recibir notificaciones sobre el envío de archivos de registros a su bucket. Amazon SNS puede notificarlo de diversas maneras, por ejemplo, a través de programación mediante Amazon Simple Queue Service. Para obtener más información, consulte Configuración de notificaciones de Amazon SNS para CloudTrail.

> **Note**
>
> Si desea recibir notificaciones de SNS sobre los envíos de archivos de registros de todas las regiones, especifique solo un tema de SNS para el registro de seguimiento. Si desea

procesar todos los eventos mediante programación, consulte Uso de la biblioteca de procesamiento de CloudTrail.

Ver los archivos de registros

Utilice Amazon S3 para recuperar los archivos de registros. Para obtener más información, consulte Obtención y visualización de archivos de registros de CloudTrail.

Monitorear eventos con CloudWatch Logs

Puede configurar el registro de seguimiento para enviar eventos a CloudWatch Logs. A continuación, puede utilizar CloudWatch Logs a fin de monitorear su cuenta para eventos y llamadas a la API específicos. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

> **Note**
>
> Si configura un registro de seguimiento que se aplica a todas las regiones para que envíe eventos a un grupo de registro de Registros de CloudWatch, CloudTrail envía eventos de todas las regiones a un solo grupo de registro.

Habilitar el cifrado de registro

El cifrado de archivos de registros proporciona una capa adicional de seguridad para sus archivos de registros. Para obtener más información, consulte Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS).

Habilitar la integridad de los archivos de registros

La validación de la integridad de los archivos de registros lo ayuda a verificar que los archivos de registros no se hayan modificado desde que CloudTrail los envió. Para obtener más información, consulte Validar la integridad de los archivos de registros de CloudTrail.

Compartir archivos de registros con otras cuentas de AWS

Puede compartir archivos de registros entre cuentas. Para obtener más información, consulte Compartir archivos de registro de CloudTrail entre cuentas de AWS.

Agrupar archivos de registros de varias cuentas

Puede agrupar archivos de registros de varias cuentas en un solo bucket. Para obtener más información, consulte Recepción de archivos de CloudTrail registro de varias cuentas.

Administración de los permisos de usuario

Utilice AWS Identity and Access Management (IAM) a fin de administrar los permisos de los usuarios para crear, configurar o eliminar registros de seguimiento, iniciar y detener la generación de registros y tener acceso a los buckets que contienen los archivos de registros. Para obtener más información, consulte Otorgar permisos de CloudTrail administración.

Registrar a un administrador delegado para que se encargue de los recursos de CloudTrail de su organización

Puede registrar un administrador delegado para que administre los registros de seguimiento de CloudTrail de su organización. Para obtener más información, consulte Administrador delegado de la organización.

Trabajar con soluciones de los socios

Analice su resultado de CloudTrail con una solución de los socios que se integra con CloudTrail. Las soluciones de los socios ofrecen un amplio conjunto de capacidades, como el seguimiento de cambios, la solución de problemas y el análisis de seguridad. Para obtener más información, consulte la página de socios de AWS CloudTrail.

CloudTrail conceptos

En esta sección se resumen los conceptos básicos relacionados con. CloudTrail

Contenido

- ¿Qué son los CloudTrail eventos?
  - ¿Qué son los eventos de administración?
  - ¿Qué son los eventos de datos?
  - ¿Qué son los eventos de Insights?
    - ¿Cómo puedo ver eventos de Insights para los registros de seguimiento y los almacenes de datos de eventos?
- ¿Qué es el historial de CloudTrail eventos?
- ¿Qué son los registros de seguimiento?

- ¿Qué son los registros de seguimiento de organización?
- ¿Cómo se gestiona CloudTrail?
  - CloudTrail consola
  - CloudTrail CLI
  - CloudTrail APIs
  - AWS SDK
  - ¿Por qué usar etiquetas para CloudTrail los recursos?
- ¿Cómo se controla el acceso a? CloudTrail
- ¿Cómo registra los eventos de administración o de datos?
- ¿Cómo se registran los eventos de CloudTrail Insights?
- ¿Cómo se ejecutan consultas complejas sobre los eventos registrados por CloudTrail?
- ¿Cómo se realiza la supervisión CloudTrail?
  - CloudWatch Registros EventBridge, y CloudTrail
- ¿Cómo se CloudTrail comporta a nivel regional y global?
  - ¿Cuáles son las ventajas de aplicar un registro de seguimiento a todas las regiones?
  - ¿Qué sucede cuando se aplica un registro de seguimiento a todas las regiones?
  - Varios registros de seguimiento por región
  - AWS Security Token Service y CloudTrail
- Eventos de servicios globales
- ¿Cómo CloudTrail se relaciona con otros servicios AWS de supervisión?
- Soluciones de socios

¿Qué son los CloudTrail eventos?

Un evento en CloudTrail es el registro de una actividad en una AWS cuenta. Esta actividad puede ser una acción realizada por una identidad de IAM o un servicio que pueda supervisarse. CloudTrail CloudTraillos eventos proporcionan un historial de la actividad de las cuentas API y ajenas a la API realizada a través de los AWS SDK AWS Management Console, las herramientas de línea de comandos y otros servicios. AWS Hay tres tipos de eventos que se pueden iniciar sesión CloudTrail: eventos de administración, eventos de datos y eventos de CloudTrail Insights. De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos registran los eventos de administración, pero no los eventos de datos o de Insights.

Todos los tipos de eventos utilizan un formato de registro CloudTrail JSON.

Para obtener información sobre la Servicios de AWS integración con CloudTrail, consulteAWS temas de servicio para CloudTrail.

¿Qué son los eventos de administración?

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su AWS cuenta. Se denominan también operaciones del plano de control.

Algunos ejemplos de eventos de administración son los siguientes:

- Configurar la seguridad (por ejemplo, las operaciones AWS Identity and Access Management `AttachRolePolicy` de la API).
- Registro de dispositivos (por ejemplo, operaciones de la API `CreateDefaultVpc` de Amazon EC2).
- Configuración de reglas para el enrutamiento de datos (por ejemplo, operaciones de la API `CreateSubnet` de Amazon EC2).
- Configurar el registro (por ejemplo, las operaciones AWS CloudTrail `CreateTrail` de la API).

Los eventos de administración también pueden incluir eventos no generados por la API que se producen en su cuenta. Por ejemplo, cuando un usuario inicia sesión en tu cuenta, CloudTrail registra el `ConsoleLogin` evento. Para obtener más información, consulte Eventos no generados por la API capturados por CloudTrail. Para obtener una lista de los eventos de administración que CloudTrail registran los AWS servicios, consulteCloudTrail servicios e integraciones compatibles.

¿Qué son los eventos de datos?

Los eventos de datos proporcionan información sobre las operaciones realizadas en un recurso o dentro de él. Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen.

Algunos ejemplos de eventos de datos son los siguientes:

- Actividad de la API en cuanto a objetos de Amazon S3 (por ejemplo, las operaciones `GetObject`, `DeleteObject` y `PutObject` de la API) en buckets y objetos en buckets.
- AWS Lambda actividad de ejecución de funciones (la `Invoke` API).

- CloudTrail `PutAuditEvents`actividad en un canal de CloudTrail Lake que se utiliza para registrar eventos del exterior AWS.
- Operaciones de la API `Publish` y `PublishBatch` de Amazon SNS sobre temas.

En la siguiente tabla, se muestran los tipos de eventos de datos disponibles para los registros de seguimiento y los almacenes de datos de eventos. En la columna Tipo de evento de datos (consola), se muestra la selección adecuada en la consola. La columna de valores resources.type muestra el `resources.type` valor que deberías especificar para incluir eventos de datos de ese tipo en tu almacén de datos de rutas o eventos mediante las AWS CLI API o. CloudTrail

En el caso de los registros de seguimiento, puede utilizar selectores de eventos básicos o avanzados para registrar eventos de datos para buckets de Amazon S3 y objetos de bucket, funciones de Lambda y tablas de DynamoDB (se muestran en las tres primeras filas de la tabla). Solo puede usar selectores de eventos avanzados para registrar los tipos de eventos de datos que se muestran en las filas restantes.

En el caso de los almacenes de datos de eventos, puede utilizar selectores de eventos avanzados para que se incluyan eventos de datos únicamente.

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon DynamoDB	Actividad de la API a nivel de objeto de Amazon DynamoDB en las tablas (por ejemplo `PutItem` `DeleteItem` , y las operaciones de la API). `UpdateItem`	DynamoDB	`AWS::DynamoDB::Table`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	Note Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterm		

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	inada. Para excluir los eventos de streaming, añada un filtro en el campo. `eventName`		
AWS Lambda	AWS Lambda actividad de ejecución de funciones (la `Invoke` API).	Lambda	`AWS::Lambda::Function`
Amazon S3	Actividad de la API en cuanto a objetos de Amazon S3 (por ejemplo, las operaciones `GetObject` , `DeleteObject` y `PutObject` de la API) en buckets y objetos en buckets.	S3	`AWS::S3::Object`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS AppConfig	AWS AppConfig Actividad de la API para operaciones de configuración, como las llamadas a `StartConfiguration Session` y `GetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Intercambio de datos B2B	Actividad de la API de intercambio de datos entre empresas para operaciones de Transformer, como las llamadas a `GetTransformerJob` y `StartTransformerJob` .	Intercambio de datos entre empresas	`AWS::B2BI::Transformer`
Amazon Bedrock	Actividad de la API de Amazon Bedrock en un alias de agente.	Alias de agente de Bedrock	`AWS::Bedrock::AgentAlias`
	Actividad de la API de Amazon Bedrock en una base de conocimientos.	Base de conocimientos de Bedrock	`AWS::Bedrock::KnowledgeBase`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon CloudFront	CloudFront Actividad de la API en un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Actividad de la API en un espacio de nombres.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Actividad de la API en un servicio.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` actividad en un canal de CloudTrail Lake que se utiliza para registrar eventos externos AWS.	CloudTrail	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Actividad CodeWhisperer de la API de Amazon en una personalización.	CodeWhisperer personalización	`AWS::CodeWhisperer::Customization`
	Actividad CodeWhisperer de la API de Amazon en un perfil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon Cognito	Actividad de la API de Amazon Cognito en los grupos de identidades de Amazon Cognito.	Grupos de identidades de Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Actividad de la API de Amazon DynamoDB en los flujos.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	API directas de Amazon Elastic Block Store (EBS), como `PutSnapshotBlock`, `GetSnapshotBlock` y `ListChangedBlocks` en instantáneas de Amazon EBS.	API directas de Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Actividad de la API de Amazon EMR en un espacio de trabajo de registros de escritura anticipada.	Espacio de trabajo de registro de escritura anticipada de EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Actividad de la API de Amazon FinSpace en entornos.	FinSpace	`AWS::FinSpace::Environment`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS Glue	AWS Glue Actividad de la API en tablas creadas por Lake Formation. **Note** AWS Glue Los eventos de datos para tablas actualmente solo se admiten en las siguientes regiones: • Este de EE. UU. (Norte de Virginia) • Este de EE. UU. (Ohio) • Oeste de EE. UU. (Oregón) • Europa (Irlanda)	Lake Formation	`AWS::Glue::Table`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	• Región de Asia-Pacífico (Tokio)		
Amazon GuardDuty	Actividad GuardDuty de la API de Amazon para un detector.	GuardDuty detector	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Actividad de la API en los almacenes de datos.	Almacén de datos de imágenes médicas	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Actividad de la API en los certificados.	Certificado IoT	`AWS::IoT::Certificate`
	AWS IoT Actividad de la API en las cosas.	Cosa de IoT	`AWS::IoT::Thing`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS IoT Greengrass Version 2	Actividad de la API de Greengrass desde un dispositivo principal de Greengrass en una versión de componentes. **Note** Greengrass no registra los eventos de acceso denegado.	Versión del componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
	Actividad de la API de Greengrass desde un dispositivo principal de Greengrass en una implementación. **Note** Greengrass no registra los eventos de acceso denegado.	Despliegue de IoT Greengrass	`AWS::GreengrassV2::Deployment`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS IoT SiteWise	Actividad de SiteWise la API de IoT en los activos.	SiteWise Activo de IoT	`AWS::IoTSiteWise::Asset`
	Actividad SiteWise de la API de IoT en series temporales.	Series SiteWise temporales de IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Actividad TwinMaker de la API de IoT en una entidad.	TwinMaker Entidad de IoT	`AWS::IoTTwinMaker::Entity`
	Actividad de TwinMaker la API de IoT en un espacio de trabajo.	TwinMaker Espacio de trabajo de IoT	`AWS::IoTTwinMaker::Workspace`
Clasificación de Amazon Kendra Intelligent	Actividad de la API de Amazon Kendra Intelligent Ranking en los planes de ejecución de nuevas puntuaciones.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (para Apache Cassandra)	Actividad de la API de Amazon Keyspaces en una tabla.	Mesa Cassandra	`AWS::Cassandra::Table`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon Kinesis	Actividad de la API de Amazon Kinesis en transmisiones de video, como llamadas a `GetMedia` y `PutMedia`.	Kinesis Video Streams	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Actividad de la API de Amazon Managed Blockchain en una red.	Red de Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Llamadas JSON-RPC de Amazon Managed Blockchain en nodos de Ethereum, como `eth_getBalance` o `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Gráfico de Amazon Neptune	Actividades de la API de datos, por ejemplo, consultas, algoritmos o búsquedas vectoriales, en un gráfico de Neptune.	Gráfico de Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Conector para la actividad de la API de Active Directory.	AWS Private CA Conector para Active Directory	`AWS::PCAConnectorAD::Connector`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon Q Business	Actividad de la API de Amazon Q Business en una aplicación.	Aplicación de Amazon Q Business	`AWS::QBusiness::Application`
	Actividad de la API de Amazon Q Business en un origen de datos.	Origen de datos de Amazon Q Business	`AWS::QBusiness::DataSource`
	Actividad de la API de Amazon Q Business en un índice.	Índice de Amazon Q Business	`AWS::QBusiness::Index`
	Actividad de la API de Amazon Q Business en una experiencia web.	Experiencia web de Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Actividad de la API de Amazon RDS en un clúster de base de datos.	API de datos de RDS: clúster de base de datos	`AWS::RDS::DBCluster`
Amazon S3	Actividad de la API de Amazon S3 en los puntos de acceso.	Punto de acceso de S3	`AWS::S3::AccessPoint`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	Actividad de la API en los puntos de acceso de Amazon S3 Object Lambda, como las llamadas a `CompleteMultipartUpload` y `GetObject` .	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 en Outposts	Actividad de la API en cuanto a objetos de Amazon S3 en Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Actividad de Amazon en los puntos finales.	SageMaker punto final	`AWS::SageMaker::Endpoint`
	Actividad SageMaker de la API de Amazon en tiendas destacadas.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	Actividad de la SageMaker API de Amazon en componentes de prueba de experimentos.	SageMaker métricas (componente de prueba de experimentos)	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Operaciones de la API `Publish` de Amazon SNS en los puntos de conexión de la plataforma.	Punto de conexión de la plataforma de SNS	`AWS::SNS::PlatformEndpoint`
	Operaciones de la API `Publish` y `PublishBatch` de Amazon SNS sobre temas.	Tema de SNS	`AWS::SNS::Topic`
Amazon SQS	Actividad de la API de Amazon SQS en los mensajes.	SQS	`AWS::SQS::Queue`
AWS Supply Chain	AWS Supply Chain Actividad de la API en una instancia.	Cadena de suministro	`AWS::SCN::Instance`
Amazon SWF	Actividad de la API Amazon SWF en los dominios.	Dominio SWF	`AWS::SWF::Domain`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS Systems Manager	Actividad de la API de Systems Manager en los canales de control.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Actividad de la API de Systems Manager en los nodos gestionados.	Nodo gestionado por Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Actividad de la API `Query` de Amazon Timestream en las bases de datos.	Base de datos de Timestream	`AWS::Timestream::Database`
	Actividad de la API `Query` de Amazon Timestream en las tablas.	Tabla de Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Actividad de la API de Amazon Verified Permissions en un almacén de políticas.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Actividad de la API de Thin Client en un dispositivo.	Dispositivo de cliente ligero	`AWS::ThinClient::Device`
	WorkSpaces Actividad de la API de Thin Client en un entorno.	Entorno de cliente ligero	`AWS::ThinClient::Environment`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS X-Ray	Actividad de la API X-Ray en las trazas.	Rastro de rayos X	`AWS::XRay::Trace`

El registro de los eventos de datos está deshabilitado de forma predeterminada cuando crea un registro de seguimiento o un almacén de datos de eventos. Para registrar CloudTrail los eventos de datos, debe añadir de forma explícita los recursos o tipos de recursos compatibles para los que desea recopilar la actividad. Para más información, consulte Creación de un registro de seguimiento y Cree un banco de datos de CloudTrail eventos para eventos.

Se aplican cargos adicionales para registrar eventos de datos. Para CloudTrail conocer los precios, consulte AWS CloudTrail Precios.

¿Qué son los eventos de Insights?

CloudTrail Los eventos de Insights capturan la actividad inusual de la tasa de llamadas a la API o la tasa de errores en su AWS cuenta mediante el análisis CloudTrail de la actividad de administración. Los eventos de Insights proporcionan información relevante, como la API asociada, el código de error, la hora del incidente y las estadísticas, que lo ayuda a conocer la actividad inusual y actuar en consecuencia. A diferencia de otros tipos de eventos que se capturan en un CloudTrail registro o un banco de datos de eventos, los eventos de Insights solo se registran cuando CloudTrail detecta cambios en el uso de la API de su cuenta o en el registro de la tasa de errores que difieren significativamente de los patrones de uso típicos de la cuenta.

Entre los ejemplos de actividad que podrían generar los eventos de Insights se incluyen los siguientes:

- Por lo general, su cuenta registra no más de 20 llamadas a la API `deleteBucket` de Amazon S3 por minuto, pero comienza a registrar un promedio de 100 llamadas a la API `deleteBucket` por minuto. Se registra un evento de Insights al inicio de la actividad inusual y se registra otro evento de Insights para marcar el final de la actividad inusual.
- Por lo general, su cuenta registra 20 llamadas por minuto a la API `AuthorizeSecurityGroupIngress` de Amazon EC2, pero comienza a registrar cero llamadas

a `AuthorizeSecurityGroupIngress`. Un evento de Insights se registra al inicio de la actividad inusual y diez minutos más tarde, cuando finaliza la actividad inusual, se registra otro evento de Insights para marcar el final de la actividad inusual.

- Normalmente, su cuenta registra menos de uno error `AccessDeniedException` en un periodo de siete días en la API AWS Identity and Access Management , `DeleteInstanceProfile`. Su cuenta comienza a registrar un promedio de 12 errores `AccessDeniedException` por minuto en la llamada a la API `DeleteInstanceProfile`. Se registra un evento de Insights al inicio de la actividad de tasa de error inusual y se registra otro evento de Insights para marcar el final de la actividad inusual.

Estos ejemplos se ofrecen únicamente con fines ilustrativos. Sus resultados pueden variar según su caso de uso.

Para registrar los eventos de CloudTrail Insights, debes habilitar explícitamente los eventos de Insights en un banco de datos de eventos o seguimiento nuevo o existente. Para obtener más información acerca de la creación de un registro de seguimiento, consulte Creación de un registro de seguimiento. Para obtener más información acerca de la creación de un almacén de datos de eventos, consulte Cree un banco de datos de eventos para los eventos de CloudTrail Insights.

Se aplican cargos adicionales por los eventos de Insights. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para obtener más información, consulte AWS CloudTrail Precios.

¿Cómo puedo ver eventos de Insights para los registros de seguimiento y los almacenes de datos de eventos?

CloudTrail admite los eventos de Insights tanto para los senderos como para los almacenes de datos de eventos; sin embargo, existen algunas diferencias en la forma de ver y acceder a los eventos de Insights.

Visualización de eventos de Insights para registros de seguimiento

Si tienes activados los eventos de Insights en una ruta y CloudTrail detecta una actividad inusual, los eventos de Insights se registran en una carpeta o prefijo diferente en el depósito de S3 de destino de tu ruta. También puede ver el tipo de información y el período de tiempo del incidente al ver los eventos de Insights en la CloudTrail consola. Para obtener más información, consulte Visualizar eventos de CloudTrail Insights para registros de seguimiento en la consola de CloudTrail.

Visualización de eventos de Insights para los almacenes de datos de eventos

Para registrar los eventos de Insights en CloudTrail Lake, necesita un almacén de datos de eventos de destino que registre los eventos de Insights y un banco de datos de eventos de origen que habilite Insights y registre los eventos de administración. Para obtener más información, consulte Cree un banco de datos de eventos para los eventos de CloudTrail Insights.

Si tiene CloudTrail Insights activado en un banco de datos de eventos de origen y CloudTrail detecta actividades inusuales, CloudTrail envía los eventos de Insights al banco de datos de eventos de destino. A continuación, puede consultar el almacén de datos de eventos de destino para obtener información sobre sus eventos de Insights y, de forma opcional, puede guardar los resultados de las consultas en un bucket de Amazon S3. Para más información, consulte Creación o edición de una consulta y Visualización de consultas de ejemplo en la consola de CloudTrail.

Puedes ver el panel de control de CloudTrail Lake para visualizar los eventos de Insights en el banco de datos de eventos de tu destino. Para obtener más información acerca de los paneles de Lake, consulte Ver los paneles de Lake.

¿Qué es el historial de CloudTrail eventos?

CloudTrail el historial de eventos proporciona un registro visible, buscable, descargable e inmutable de los últimos 90 días de eventos de CloudTrail gestión en un. Región de AWS Puedes usar este historial para ver las acciones realizadas en tu AWS cuenta en los AWS SDK AWS Management Console, las herramientas de línea de comandos y otros servicios. AWS Puedes personalizar la vista del historial de eventos en la CloudTrail consola seleccionando las columnas que se muestran. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

¿Qué son los registros de seguimiento?

Una ruta es una configuración que permite la entrega de CloudTrail eventos a un bucket de Amazon S3, a CloudWatch Logs y a Amazon EventBridge. Puede utilizar un registro para filtrar los CloudTrail eventos que desea que se envíen, cifrar los archivos de registro de CloudTrail eventos con una AWS KMS clave y configurar las notificaciones de Amazon SNS para la entrega de los archivos de registro. Para obtener más información acerca de cómo crear y administrar un registro de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS.

¿Qué son los registros de seguimiento de organización?

Un registro de la organización es una configuración que permite enviar CloudTrail eventos de la cuenta de administración y de todas las cuentas de los miembros de una AWS Organizations

organización al mismo bucket de Amazon S3, a los mismos CloudWatch registros y a Amazon EventBridge. La creación de un registro de seguimiento de organización lo ayuda a definir una estrategia uniforme de registro de eventos para su organización.

Todos los registros organizativos creados con la consola son registros organizativos multirregionales que registran los eventos de las cuentas Regiones de AWS habilitadas de cada miembro de la organización. Para registrar los eventos en todas las AWS particiones de su organización, cree un registro de organización multirregional en cada partición. Puede crear un registro organizativo de una sola región o de varias regiones mediante el. AWS CLI Si crea un sendero de una sola región, registrará la actividad únicamente en el sendero Región de AWS (también denominado región de origen).

Aunque la mayoría Regiones de AWS están habilitadas de forma predeterminada Cuenta de AWS, debes habilitar manualmente determinadas regiones (también denominadas regiones de suscripción). Para obtener información sobre qué regiones están habilitadas de forma predeterminada, consulte Consideraciones antes de habilitar o deshabilitar las regiones en la Guía de AWS Account Management referencia. Para ver la lista de regiones CloudTrail compatibles, consulteCloudTrail regiones compatibles.

Cuando crea un registro de la organización, se crea una copia del registro con el nombre que le dé en las cuentas de los miembros que pertenecen a su organización.

- Si el registro de la organización es para una sola región y la región de origen de la ruta no es una región opcional, se crea una copia de la ruta en la región de origen de la ruta de la organización, en la cuenta de cada miembro.
- Si el registro de la organización es para una región única y la región de origen del sendero es una región opcional, se crea una copia del registro en la región de origen del sendero de la organización, en las cuentas de los miembros que han habilitado esa región.
- Si la ruta organizativa es multirregional y la región de origen de la ruta no es una región opcional, se crea una copia de la ruta en cada una de las cuentas habilitadas Región de AWS en cada cuenta de miembro. Cuando la cuenta de un miembro habilita una región opcional, se crea una copia del recorrido multiregional en la región que acaba de registrarse para la cuenta del miembro una vez que se haya completado la activación de esa región.
- Si el registro de la organización es multirregional y la región de origen es una región opcional, las cuentas de los miembros no enviarán la actividad al registro de la organización a menos que opten por hacerlo en el Región de AWS lugar en el que se creó el registro multirregional. Por ejemplo, si creas una ruta multirregional y eliges la región de Europa (España) como región de origen de la

ruta, solo las cuentas de los miembros que hayan habilitado la región de Europa (España) en su cuenta enviarán la actividad de su cuenta a la ruta de la organización.

> **Note**
>
> CloudTrail crea registros organizativos en las cuentas de los miembros incluso si se produce un error en la validación de un recurso. Entre los ejemplos de errores de validación se incluyen los siguientes:
>
> - una política de bucket de Amazon S3 incorrecta
> - una política de temas de Amazon SNS incorrecta
> - incapacidad para realizar la entrega a un CloudWatch grupo de registros
> - permiso insuficiente para cifrar mediante una clave KMS
>
> Una cuenta de miembro con CloudTrail permisos puede ver cualquier error de validación del registro de una organización consultando la página de detalles del registro en la CloudTrail consola o ejecutando el AWS CLI get-trail-statuscomando.

Los usuarios con CloudTrail permisos en las cuentas de los miembros podrán ver los registros de la organización (incluido el ARN de la ruta) cuando inicien sesión en la AWS CloudTrail consola desde sus AWS cuentas o cuando ejecuten AWS CLI comandos como `describe-trails` (aunque las cuentas de los miembros deben usar el ARN para el registro de la organización y no el nombre cuando usen el). AWS CLI Sin embargo, los usuarios de las cuentas de los miembros no tendrán permisos suficientes para eliminar los registros de la organización, activar o desactivar el inicio de sesión, cambiar los tipos de eventos que se registran o alterar de algún modo los registros de la organización. Para obtener más información sobre AWS Organizations, consulte Terminología y conceptos de Organizations. Para obtener más información acerca de la creación y el uso de registros de seguimiento de organización, consulte Creación de un registro de seguimiento para una organización.

¿Cómo se gestiona CloudTrail?

CloudTrail consola

Puede utilizar y gestionar el servicio con la AWS CloudTrail consola. La consola proporciona una interfaz de usuario para realizar muchas CloudTrail tareas, tales como:

- Ver los eventos recientes y el historial de eventos de tu AWS cuenta.
- Descarga de un archivo filtrado o completo de los últimos 90 días de eventos administración.
- Creación y edición de CloudTrail rutas.
- Creación y edición de almacenes de datos de eventos de CloudTrail Lake.
- Ejecución de consultas en almacenes de datos de eventos
- Configuración de CloudTrail senderos, que incluyen:
  - Selección de un bucket de Amazon S3 para registros de seguimiento
  - Establecer un prefijo.
  - Configuración de la entrega a CloudWatch Logs.
  - Uso de AWS KMS claves para cifrar los datos de los senderos.
  - Habilitación de las notificaciones de Amazon SNS para el envío de archivos de registros a registros de seguimiento
  - Agregar y administrar etiquetas para los registros de seguimiento.
- Configuración de los almacenes de datos de eventos de CloudTrail Lake, que incluyen:
  - Integrar los almacenes de datos de eventos con CloudTrail socios o con sus propias aplicaciones para registrar eventos de fuentes externas AWS.
  - Uso de AWS KMS claves para cifrar los datos del almacén de datos de eventos.
  - Agregar y administrar etiquetas para sus almacenes de datos de eventos.

A partir del 12 de abril de 2019, los senderos solo se podrán ver en AWS las regiones en las que se registren los eventos. Si creáis un registro que registre los eventos en todas AWS las regiones, aparecerá en la consola en todas AWS las regiones. Si creas un registro que solo registre los eventos en una sola AWS región, solo podrás verlo y administrarlo en esa AWS región.

Para obtener más información sobre el AWS Management Console, consulte AWS Management Console.

CloudTrail CLI

AWS Command Line Interface Es una herramienta unificada con la que puede interactuar CloudTrail desde la línea de comandos. Para más información, consulte la Guía del usuario de AWS Command Line Interface. Para obtener una lista completa de los comandos de CloudTrail CLI, consulte Comandos disponibles.

CloudTrail APIs

Además de la consola y la CLI, también puede utilizar las API CloudTrail RESTful para programar CloudTrail directamente. Para obtener más información, consulte la Referencia de la API de AWS CloudTrail.

AWS SDK

Como alternativa al uso de la CloudTrail API, puedes usar uno de los AWS SDK. Cada SDK se compone de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas. Los SDK proporcionan una forma cómoda de crear un acceso programático a. CloudTrail Por ejemplo, puede usar los SDK para firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. A fin de obtener más información, consulte la página de Herramientas para Amazon Web Services.

¿Por qué usar etiquetas para CloudTrail los recursos?

Una etiqueta es una clave definida por el cliente y un valor opcional que se puede asignar a AWS recursos, como CloudTrail rutas, almacenes de datos de eventos y canales, depósitos de Amazon S3 utilizados para almacenar archivos de CloudTrail registro, AWS Organizations organizaciones y unidades organizativas, y muchos más. Si agrega las mismas etiquetas a los registros de seguimiento y a los buckets de Amazon S3 que utiliza para almacenar los archivos de registros de los registros de seguimiento, puede hacer que sea más sencillo administrar, buscar y filtrar estos recursos con AWS Resource Groups. Puede implementar estrategias de etiquetado que le ayuden a encontrar y administrar los recursos de forma sencilla, coherente y eficaz. Para obtener más información, consulte Estrategias de etiquetado de AWS.

¿Cómo se controla el acceso a? CloudTrail

AWS Identity and Access Management es un servicio web que permite a los clientes de Amazon Web Services (AWS) controlar de forma segura el acceso a AWS los recursos. Con IAM, puede gestionar de forma centralizada los permisos que controlan a qué CloudTrail recursos pueden acceder los usuarios. Para obtener más información acerca del control de los permisos de usuario, consulte Controlar los permisos de usuario para los registros de seguimiento de CloudTrail.

¿Cómo registra los eventos de administración o de datos?

De forma predeterminada, las rutas registran los eventos de administración de tu AWS cuenta y no incluyen los eventos de datos. Puede elegir crear registros de seguimiento para que registren los

eventos de datos o actualizar los existentes para que lo hagan. Solo los eventos que coincidan con la configuración de su ruta se envían a su bucket de Amazon S3 y, opcionalmente, a un grupo de CloudWatch registros de Amazon Logs. Si el evento no coincide con la configuración de un registro de seguimiento, este no registra el evento. Para obtener más información, consulte Trabajar con archivos de registros de CloudTrail.

¿Cómo se registran los eventos de CloudTrail Insights?

AWS CloudTrail Insights ayuda a AWS los usuarios a identificar y responder a volúmenes inusuales de llamadas a la API o a los errores registrados en las llamadas a la API mediante el análisis continuo CloudTrail de los eventos de administración. Un evento de Insights es un registro de niveles inusuales de actividad de API de administración `write` o niveles inusuales de errores devueltos en la actividad de la API de administración. De forma predeterminada, los registros y los almacenes de datos de eventos no registran los eventos de CloudTrail Insights. En la consola, puede elegir registrar eventos de Insights cuando cree o actualice un registro de seguimiento o un almacén de datos de eventos. Cuando utilizas la CloudTrail API, puedes registrar los eventos de Insights editando la configuración de un banco de datos de senderos o eventos existente con la `PutInsightSelectors`API. Se aplican cargos adicionales por registrar los eventos de CloudTrail Insights. Para obtener más información, consulte Registro de eventos de Insights y Precios de AWS CloudTrail.

¿Cómo se ejecutan consultas complejas sobre los eventos registrados por CloudTrail?

CloudTrail Lake le permite ejecutar consultas detalladas basadas en SQL sobre sus eventos y registrar los eventos de fuentes externas AWS, incluidas las de sus propias aplicaciones y de los socios con los que están integrados. CloudTrail No necesita tener una ruta configurada en su cuenta para usar Lake. CloudTrail Los almacenes de datos de eventos son colecciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción Precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción Precio de retención de siete años. Puede guardar las consultas de Lake para utilizarlas en el futuro y ver los resultados de las consultas durante un máximo de siete días. También puedes guardar los resultados de las consultas en un depósito de Amazon Simple Storage Service. CloudTrail Lake también puede almacenar eventos de una organización AWS Organizations en un almacén de datos de eventos o eventos de varias regiones y cuentas. CloudTrail Lake forma parte de una solución de auditoría que le ayuda a realizar investigaciones de seguridad

y solucionar problemas. Para obtener más información, consulte Trabajando con AWS CloudTrail Lake.

¿Cómo se realiza la supervisión CloudTrail?

CloudWatch Registros EventBridge, y CloudTrail

Amazon CloudWatch es un servicio web que recopila y realiza un seguimiento de las métricas para supervisar los recursos de Amazon Web Services (AWS) y las aplicaciones en las que se ejecuta AWS. Amazon CloudWatch Logs es una función CloudWatch que puedes usar específicamente para monitorear los datos de registro. La integración con CloudWatch Logs permite CloudTrail enviar los eventos que contienen la actividad de la API en su AWS cuenta a un grupo de CloudWatch registros de Logs. CloudTrail los eventos que se envían a CloudWatch Logs pueden activar alarmas según los filtros de métricas que definas. Si lo desea, puede configurar CloudWatch las alarmas para enviar notificaciones o realizar cambios en los recursos que está supervisando en función de los eventos del flujo de registro que extraigan los filtros de métricas. Con CloudWatch los registros, también puede realizar un seguimiento de CloudTrail los eventos junto con los eventos del sistema operativo, las aplicaciones u otros AWS servicios que se envían a CloudWatch los registros. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Amazon EventBridge es un AWS servicio que ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. En EventBridge, puede crear reglas que respondan a los eventos registrados por CloudTrail. Para obtener más información, consulta Crear una regla en Amazon EventBridge.

Puedes ofrecer eventos a los que estés suscrito EventBridge durante tu recorrido. Cuando cree una regla con la EventBridge consola, elija el tipo de `AWS API Call via CloudTrail` detalle para entregar los CloudTrail datos y los eventos de gestión, o el tipo de `AWS Insight via CloudTrail` detalle para entregar los eventos de Insights.

Para registrar eventos con un valor de detail-type `AWS API Call via CloudTrail`, debe tener un registro activo que registre los eventos de administración o de datos. Para obtener más información sobre cómo crear y administrar un registro de seguimiento, consulte Creación de un registro de seguimiento.

Para registrar eventos con un valor de detail-type `AWS Insight via CloudTrail`, debe tener un registro activo que registre los eventos de Insights. Para obtener información sobre cómo registrar eventos de Insights, consulte Registro de eventos de Insights.

¿Cómo se CloudTrail comporta a nivel regional y global?

Los registros de seguimiento se pueden aplicar a todas las regiones o a una sola. Como práctica recomendada se aconseja crear los registros de seguimiento que se aplican a todas las regiones en la partición de AWS en la que trabaja. Esta es la configuración predeterminada al crear una ruta en la CloudTrail consola.

> **Note**
>
> Activar una ruta significa crear una ruta e iniciar la entrega de los archivos de registro de CloudTrail eventos a un bucket de Amazon S3. En la CloudTrail consola, el registro se activa automáticamente al crear una ruta.

¿Cuáles son las ventajas de aplicar un registro de seguimiento a todas las regiones?

Un sendero que se aplique a todas AWS las regiones tiene las siguientes ventajas:

- Los valores de configuración del registro de seguimiento se aplican de forma sistemática a todas las regiones de AWS .
- Recibe los CloudTrail eventos de todas AWS las regiones en un único bucket de Amazon S3 y, de forma opcional, en un grupo de CloudWatch registros.
- Usted administra la configuración de los senderos de todas AWS las regiones desde una sola ubicación.
- Recibirás inmediatamente los eventos de una nueva AWS región. Cuando se lanza una nueva AWS región, crea CloudTrail automáticamente una copia de todas las rutas de tu región para ti en la nueva región con la misma configuración que la ruta original.
- No necesitas crear senderos en AWS regiones que no utilices con frecuencia para detectar actividades inusuales. Cualquier actividad en cualquier AWS región se registra en una ruta que se aplica a todas AWS las regiones.

¿Qué sucede cuando se aplica un registro de seguimiento a todas las regiones?

Al aplicar un sendero a todas AWS las regiones, CloudTrail utiliza el sendero que haya creado en una región concreta para crear senderos con configuraciones idénticas en todas las demás regiones de la AWS partición en la que esté trabajando.

Esto tiene las siguientes consecuencias:

- CloudTrail entrega los archivos de registro de la actividad de las cuentas de todas AWS las regiones al único depósito de Amazon S3 que especifique y, opcionalmente, a un grupo de CloudWatch registros.
- Si ha configurado un tema de Amazon SNS para la ruta, las notificaciones de SNS sobre las entregas de archivos de registro en todas las AWS regiones se envían a ese único tema de SNS.
- Si lo ha activado, la validación de la integridad de los archivos de registro estará habilitada para el registro en todas las regiones. AWS Para obtener más información, consulte Validar la integridad de los archivos de registros de CloudTrail.

Independientemente de si una ruta es multirregional o de una sola región, los eventos que se envían a Amazon EventBridge se reciben en el bus de eventos de cada región, en lugar de en un único bus de eventos.

Varios registros de seguimiento por región

Si tiene diferentes grupos de usuarios, pero que están relacionados, como desarrolladores, personal de seguridad y auditores de TI, puede crear varios registros de seguimiento en cada región. De este modo, cada grupo recibe su propia copia de los archivos de registro.

CloudTrail admite cinco rutas por región. Un sendero que se aplica a todas AWS las regiones cuenta como un sendero en cada región.

El siguiente ejemplo es una región con cinco registros de seguimiento:

- Crea dos registros de seguimiento en la región EE. UU. Oeste (Norte de California) que se aplicarán únicamente a esta región.
- Crea dos registros de seguimiento más en la región EE. UU. Oeste (Norte de California) que se aplican a todas las regiones de AWS .
- Crea un registro de seguimiento en la región Asia Pacífico (Sídney) que se aplicará a todas las regiones de AWS . Este registro de seguimiento también existe como un registro de seguimiento en la región EE. UU. Oeste (Norte de California).

Los senderos aparecen en la AWS región en la que se encuentran. Los registros de seguimiento que registran eventos en todas las regiones de AWS aparecen en cada región. Puedes ver una lista de las rutas de una AWS región en la página Rutas de la CloudTrail consola. Para obtener más

información, consulte Actualización de un registro de seguimiento. Para ver CloudTrail los precios, consulta AWS CloudTrail los precios.

AWS Security Token Service y CloudTrail

AWS Security Token Service (AWS STS) es un servicio que tiene un punto final global y también es compatible con puntos finales específicos de la región. Un punto de enlace es una dirección URL que funciona como punto de entrada para solicitudes de servicios web. Por ejemplo, `https://cloudtrail.us-west-2.amazonaws.com` es el punto de entrada regional de EE. UU. Oeste (Oregón) para el servicio. AWS CloudTrail Los puntos de enlace regionales ayudan a reducir la latencia en sus aplicaciones.

Cuando se utiliza un punto final AWS STS específico de una región, el recorrido de esa región muestra solo los AWS STS eventos que se producen en esa región. Por ejemplo, si utilizas el punto final`sts.us-west-2.amazonaws.com`, el sendero de us-west-2 muestra solo los AWS STS eventos que se originan en us-west-2. Para obtener más información sobre los puntos finales AWS STS regionales, consulte Activación y desactivación AWS STS en una AWS región en la Guía del usuario de IAM.

Para obtener una lista completa de los puntos de enlace AWS regionales, consulte AWS Regiones y puntos de enlace en la. Referencia general de AWS Para obtener información detallada sobre los puntos de enlace de AWS STS , consulte Eventos de servicios globales.

Eventos de servicios globales

> **Important**
>
> A partir del 22 de noviembre de 2021, se AWS CloudTrail modificó la forma en que los senderos capturan los eventos de servicio globales. Ahora, los eventos creados por Amazon CloudFront AWS STS se registran en la región en la que se crearon, la región de EE. UU. Este (Virginia del Norte), us-east-1. AWS Identity and Access Management Esto hace que la forma en que se CloudTrail tratan estos servicios sea coherente con la de otros servicios AWS globales. Para continuar recibiendo eventos de servicios globales fuera de Este de EE. UU. (Norte de Virginia), asegúrese de convertir los registros de seguimiento de una sola región con el uso de eventos de servicio globales fuera de Este de EE. UU. (Norte de Virginia) en los registros de seguimiento de varias regiones. Para obtener más información acerca de la captura de eventos de servicios globales, consulte Habilitación y desactivación del registro de eventos de servicios globales más adelante en esta sección.

Por el contrario, el historial de eventos de la CloudTrail consola y el aws cloudtrail lookup-events comando mostrarán estos eventos en el Región de AWS lugar en el que ocurrieron.

En la mayoría de los servicios, los eventos se registran en la región en la que se produjo la acción. En el caso de servicios globales como AWS Identity and Access Management (IAM) y Amazon CloudFront, los eventos se entregan en cualquier ruta que incluya servicios globales. AWS STS

En el caso de la mayoría de los servicios globales, los eventos se registran como si se produjeran en la región Este de EE. UU. (Norte de Virginia), pero algunos eventos de servicio globales se registran como si se produjeran en otras regiones, como las regiones Este de EE. UU. (Ohio) u Oeste de EE. UU. (Oregón).

Para evitar recibir eventos de servicios globales duplicados, recuerde lo siguiente:

- Los eventos de servicio global se envían de forma predeterminada a los senderos que se crean con la CloudTrail consola. Los eventos se envían al bucket del registro de seguimiento.
- Si dispone de varios registros de seguimiento para una única región, considere la posibilidad de configurarlos de forma que los eventos de servicios globales se envíen únicamente a uno de ellos. Para obtener más información, consulte Habilitación y desactivación del registro de eventos de servicios globales.
- Si cambia la configuración de un registro de seguimiento, tras pasar de registrar todas las regiones a registrar una única región, el registro de eventos de servicios globales se desactiva automáticamente para dicho registro de seguimiento. Del mismo modo, si cambia la configuración de un registro de seguimiento al pasar de registrar una única región a registrar todas las regiones, el registro de eventos de servicios globales se activa automáticamente para dicho registro de seguimiento.

  Para obtener más información sobre cómo cambiar el registro de eventos de servicios globales de un registro de seguimiento, consulte Habilitación y desactivación del registro de eventos de servicios globales.

Ejemplo:

1. Los senderos se crean en la CloudTrail consola. De forma predeterminada, este registro de seguimiento registra eventos de servicios globales.
2. Tiene múltiples registros de seguimiento de una sola región.

3. No es necesario que incluya los servicios globales para los registros de seguimiento de una sola región. Los eventos de servicios globales se envían al primer registro de seguimiento. Para obtener más información, consulte Creación, actualización y gestión de senderos con AWS Command Line Interface.

> **Note**
>
> Al crear o actualizar una ruta con los AWS CLI AWS SDK o la CloudTrail API, puede especificar si desea incluir o excluir los eventos de servicio global para las rutas. No puede configurar el registro de eventos de servicio global desde la CloudTrail consola.

¿Cómo CloudTrail se relaciona con otros servicios AWS de supervisión?

CloudTrail añade otra dimensión a las capacidades de monitoreo que ya ofrece AWS. No cambia ni reemplaza las funciones de registro que quizás ya esté utilizando, como las de Amazon S3 o CloudFront las suscripciones de Amazon. Amazon CloudWatch se centra en la supervisión del rendimiento y el estado del sistema. CloudTrail se centra en la actividad de las API. Aunque CloudTrail no informa sobre el rendimiento o el estado del sistema, puede CloudTrail utilizarla con CloudWatch alarmas para notificarle sobre alguna actividad que pueda interesarle.

Soluciones de socios

AWS colabora con especialistas externos en el registro y el análisis para ofrecer soluciones que utilicen los CloudTrail resultados. Para obtener más información, visite la página de CloudTrail detalles en AWS CloudTrail.

CloudTrail regiones compatibles

> **Note**
>
> Para obtener información sobre las regiones compatibles con CloudTrail Lake, consulteRegiones en las que se admite CloudTrail Lake.
> Para obtener información sobre los puntos finales del plano de datos, consulte los puntos finales del plano de datos en el. Referencia general de AWS

Nombre de la región	Región	Punto final del plano de control	Protocolo	Fecha de compatibilidad
Este de EE. UU. (Norte de Virginia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	13/11/2013
Este de EE. UU. (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	17/10/2016
Oeste de EE. UU. (Norte de California)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	13/5/2014
EE. UU. Oeste (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	13/11/2013
Canadá (Central)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	8/12/2016
Oeste de Canadá (Calgary)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	20/12/2023
África (Ciudad del Cabo)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	22/04/2020
Asia Pacífico (Hong Kong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	24/02/2019

Nombre de la región	Región	Punto final del plano de control	Protocolo	Fecha de compatibilidad
Asia Pacífico (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	27/6/2016
Asia-Pacífico (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	22/11/2022
Asia Pacífico (Tokio)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	30/06/2014
Asia-Pacífico (Seúl)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	6/1/2016
Asia Pacífico (Osaka)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	12/02/2018
Asia Pacífico (Singapur)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	30/06/2014
Asia Pacífico (Sídney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	13/5/2014
Asia-Pacífico (Yakarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	13/12/2021
Asia-Pacífico (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	23/01/2023

Nombre de la región	Región	Punto final del plano de control	Protocolo	Fecha de compatibilidad
China (Beijing)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	01/03/2014
China (Ningxia)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	11/12/2017
Europa (Fráncfort)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	23/10/2014
Europa (Zúrich)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
Europa (Estocolmo)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	11/12/2018
Europa (Irlanda)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	13/5/2014
Europa (Londres)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	13/12/2016
Europa (París)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	18/12/2017
Europa (Milán)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	27/04/2020
Europa (España)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	16/11/2022
Israel (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	31/07/2023

Nombre de la región	Región	Punto final del plano de control	Protocolo	Fecha de compatibilidad
Medio Oriente (EAU)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	30/08/2022
Medio Oriente (Baréin)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	29/07/2019
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	12/11/2018
AWS GovCloud (EE. UU.-Oeste)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	16/08/2011
América del Sur (São Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	30/06/2014

Para obtener más información sobre el uso CloudTrail en la región AWS GovCloud (EE. UU. Este), consulte los puntos finales AWS GovCloud (EE. UU. Este) en la Guía del AWS GovCloud (US) usuario.

Para obtener más información sobre el uso CloudTrail en la región AWS GovCloud (EE. UU. Oeste), consulte los puntos finales AWS GovCloud (EE. UU.) en la Guía del usuario. AWS GovCloud (US)

Para obtener más información sobre el uso CloudTrail en la región de China (Pekín), consulte los puntos finales de la región de China (Pekín) en el. Referencia general de Amazon Web Services

Ejemplos de archivos de registros de CloudTrail

CloudTrail monitorea eventos para su cuenta. Si crea un registro de seguimiento, envía estos eventos como archivos de registros a su bucket de Amazon S3. Cuando crea un almacén de datos de eventos en CloudTrail Lake, los eventos se registran en su almacén de datos de eventos. Los almacenes de datos de eventos no utilizan buckets de S3.

Temas

- Formato de nombre de archivo de registros de CloudTrail
- Ejemplos de archivos de registros

Formato de nombre de archivo de registros de CloudTrail

CloudTrail utiliza el siguiente formato de nombre de archivo para los objetos de archivo de registros que envía a su bucket de Amazon S3:

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- `YYYY`, `MM`, `DD`, `HH` y `mm` son los dígitos del año, mes, día, hora y minuto cuando se envió el archivo de registro. Las horas están en formato de 24 horas. La `Z` indica que la hora se muestra en UTC.

  > **Note**
  >
  > Un archivo de registro enviado en un momento específico puede contener registros escritos en cualquier momento antes de ese momento.

- El componente `UniqueString` de 16 caracteres del nombre del archivo de registro sirve para impedir que se sobrescriban los archivos. No tiene ningún significado y el software de procesamiento de archivos de registro debería omitirlo.
- `FileNameFormat` es la codificación del archivo. Actualmente, es `json.gz`, que es un archivo de texto JSON en formato gzip comprimido.

Ejemplo de nombre de archivo de registros de CloudTrail

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

Ejemplos de archivos de registros

Un archivo de registro contiene uno o más registros. Los siguientes ejemplos son fragmentos de archivos de registro que muestran los registros de una acción que inició la creación de un archivo de registro.

Para más información acerca de los campos de los registros de eventos de CloudTrail, consulte CloudTrail contenido del registro.

Contenido

- Ejemplos de registros de Amazon EC2
- Ejemplos de registro de IAM
- Ejemplo de código de error y registro de mensajes
- Ejemplo de registro de eventos de CloudTrail Insights

Ejemplos de registros de Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación de tamaño variable en la Nube de AWS. Puede lanzar servidores virtuales, configurar la seguridad y las redes, y administrar el almacenamiento. Amazon EC2 puede reducir o escalar verticalmente con rapidez para adaptarlo a cambios en los requisitos o picos de popularidad, con lo que se reduce la necesidad de pronosticar el tráfico de los servidores. A fin de obtener más información, consulte la Guía del usuario de Amazon EC2 para instancias de Linux.

En el siguiente ejemplo, se muestra que un usuario de IAM llamado `Mateo` utilizó el comando aws ec2 start-instances para llamar a la acción `StartInstances` de Amazon EC2 para las instancias `i-EXAMPLE56126103cb` y `i-EXAMPLEaff4840c22`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
```

```
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

En el siguiente ejemplo, se muestra que un usuario de IAM llamado `Nikki` utilizó el comando aws ec2 stop-instances para llamar a la acción `StopInstances` de Amazon EC2 para detener dos instancias.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
```

```
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

En el siguiente ejemplo, se muestra que un usuario de IAM llamado `Arnav` utilizó el comando aws ec2 create-key-pair para llamar a la acción `CreateKeyPair`. Tenga en cuenta que los `responseElements` contienen un hash del par de claves y que AWS eliminó el material de las claves.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Ejemplos de registro de IAM

AWS Identity and Access Management (IAM) es un servicio web que lo ayuda a controlar de forma segura el acceso a los recursos de AWS. Con IAM, puede administrar de forma centralizada los permisos que controlan a qué recursos de AWS pueden acceder los usuarios. Utilice IAM; para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos. Para obtener más información, consulte la Guía del usuario de IAM.

En el siguiente ejemplo, se muestra que la usuaria de IAM `Mary` utilizó el comando aws iam create-user para llamar a la acción `CreateUser` para crear un usuario nuevo llamado `Richard`.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
```

```
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

En el siguiente ejemplo, se muestra que el usuario de IAM `Paulo` utilizó el comando aws iam add-user-to-group para llamar a la acción `AddUserToGroup` para agregar una usuaria nueva llamada `Jane` al grupo `Admin`.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
```

```
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


En el siguiente ejemplo, se muestra que la usuaria de IAM `Saanvi` utilizó el comando aws iam create-role para llamar a la acción `CreateRole` para crear un rol.


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
```

```
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
```

```
}]}
```

Ejemplo de código de error y registro de mensajes

En el siguiente ejemplo, se muestra que el usuario de IAM `Terry` utilizó el comando aws cloudtrail update-trail para llamar a la acción `UpdateTrail` para actualizar un registro de seguimiento llamado `myTrail2`, pero no se encontró el nombre del registro de seguimiento. El archivo de registro muestra este error en los elementos `errorCode` y `errorMessage`.

```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Ejemplo de registro de eventos de CloudTrail Insights

En el siguiente ejemplo se muestra un registro de eventos de CloudTrail Insights. Un evento de Insights es en realidad un par de eventos que marcan el inicio y el final de un periodo de actividad inusual de escritura de la API de administración o de actividad de respuesta a error . El campo `state` muestra si el evento se registró al principio o al final del periodo de actividad inusual. El nombre del evento, `UpdateInstanceInformation`, es el mismo nombre de la API de AWS Systems Manager para la que CloudTrail analizó eventos de administración con el fin de determinar si se produjo una actividad inusual. Aunque los eventos de inicio y fin tienen valores `eventID` únicos, también tienen un valor `sharedEventID` utilizado en el par. El evento de Insights muestra el `baseline`, o el patrón normal de actividad, `insight`, o la actividad inusual promedio que desencadenó el evento de Insights inicial y, en el evento final, el valor `insight` de la actividad inusual promedio durante el evento de Insights. Para obtener más información sobre CloudTrail Insights, consulte Registro de eventos de Insights.

```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
```

```
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

CloudTrail servicios e integraciones compatibles

CloudTrail admite el registro de eventos para muchos AWS servicios. Encontrará información sobre los aspectos específicos de cada servicio compatible en la guía de dicho servicio. A continuación, se incluyen enlaces a estos temas específicos de los servicios. Además, algunos AWS servicios se pueden utilizar para analizar los datos recopilados en los CloudTrail registros y actuar en función de ellos. Puede acceder a una descripción general de estas integraciones de servicios aquí.

> **Note**
>
> Para ver la lista de regiones compatibles con cada servicio, consulte Puntos de conexión y cuotas del servicio en la Referencia general de Amazon Web Services.

Temas

- AWS integraciones de servicios con registros CloudTrail
- CloudTrail integración con Amazon EventBridge
- CloudTrail integración con AWS Organizations
- AWS temas de servicio para CloudTrail
- Servicios CloudTrail no compatibles

AWS integraciones de servicios con registros CloudTrail

> **Note**
>
> También puede usar CloudTrail Lake para consultar y analizar sus eventos. CloudTrail Las consultas de Lake ofrecen una visión más profunda y personalizable de los eventos que las simples búsquedas de claves y valores en el historial de eventos o en curso. `LookupEvents` CloudTrail Los usuarios de Lake pueden ejecutar consultas complejas en lenguaje de consulta estándar (SQL) en varios campos en un CloudTrail evento. Para más información, consulte Trabajando con AWS CloudTrail Lake y Copiar los eventos del sendero al CloudTrail lago.
>
> CloudTrail Los almacenes de datos y las consultas de eventos de Lake conllevan CloudTrail cargos. Para obtener más información sobre los precios de CloudTrail Lake, consulta AWS CloudTrail los precios.

Puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas.

AWS Servicio	Tema	Descripción
Amazon Athena	Consultando registros AWS CloudTrail	El uso de Athena con CloudTrail registros es una forma eficaz de mejorar el análisis de la actividad del AWS servicio. Por ejemplo, puede utilizar consultas para identificar tendencias y aislar la actividad por atributo, como el usuario o la dirección IP de fuente. Puede crear automátic amente tablas para consultar registros directamente desde la CloudTrail consola y utilizar esas tablas para ejecutar consultas en Athena. Para obtener más información, consulte Creación de una tabla de CloudTrail registros en la CloudTrail consola en la Guía del usuario de Amazon Athena. **Note** La ejecución de consultas en Amazon Athena genera costos adicionales. Para obtener más informaci

AWS Servicio	Tema	Descripción
		ón, consulte Precios de Amazon Athena.
Amazon CloudWatch Logs	Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs	Puede configurarlo CloudTrail con CloudWatch Logs para monitorear sus registros de rastreo y recibir notificaciones cuando se produzca una actividad específica. Por ejemplo, puedes definir filtros métricos de CloudWatch Logs que activen CloudWatch las alarmas y te envíen notificaciones cuando se activen esas alarmas. **Note** Se aplica el precio estándar para Amazon CloudWatch y Amazon CloudWatch Logs. Para obtener más información, consulte Precios de Amazon CloudWatch .

CloudTrail integración con Amazon EventBridge

Amazon EventBridge es un AWS servicio que ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. En EventBridge, puede crear reglas que respondan a los eventos registrados por CloudTrail. Para obtener más información, consulta Crear una regla en Amazon EventBridge.

Puedes ofrecer eventos a los que estés suscrito EventBridge durante tu recorrido. Cuando cree una regla con la EventBridge consola, elija el tipo de `AWS API Call via CloudTrail` detalle para entregar los CloudTrail datos y los eventos de gestión, o el tipo de `AWS Insight via CloudTrail` detalle para entregar los eventos de Insights.

Para registrar eventos con un valor de tipo detalle de`AWS API Call via CloudTrail`, debe tener un registro que registre actualmente los eventos de administración o de datos. Para obtener más información sobre cómo crear y administrar un registro de seguimiento, consulte Creación de un registro de seguimiento.

Para registrar eventos con un valor de tipo detalle de`AWS Insight via CloudTrail`, debe tener un registro que registre actualmente los eventos de Insights. Para obtener información sobre cómo registrar eventos de Insights, consulte Registro de eventos de Insights.

CloudTrail integración con AWS Organizations

La cuenta de administración de una AWS Organizations organización puede añadir un administrador delegado para gestionar los CloudTrail recursos de la organización. Puede crear un registro de seguimiento de la organización o un almacén de datos de eventos de la organización en la cuenta de administración o la cuenta del administrador delegado de una organización que recopile todos los datos de eventos de cada una de las cuentas de AWS en una organización en AWS Organizations. La creación de un registro de seguimiento de organización lo ayuda a definir una estrategia uniforme de registro de eventos para su organización.

Se aplica automáticamente un registro de la organización a cada AWS cuenta de la organización. Los usuarios de las cuentas miembro pueden ver estos registros de seguimiento, pero no pueden modificarlos y, de forma predeterminada, no pueden ver los archivos de registros creados para el registro de seguimiento de organización. Para obtener más información, consulte Creación de un registro de seguimiento para una organización.

AWS temas de servicio para CloudTrail

Puede obtener más información sobre cómo se registran los eventos de AWS los servicios individuales en CloudTrail los registros, incluidos ejemplos de eventos de ese servicio en los archivos de registro. Para obtener más información sobre cómo se integran AWS los servicios específicos CloudTrail, consulte el tema sobre la integración en la guía individual de ese servicio.

Los servicios que aún se encuentran en versión preliminar, que aún no se han lanzado para su disponibilidad general (GA) o que no tienen API públicas, no se consideran compatibles. CloudTrail actualmente no registra los eventos específicos de la política de puntos finales de Amazon VPC.

> **Note**
>
> Para ver la lista de regiones compatibles con cada servicio, consulte Puntos de conexión y cuotas del servicio en la Referencia general de Amazon Web Services.
> Para obtener información sobre qué servicios registran eventos de datos, consulte Eventos de datos.

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon API Gateway	Registre las llamadas de administración de API en Amazon API Gateway mediante AWS CloudTrail	09/07/2015
Amazon AppFlow	Registrar llamadas a AppFlow la API de Amazon con AWS CloudTrail	22/04/2020
Amazon AppStream 2.0	Registrar llamadas a la API de Amazon AppStream 2.0 con AWS CloudTrail	25/04/2019
Amazon Athena	Registro de llamadas a la API de Amazon Athena con AWS CloudTrail	19/05/2017
Amazon Aurora	Supervisión de las llamadas a la API de Amazon Aurora AWS CloudTrail	31/08/2018
Amazon Bedrock	Registre las llamadas a la API de Amazon Bedrock mediante AWS CloudTrail	23 de octubre de 2023

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Braket	Registro de la API Amazon Braket con CloudTrail	08/12/2020
Amazon Chime	Registre las llamadas de administración de Amazon Chime mediante AWS CloudTrail	27/09/2017
Amazon Cloud Directory	Registro de llamadas a la API de Amazon Cloud Directory mediante AWS CloudTrail	26/01/2017
Amazon CloudFront	Se utiliza AWS CloudTrail para capturar las solicitudes enviadas a la CloudFront API	28/05/2014
Amazon CloudSearch	Registro de llamadas a Amazon CloudSearch Configuration Service mediante AWS CloudTrail	16/10/2014
Amazon CloudWatch	Registro de llamadas a CloudWatch la API de Amazon AWS CloudTrail	30/04/2014
CloudWatch Eventos de Amazon	Registro de llamadas a la API de Amazon CloudWatch Events AWS CloudTrail	16/01/2016
Amazon CloudWatch Logs	Registro de llamadas a la API de Amazon CloudWatch Logs AWS CloudTrail	10/03/2016
Amazon CodeCatalyst	Registrar las llamadas a la CodeCatalyst API conectada s Cuentas de AWS mediante AWS CloudTrail	12/01/2022

AWS Servicio	CloudTrail Temas	Solución compatible desde
CodeGuru Revisor de Amazon	Registrar llamadas a la API de Amazon CodeGuru Reviewer con AWS CloudTrail	02/12/2019
Amazon CodeWhisperer	AWS CloudTrail y CodeWhisperer API	13/04/2023
Amazon Cognito	Registro de llamadas a la API de Amazon Cognito con AWS CloudTrail	18/02/2016
Amazon Comprehend	Registro de llamadas a la API Amazon Comprehend con AWS CloudTrail	17/01/2018
Amazon Comprehend Medical	Registro de llamadas a la API de Amazon Comprehend Medical mediante AWS CloudTrail	27/11/2018
Amazon Connect	Registro de llamadas a la API de Amazon Connect con AWS CloudTrail	11/12/2019
Amazon Data Lifecycle Manager	Registro de llamadas a la API de Amazon Data Lifecycle Manager mediante AWS CloudTrail	24/07/2018
Amazon Detective	Registro de llamadas a la API de Amazon Detective con AWS CloudTrail	31/03/2020
El DevOps gurú de Amazon	Registrar llamadas a la API de Amazon DevOps Guru con AWS CloudTrail	05/04/2021

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon DocumentDB (con compatibilidad con MongoDB)	Registro de llamadas a la API de Amazon DocumentDB con AWS CloudTrail	01/09/2019
Amazon DynamoDB	Registro de operaciones de DynamoDB mediante AWS CloudTrail	28/05/2015
Amazon EC2	Registro de llamadas a la API mediante AWS CloudTrail	13/11/2013
Amazon EC2 Auto Scaling	Registro de llamadas a la API de Auto Scaling mediante CloudTrail	16/07/2014
Bloques de capacidad de Amazon EC2	La capacidad de registro bloquea las llamadas a la API con AWS CloudTrail	31/10/2023
Amazon EC2 Image Builder	Registro de llamadas a la API Image Builder de EC2 mediante CloudTrail	02/12/2019
Amazon Elastic Block Store (Amazon EBS) API directas de EBS	Registro de llamadas a la API mediante AWS CloudTrail Registro de llamadas a la API de las API directas de EBS con AWS CloudTrail	Amazon EBS: 13/11/2013 API directas de EBS: 30/06/2020
Amazon Elastic Container Registry (Amazon ECR)	Registro de llamadas a la API Amazon ECR mediante AWS CloudTrail	21/12/2015
Amazon Elastic Container Service (Amazon ECS)	Registro de llamadas a la API de Amazon ECS mediante AWS CloudTrail	09/04/2015

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Elastic File System (Amazon EFS)	Registro de llamadas a la API de Amazon EFS con AWS CloudTrail	28/06/2016
Amazon Elastic Kubernetes Service (Amazon EKS)	Registro de llamadas a la API de Amazon EKS con AWS CloudTrail	05/06/2018
Amazon Elastic Transcoder	Registro de llamadas a la API de Amazon Elastic Transcoder con AWS CloudTrail	27/10/2014
Amazon ElastiCache	Registro de llamadas a ElastiCache la API de Amazon mediante AWS CloudTrail	15/09/2014
Amazon EMR	Registro de llamadas a la API de Amazon EMR AWS CloudTrail	04/04/2014
Amazon EMR en EKS	Registro de llamadas a la API de Amazon EMR en EKS mediante AWS CloudTrail	12/09/2020
Amazon EventBridge	EventBridge información en AWS CloudTrail	07/11/2019
Amazon FinSpace	Consultando registros AWS CloudTrail	18/10/2022
Amazon Forecast	Registrar llamadas a la API Amazon Forecast con AWS CloudTrail	28/11/2018
Amazon Fraud Detector	Registro de llamadas a la API de Amazon Fraud Detector con AWS CloudTrail	01/09/2020

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon FSx para Lustre	Registro de llamadas a la API Amazon FSx for Lustre con AWS CloudTrail	11/01/2019
Amazon FSx para Windows File Server	Supervisión con AWS CloudTrail	28/11/2018
Amazon GameLift	Registrar llamadas a GameLift la API de Amazon con AWS CloudTrail	27/01/2016
Amazon GuardDuty	Registrar llamadas a GuardDuty la API de Amazon con AWS CloudTrail	12/02/2018
Amazon Honeycode	Registro de llamadas a la API de Amazon Honeycode con AWS CloudTrail	24/06/2020
Amazon Inspector	Registrar llamadas a la API de Amazon Inspector con AWS CloudTrail	20/04/2016
Escaneo de Amazon Inspector	Amazon Inspector Escanea la información en CloudTrail	27/11/2023
Amazon Interactive Video Service	Registro de llamadas a la API de Amazon IVS con AWS CloudTrail	15/07/2020
Amazon Kendra	Registrar las llamadas a la API de Amazon Kendra AWS CloudTrail y registrar las llamadas a la API Amazon Kendra Intelligent Ranking con registros AWS CloudTrail	11/05/2020

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Keyspaces (para Apache Cassandra)	Registro de llamadas a la API de Amazon Keyspaces con AWS CloudTrail	13/01/2020
Amazon Managed Service para Apache Flink	Supervisión de Amazon Managed Service para Apache Flink con AWS CloudTrail (aplicaciones SQL) y supervisión de Amazon Managed Service para Apache Flink con AWS CloudTrail (aplicaciones Apache Flink)	22/03/2019
Amazon Data Firehose	Supervisión de las llamadas a la API Amazon Data Firehose con AWS CloudTrail	17/03/2016
Amazon Kinesis Data Streams	Registro de llamadas a la API de Amazon Kinesis Data Streams mediante AWS CloudTrail	25/04/2014
Amazon Kinesis Video Streams	Registro de llamadas a la API de Kinesis Video Streams con AWS CloudTrail	24/05/2018
Amazon Lex	Registro de llamadas a la API de Amazon Lex con CloudTrail	15/08/2017
Amazon Lightsail	Registro de llamadas a la API de Lightsail con AWS CloudTrail	23/12/2016
Amazon Location Service	Registro y monitoreo con AWS CloudTrail	15 de diciembre de 2020

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Lookout for Equipment	Monitorización de las llamadas de Amazon Lookout for Equipment con AWS CloudTrail	01/12/2020
Amazon Lookout for Metrics	Visualización de la actividad de la API de Amazon Lookout for Metrics en AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	Registro de llamadas de Amazon Lookout for Vision con AWS CloudTrail	12/01/2020
Amazon Machine Learning	Registro de llamadas a la API de Amazon ML mediante AWS CloudTrail	10/12/2015
Amazon Macie	Registro de llamadas a la API de Amazon Macie mediante AWS CloudTrail	13/05/2020
Amazon Managed Blockchain	Registro de llamadas a la API de Amazon Managed Blockchain mediante AWS CloudTrail Registro de Ethereum para las llamadas a la API de Managed Blockchain mediante AWS CloudTrail (vista previa)	04/01/2019
Amazon Managed Grafana	Registro de llamadas a la API de Amazon Managed Grafana mediante AWS CloudTrail	15/12/2020

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Managed Service para Prometheus	Registro de llamadas a la API de Amazon Managed Service for Prometheus mediante AWS CloudTrail	15/12/2020
Amazon Managed Streaming for Apache Kafka	Registrar llamadas a la API de Amazon MSK con AWS CloudTrail	11/12/2018
Amazon Managed Workflows para Apache Airflow	Monitoreo de la actividad de la API de Amazon MWAA con AWS CloudTrail	24 de noviembre de 2020
Amazon MemoryDB para Redis	Registro de llamadas a la API de Amazon MemoryDB para Redis con AWS CloudTrail	19/08/2021
Amazon MQ	Registro de llamadas a la API de Amazon MQ mediante AWS CloudTrail	19/07/2018
Amazon Neptune	Registro de llamadas a la API de Amazon Neptune mediante AWS CloudTrail	30/05/2018
Amazon Nimble Studio	Registro de llamadas de Nimble Studio mediante AWS CloudTrail	19/06/2023
Amazon One Enterprise	Registro de llamadas a la API de Amazon One Enterprise mediante AWS CloudTrail	27/11/2023
OpenSearch Servicio Amazon	Auditoría de dominios OpenSearch de Amazon Service con AWS CloudTrail	01/10/2015

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Personalize	Registro de llamadas a la API de Amazon Personalize con AWS CloudTrail	28/11/2018
Amazon Pinpoint	Registro de llamadas a la API Amazon Pinpoint con AWS CloudTrail	06/02/2018
API de SMS y voz de Amazon Pinpoint	Registro de llamadas a la API Amazon Pinpoint con AWS CloudTrail	16/11/2018
Amazon Polly	Registro de llamadas a la API de Amazon Polly con AWS CloudTrail	30/11/2016
Amazon Q (para uso corporativo)	Registro de llamadas a la API de Amazon Q mediante AWS CloudTrail	28/11/2023
Amazon Q (para uso de AWS constructores)	Registro de llamadas a la API de Amazon Q mediante AWS CloudTrail	28/11/2023
Amazon Quantum Ledger Database (Amazon QLDB)	Registro de llamadas a la API de Amazon QLDB con AWS CloudTrail	10/09/2019
Amazon QuickSight	Operaciones de registro con CloudTrail	28/04/2017
Amazon Relational Database Service (Amazon RDS)	Registro de llamadas a la API de Amazon RDS mediante AWS CloudTrail	13/11/2013

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon RDS Performance Insights	Registro de llamadas a la API de Amazon RDS mediante AWS CloudTrail La API de Amazon RDS Performance Insights es un subconjunto de la API de Amazon RDS.	21/06/2018
Amazon Redshift	Registro de llamadas a la API de Amazon Redshift con AWS CloudTrail	10/06/2014
Amazon Rekognition	Registro de llamadas a la API Amazon Rekognition mediante AWS CloudTrail	06/04/2018
Amazon Route 53	Uso de AWS CloudTrail para capturar las solicitudes enviadas a la API de Route 53	11/02/2015
Controlador de recuperación de aplicaciones de Amazon Route 53	Registro de llamadas a la API de Amazon Route 53 Application Recovery Controller mediante AWS CloudTrail	27/07/2021
Amazon S3	Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail	Eventos de administración: 01/09/2015 Eventos de datos: 21/11/2016
Amazon S3 Glacier	Registrar las llamadas a la API de S3 Glacier mediante AWS CloudTrail	11/12/2014

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon SageMaker	Registrar llamadas a SageMaker la API de Amazon con AWS CloudTrail	11/01/2018
Amazon Security Lake	Registro de llamadas a la API de Amazon Security Lake mediante CloudTrail	30/05/2023
Amazon Simple Email Service (Amazon SES)	Registro de llamadas a la API de Amazon SES mediante AWS CloudTrail	07/05/2015
Amazon Simple Notification Service (Amazon SNS)	Registro de llamadas a la API de Amazon Simple Notification Service mediante AWS CloudTrail	09/10/2014
Amazon Simple Queue Service (Amazon SQS)	Registro de acciones de la API de Amazon SQS mediante AWS CloudTrail	16/07/2014
Amazon Simple Workflow Service (Amazon SWF)	Grabar llamadas a la API con AWS CloudTrail	Eventos de gestión: 13/05/2014 Eventos de datos: 14/02/2024
Amazon Textract	Registro de llamadas a la API Amazon Textract con AWS CloudTrail	29/05/2019
Amazon Timestream	Registrar las llamadas a la API de Timestream con AWS CloudTrail	30/09/2020
Amazon Transcribe	Registro de llamadas a la API Amazon Transcribe con AWS CloudTrail	28/06/2018

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon Translate	Registro de llamadas a la API de Amazon Translate con AWS CloudTrail	04/04/2018
Amazon Verified Permissions	Registro de llamadas a la API de permisos verificados de Amazon mediante AWS CloudTrail	13/06/2023
Amazon Virtual Private Cloud (Amazon VPC)	Registro de llamadas a la API mediante AWS CloudTrail La API de Amazon VPC es un subconjunto de la API de Amazon EC2.	13/11/2013
Amazon VPC Lattice	CloudTrail registros	31/03/2023
Analizador de accesibilidad de Amazon VPC	Registro de llamadas a la API de Reachability Analyzer mediante AWS CloudTrail	27/11/2023
Amazon WorkDocs	Registro de llamadas a WorkDocs la API de Amazon mediante AWS CloudTrail	27/08/2014
Amazon WorkMail	Registro de llamadas a WorkMail la API de Amazon mediante AWS CloudTrail	12/12/2017
Amazon WorkSpaces	Registro de llamadas a WorkSpaces la API de Amazon mediante CloudTrail	09/04/2015

AWS Servicio	CloudTrail Temas	Solución compatible desde
Amazon WorkSpaces Thin Client	Registro de llamadas a la API de Amazon WorkSpaces Thin Client mediante AWS CloudTrail	26/11/2023
Amazon WorkSpaces Web	Registro de llamadas a WorkSpaces la API de Amazon Web mediante AWS CloudTrail	30/11/2021
Aplicación de escalado automático	Registro de llamadas a la API Application Auto Scaling con AWS CloudTrail	31/10/2016
AWS Amplify	Registro de llamadas a la API de Amplify mediante AWS CloudTrail	30 de noviembre de 2020
AWS App Mesh	Registro de llamadas a la API App Mesh con AWS CloudTrail	AWS App Mesh 30 de octubre de 2019 Servicio de administración de enviados de App Mesh 18/03/2022
AWS App Runner	Registrar las llamadas a la API de App Runner con AWS CloudTrail	18/05/2021
AWS AppConfig	Registro de llamadas a la AWS AppConfig API mediante AWS CloudTrail	Eventos de gestión: 31/07/2020 Eventos de datos: 04/01/2024
AWS AppFabric	Registro de llamadas a la AWS AppFabric API mediante AWS CloudTrail	27/06/2023

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Elaborador de perfiles de costes de aplicaciones	AWS Referencia de la API de Application Cost Profiler	13/05/2021
AWS Application Discovery Service	Registro de llamadas a la API de Application Discovery Service con AWS CloudTrail	12/05/2016
AWS Servicio de transform ación de aplicaciones	(Servicio de backend utilizado por AWS herramientas, como AWS Microservice Extractor para .NET)	26/08/2023
AWS AppSync	Registrar llamadas a la AWS AppSync API con AWS CloudTrail	13/02/2018
AWS Artifact	Registrar llamadas a la AWS Artifact API con AWS CloudTrail	27/01/2023
AWS Audit Manager	Registrar llamadas a la AWS Audit Manager API con AWS CloudTrail	12/07/2020
AWS Auto Scaling	Registro de llamadas a AWS Auto Scaling la API mediante CloudTrail	15/08/2018
AWS Intercambio de datos B2B	Registro de llamadas a la API de intercambio de datos AWS B2B mediante AWS CloudTrail	01/12/2023
AWS Backup	Registrar llamadas a la AWS Backup API con AWS CloudTrail	04/02/2019

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Batch	Registrar llamadas a la AWS Batch API con AWS CloudTrail	10/01/2018
AWS Billing and Cost Management	Registrar llamadas a la AWS Billing and Cost Management API con AWS CloudTrail	07/06/2018
AWS Billing Conductor	Registrar llamadas a la AWS Billing Conductor API mediante AWS CloudTrail	12/03/2024
AWS BugBust	Registrar llamadas a la BugBust API mediante CloudTrail	24/06/2021
AWS Certificate Manager	Uso de AWS CloudTrail	25/03/2016
AWS Clean Rooms	Registro de llamadas a la AWS Clean Rooms API mediante AWS CloudTrail	21/03/2023
AWS Cloud Map	Registrar llamadas a la API de AWS Cloud Map con AWS CloudTrail	28/11/2018
AWS Cloud9	Registrar llamadas a la AWS Cloud9 API con AWS CloudTrail	21/01/2019
AWS CloudFormation	Registrar las llamadas a la AWS CloudFormation API AWS CloudTrail	02/04/2014
AWS CloudHSM	Registro AWS CloudHSM de llamadas a la API mediante AWS CloudTrail	08/01/2015

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS CloudShell	Inicio de sesión y supervisión AWS CloudShell	15 de diciembre de 2020
AWS CloudTrail	AWS CloudTrail Referencia de la API (todas las llamadas a la CloudTrail API se registran en.) CloudTrail	13/11/2013
AWS CodeArtifact	Registrar las llamadas a la CodeArtifact API con AWS CloudTrail	06/10/2020
AWS CodeBuild	Registrar llamadas a la AWS CodeBuild API con AWS CloudTrail	01/12/2016
AWS CodeCommit	Registrar llamadas a la AWS CodeCommit API con AWS CloudTrail	11/01/2017
AWS CodeDeploy	Supervisar las implement aciones con AWS CloudTrail	16/12/2014
AWS CodePipeline	Registro de llamadas a la CodePipeline API mediante AWS CloudTrail	09/07/2015
AWS CodeStar	Registrar llamadas a la AWS CodeStar API con AWS CloudTrail	14/06/2017
AWS CodeStar Notificaciones	Registrar AWS CodeStar las llamadas a la API de notificac iones con AWS CloudTrail	05/11/2019

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Config	Registrar las llamadas a la AWS Config API mediante AWS CloudTrail	10/02/2015
AWS Control Tower	Registrar AWS Control Tower acciones con AWS CloudTrail	12/08/2019
AWS Data Pipeline	Registrar llamadas a la AWS Data Pipeline API mediante AWS CloudTrail	02/12/2014
AWS Database Migration Service (AWS DMS)	Registro de llamadas a la AWS Database Migration Service API mediante AWS CloudTrail	04/02/2016
AWS DataSync	Registrar llamadas a la AWS DataSync API con AWS CloudTrail	26/11/2018
AWS Deadline Cloud	Registrar llamadas con CloudTrail	04/02/2024
AWS Device Farm	Registro de llamadas a la AWS Device Farm API mediante AWS CloudTrail	13/07/2015
AWS Direct Connect	Registrar las llamadas a la AWS Direct Connect API AWS CloudTrail	08/03/2014
AWS Directory Service	Registro AWS Directory Service de llamadas a la API mediante CloudTrail	14/05/2015

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Elastic Beanstalk (Elastic Beanstalk)	Uso de llamadas a la API de Elastic Beanstalk con AWS CloudTrail	31/03/2014
AWS Elastic Disaster Recovery	Registrar llamadas AWS Elastic Disaster Recovery a la API mediante AWS CloudTrail	17/11/2021
AWS Elemental MediaConnect	Registrar llamadas a la AWS Elemental MediaConnect API con AWS CloudTrail	27/11/2018
AWS Elemental MediaConvert	Registrar llamadas a la AWS Elemental MediaConvert API con CloudTrail	27/11/2017
AWS Elemental MediaLive	Registrar llamadas a la MediaLive API con AWS CloudTrail	19/01/2019
AWS Elemental MediaPackage	Registrar llamadas a la AWS Elemental MediaPackage API con AWS CloudTrail	21/12/2018
AWS Elemental MediaStore	Registrar llamadas a la AWS Elemental MediaStore API con CloudTrail	27/11/2017
AWS Elemental MediaTailor	Registrar llamadas a la AWS Elemental MediaTailor API con AWS CloudTrail	02/11/2019
AWS Resolución de entidades	Registro de llamadas a la API de resolución de AWS entidades mediante A AWS CloudTrail	26/07/2023

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Fault Injection Service	Registra las llamadas a la API con AWS CloudTrail	15/03/2021
AWS Firewall Manager	Registrar llamadas a la AWS Firewall Manager API con AWS CloudTrail	05/04/2018
AWS Global Accelerator	Registrar llamadas a la API de AWS Global Accelerator con AWS CloudTrail	26/11/2018
AWS Glue	Registrar AWS Glue oper aciones mediante AWS CloudTrail	07/11/2017
AWS Ground Station	Registrar llamadas a la AWS Ground Station API con AWS CloudTrail	31/05/2019
AWS Health	Registrar llamadas a la AWS Health API con AWS CloudTrail	21/11/2016
AWS Health Dashboard	Registrar llamadas a la AWS Health API con AWS CloudTrail	01/12/2016
AWS HealthImaging	Registrar llamadas a la AWS HealthImaging API mediante AWS CloudTrail	26/07/2023
AWS HealthLake	Registrar llamadas a la AWS HealthLake API con AWS CloudTrail	12/07/2020

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS HealthOmics	Registro de llamadas a la AWS HealthOmics API mediante AWS CloudTrail	29/11/2022
AWS IAM Identity Center	Registro de llamadas a la API de IAM Identity Center con AWS CloudTrail	07/12/2017
AWS Identity and Access Management (IAM)	Registro de eventos de IAM con AWS CloudTrail	13/11/2013
AWS IoT	Registrar llamadas a AWS IoT la API con AWS CloudTrail	11/04/2016
AWS IoT 1-Click	Registrar llamadas a la AWS IoT 1-Click API con AWS CloudTrail	14/05/2018
AWS IoT Análisis	Registrar las llamadas a la API de AWS IoT Analytics con AWS CloudTrail	23/04/2018
AWS IoT Eventos	Registrar llamadas a la API de AWS IoT eventos con AWS CloudTrail	11/06/2019
AWS IoT Greengrass	Registrar llamadas a la AWS IoT Greengrass API con AWS CloudTrail	29/10/2018
AWS IoT Greengrass V2	Registra las llamadas a la API AWS IoT Greengrass V2 con AWS CloudTrail	14/12/2020
AWS IoT SiteWise	Registrar llamadas a la AWS IoT SiteWise API con AWS CloudTrail	29/04/2020

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Key Management Service (AWS KMS)	Registrar llamadas a la AWS KMS API mediante AWS CloudTrail	12/11/2014
AWS Lake Formation	Registro de llamadas a la AWS Lake Formation API mediante AWS CloudTrail	08/09/2019
AWS Lambda	Registro de llamadas a AWS Lambda la API mediante AWS CloudTrail Uso de Lambda con AWS CloudTrail	Eventos de administración: 09/04/2015 Eventos de datos: 30/11/2017
AWS Launch Wizard	Registrar llamadas a AWS Launch Wizard la API mediante AWS CloudTrail	11/08/2023
AWS License Manager	Registro de llamadas a la API de AWS License Manager con AWS CloudTrail	01/03/2019
AWS Mainframe Modernization	Registrar llamadas a la AWS Mainframe Modernization API mediante AWS CloudTrail	06/08/2022
AWS Managed Services	Administración de registros en AMS Accelerate	21/12/2016
AWS Marketplace	Registrar llamadas a la AWS Marketplace API con AWS CloudTrail	02/05/2017
AWS Marketplace Acuerdos	Registro de llamadas a la API de acuerdos mediante AWS CloudTrail	09/01/2023

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Marketplace Servicio de despliegue	Registrar las llamadas del Servicio de AWS Marketplace Despliegue con CloudTrail	29/11/2023
AWS Marketplace Descubrimiento	Registrar las llamadas a la API AWS Marketplace Discovery mediante AWS CloudTrail	15 de diciembre de 2022
AWS Marketplace Servicio de medición	Registrar llamadas a AWS Marketplace la API con AWS CloudTrail	22/08/2018
AWS Migration Hub	Registrar llamadas a la API de AWS Migration Hub con AWS CloudTrail	14/08/2017
AWS Mobile Hub	Registro de llamadas a la API CLI AWS móvil con AWS CloudTrail	29/06/2018
AWS Network Firewall	Registrar llamadas a la AWS Network Firewall API con AWS CloudTrail	17/11/2020
AWS OpsWorks for Chef Automate	Registrar llamadas a la AWS OpsWorks for Chef Automate API con AWS CloudTrail	16/07/2018
AWS OpsWorks for Puppet Enterprise	Registrar OpsWorks las llamadas a la API de Puppet Enterprise con AWS CloudTrail	16/07/2018
AWS OpsWorks Stacks	Registrar llamadas a AWS OpsWorks Stacks la API con AWS CloudTrail	04/06/2014

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Organizations	Registrar llamadas a la AWS Organizations API con AWS CloudTrail	27/02/2017
AWS Outposts	Registrar llamadas a la AWS Outposts API con AWS CloudTrail	04/02/2020
AWS Panorama	Referencia de la API de AWS Panorama	20/10/2021
AWS Payment Cryptography	Registrar llamadas a la AWS Payment Cryptography API mediante AWS CloudTrail	06/08/2023
AWS 5G privado	Registro de llamadas AWS privadas a la API 5G mediante AWS CloudTrail	11/08/2022
AWS Private Certificate Authority (AWS Private CA)	Usando CloudTrail	04/04/2018
AWS Proton	Inicio de sesión y supervisión AWS Proton	06/09/2021
AWS re:Post Privado	Registro de llamadas a la API AWS re:Post privada mediante AWS CloudTrail	26/11/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	Registrar llamadas a la AWS RAM API con AWS CloudTrail	20/11/2018

AWS Servicio	CloudTrail Temas	Solución compatible desde
Explorador de recursos de AWS	Registrar llamadas a la Explorador de recursos de AWS API mediante AWS CloudTrail	11/07/2022
AWS Resource Groups	Registrar llamadas a la AWS Resource Groups API con AWS CloudTrail	29/06/2018
AWS RoboMaker	Registrar llamadas a la AWS RoboMaker API con AWS CloudTrail	16/01/2019
AWS Secrets Manager	Supervise el uso de sus AWS Secrets Manager secretos	05/04/2018
AWS Security Hub	Registrar llamadas a la AWS Security Hub API con AWS CloudTrail	27/11/2018
AWS Security Token Service (AWS STS)	Registrar eventos de IAM con AWS CloudTrail El tema de IAM incluye información sobre. AWS STS	13/11/2013
AWS Serverless Application Repository	Registrar llamadas a AWS Serverless Application Repository la API con AWS CloudTrail	20/02/2018
AWS Service Catalog	Registro de llamadas a la API de Service Catalog con AWS CloudTrail	06/07/2016

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Shield	Llamadas a la API avanzada de Logging Shield con AWS CloudTrail	08/02/2018
AWS Snowball	Registrar llamadas a la AWS Snowball API con AWS CloudTrail	25/01/2019
AWS Snowball Edge	Registrar llamadas a la API de AWS Snowball Edge con AWS CloudTrail	25/01/2019
AWS Step Functions	Registrar llamadas a la AWS Step Functions API con AWS CloudTrail	01/12/2016
Storage Gateway	Registro de llamadas a la API Storage Gateway mediante AWS CloudTrail	16/12/2014
AWS Support	Registrar llamadas a la AWS Support API con AWS CloudTrail	21/04/2016
AWS Systems Manager	Registrar llamadas a la AWS Systems Manager API con AWS CloudTrail	29/11/2017
Administrador de incidentes de AWS Systems Manager	Registrar las llamadas a la API de AWS Systems Manager Incident Manager mediante AWS CloudTrail	10/05/2021
AWS Creador de redes de telecomunicaciones (TNB)AWS	Registro de llamadas a la API de AWS Telco Network Builder mediante AWS CloudTrail	21/02/2023

AWS Servicio	CloudTrail Temas	Solución compatible desde
AWS Transfer for SFTP	Registrar llamadas a la AWS Transfer for SFTP API con AWS CloudTrail	08/01/2019
AWS Transit Gateway	Registro de llamadas a la API para Transit Gateway con AWS CloudTrail	26/11/2018
AWS Trusted Advisor	Registrar las acciones de la AWS Trusted Advisor consola con AWS CloudTrail	22/10/2020
Acceso verificado de AWS	Registre las llamadas a Acceso verificado de AWS la API mediante AWS CloudTrail	27/04/2023
AWS WAF	Registrar llamadas a la AWS WAF API con AWS CloudTrail	28/04/2016
AWS Well-Architected Tool	Registrar llamadas a la AWS Well-Architected Tool API con AWS CloudTrail	15 de diciembre de 2020
AWS X-Ray	Registrar llamadas a la AWS X-Ray API con CloudTrail	25/04/2018
Elastic Load Balancing	AWS CloudTrail Registro de su Load Balancer clásico y AWS CloudTrail registro de su aplicación Load Balancer	04/04/2014
Actualizaciones de transmisión terrestre (OTA) de FreeRTOS	Registrar las llamadas a la API AWS IoT OTA con AWS CloudTrail	22/05/2019

AWS Servicio	CloudTrail Temas	Solución compatible desde
Service Quotas	Registro de llamadas a la API Service Quotas mediante AWS CloudTrail	24/06/2019

Servicios CloudTrail no compatibles

Los servicios que aún se encuentran en versión preliminar, que aún no se han lanzado para su disponibilidad general (GA) o que no tienen API públicas, no se consideran compatibles.

Además, no se admiten los siguientes servicios y eventos de AWS:

- AWS Import/Export
- Eventos específicos de la política de puntos de conexión de Amazon VPC

Para obtener una lista de los servicios de AWS compatibles, consulte AWS temas de servicio para CloudTrail.

Cuotas en AWS CloudTrail

En la siguiente tabla se describen las cuotas (anteriormente denominadas límites) dentro de CloudTrail. CloudTrail no tiene cuotas ajustables. Para obtener información sobre otras cuotas en AWS, consulte Cuotas de servicio de AWS.

Recurso	Cuota predeterminada	Comentarios
Registros de seguimiento por región	5	Esta cuota no puede incrementarse.
Obtener, describir y mostrar las API	10 transacciones por segundo (TPS)	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación. Las `StartQuery` API `CancelQuery` `LookupEve`

Recurso	Cuota predeterminada	Comentarios
		`nts` ,`ListInsig htsMetric Data` ,`PutAuditEvents` , y no se incluyen en esta categoría.
CancelQuery, StartQuery API	3 transacciones por segundo (TPS)	Número máximo de solicitud es de operación que puede realizar por segundo sin que aplique una limitación. Esta cuota no puede incrementarse.
LookupEvents API	2 transacciones por segundo (TPS)	Número máximo de solicitud es de operación que puede realizar por segundo sin que aplique una limitación. Esta cuota no puede incrementarse.
ListInsightsMetricData API	1 transacción por segundo (TPS)	Número máximo de solicitud es de operación que puede realizar por segundo sin que aplique una limitación. Esta cuota no puede incrementarse.
PutAuditEvents API	100 transacciones por segundo (TPS)	Número máximo de solicitud es de operación que puede realizar por segundo sin que aplique una limitación. Esta cuota no puede incrementarse.

Recurso	Cuota predeterminada	Comentarios
Todas las demás API	1 transacción por segundo (TPS)	Número máximo de solicitudes de operación que puede realizar por segundo sin que aplique una limitación. Esta cuota no puede incrementarse.
Almacenes de datos de eventos	10	La cantidad máxima de almacenes de datos de eventos que puede haber en una Región de AWS. Esto incluye los almacenes de datos de eventos de una sola región para la región, así como cualquier almacén de datos de eventos de varias regiones para todas las Regiones de AWS. Esto incluye los almacenes de datos de eventos en cualquier etapa del ciclo de vida. Esta cuota no puede incrementarse.
Canales	25	Esta cuota se aplica a los canales utilizados para las integraciones de CloudTrail Lake con fuentes de AWS eventos externas y no se aplica a los canales vinculados a servicios. Esta cuota no puede incrementarse.

Recurso	Cuota predeterminada	Comentarios
Consultas simultáneas	10	El número máximo de consultas en cola o en ejecución que puedes ejecutar simultáneamente en Lake. CloudTrail Esta cuota no puede incrementarse.
Eventos por solicitud PutAuditEvents	100	Puede agregar hasta 100 eventos de actividad (o hasta 1 MB) por solicitud `PutAuditEvents` . Esta cuota no puede incrementarse.
Selectores de eventos	5 por registro de seguimiento	Esta cuota no puede incrementarse.

Recurso	Cuota predeterminada	Comentarios
Selectores de eventos avanzados	500 condiciones en todos los selectores de eventos avanzados	Si un registro de seguimiento o almacén de datos de eventos utiliza selectores de eventos avanzados, se permite un máximo de 500 valores totales para todas las condiciones en todos los selectores de eventos avanzados. A menos que un registro de seguimiento o almacén de datos de eventos registre eventos de datos en todos los recursos, como todos los buckets de S3 o todas las funciones de Lambda, el registro de seguimiento se limita a 250 recursos de datos. Los recursos de datos se pueden distribuir entre selectores de eventos, pero el total no puede superar los 250. Esta cuota no puede incrementarse.

Recurso	Cuota predeterminada	Comentarios
Recursos de datos en selectores de eventos	250 en todos los selectores eventos, en un registro de seguimiento	Si elige limitar eventos de datos mediante selectores de eventos o selectores de eventos avanzados, la cantidad total de recursos de datos no puede superar los 250 en todos los selectores de eventos en un registro de seguimiento. El límite de la cantidad de recursos de un selector de eventos individual se puede configurar hasta 250. Este límite superior solo se permite si la cantidad total de recursos de datos no supera 250 en el conjunto de todos los selectores de eventos. Ejemplos: • Se permite un registro de seguimiento con 5 selectores de evento (cada evento configurado con 50 recursos de datos). (5*50=250) • También se permite un registro de seguimiento con 5 selectores de eventos, de los cuales 3 estarán configurados con 50 recursos de datos, 1 con 99 recursos de datos y 1 con 1 recurso de datos. [(3*50)+1+99=250]

Recurso	Cuota predeterminada	Comentarios
		• No se permite un registro de seguimiento configura do con 5 selectores de eventos, cada uno de ellos configurado con 100 recursos de datos. (5*100=500) Los selectores de eventos se aplican solo a los registros de seguimiento. Para almacenes de datos de eventos, debe utilizar selectores de eventos avanzados. Esta cuota no puede incrementarse. La cuota no se aplica si elige registrar eventos de datos en todos los recursos, como todos los buckets de S3 o todas las funciones de Lambda.

Recurso	Cuota predeterminada	Comentarios
Tamaño de eventos	Todas las versiones de eventos: los eventos de más de 256 KB no se pueden enviar a CloudWatch los registros Versión 1.05 y posterior del evento: límite de tamaño total del evento de 256 KB	Amazon CloudWatch Logs y Amazon permiten un tamaño máximo de evento de 256 KB EventBridge cada uno. CloudTrail no envía eventos de más de 256 KB a CloudWatch Logs o EventBrid ge. A partir de la versión 1.05 del evento, los eventos tienen un tamaño máximo de 256 KB. El objetivo es evitar que actores malintencionados exploten los eventos y permitir que otros AWS servicios, como CloudWatch Logs y EventBrid ge.
CloudTrail tamaño del archivo enviado a Amazon S3	Archivo ZIP de 50 MB, después de la compresión	Tanto para los eventos de administración como para los de datos, CloudTrail envía los eventos a S3 en archivos ZIP (comprimidos) de un máximo de 50 MB. Si está habilitada en la ruta, Amazon SNS envía las notificaciones de entrega de registros después CloudTrai l de enviar los archivos ZIP a S3.

Cómo empezar con AWS CloudTrail los tutoriales

Si es la primera vez que lo utiliza AWS CloudTrail, estos tutoriales le ayudarán a aprender a utilizar sus funciones.

Temas

- Requisitos previos
- Tutorial: Revisa la actividad AWS de la cuenta en el historial de eventos
- Tutorial: Crear un registro de seguimiento
- Tutoriales para Lake CloudTrail

Requisitos previos

En esta sección se proporciona información general acerca de cómo configurar una Cuenta de AWS y se describe políticas gestionadas disponibles para CloudTrail.

Temas

- Inscríbase en una Cuenta de AWS
- Cómo crear un usuario administrativo
- Otorgue permisos de uso CloudTrail

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como

práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para ejecutar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Cómo crear un usuario administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda sobre cómo iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Cómo crear un usuario administrativo

1. Activar IAM Identity Center

   Consulte las instrucciones en Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En el Centro de identidades de IAM, conceda acceso administrativo a un usuario administrativo.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario administrativo

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Otorgue permisos de uso CloudTrail

Para crear, actualizar y gestionar CloudTrail recursos como rutas, almacenes de datos de eventos y canales, debes conceder permisos de uso CloudTrail.

> **Note**
>
> Los permisos que concede a los usuarios para realizar tareas de CloudTrail administración no son los mismos que CloudTrail los permisos necesarios para entregar archivos de registro a los buckets de Amazon S3 o enviar notificaciones a los temas de Amazon SNS. Para obtener más información acerca de estos permisos, consulte Política de bucket de Amazon S3 para CloudTrail.
> Si configura la integración con Amazon CloudWatch Logs, CloudTrail también se requiere un rol que pueda asumir para entregar eventos a un grupo de CloudWatch registros de Amazon Logs. Debe crear el rol que CloudTrail utiliza. Para más información, consulte Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola y Envío de eventos a Amazon CloudWatch Logs.

Las siguientes políticas AWS administradas están disponibles para CloudTrail:

- AWSCloudTrail_FullAccess— Esta política proporciona acceso total a CloudTrail las acciones en CloudTrail los recursos, como las rutas, los almacenes de datos de eventos y los canales. Esta política proporciona los permisos necesarios para crear, actualizar y eliminar CloudTrail rutas, almacenes de datos de eventos y canales.

  Esta política también proporciona permisos para administrar el bucket de Amazon S3, el grupo de CloudWatch registros de Logs y un tema de Amazon SNS para un rastro. Sin embargo, la política `AWSCloudTrail_FullAccess` gestionada no proporciona permisos para eliminar el bucket de Amazon S3, el grupo de CloudWatch registros de Logs o un tema de Amazon SNS.

Para obtener información sobre las políticas administradas para otros AWS servicios, consulte la Guía de referencia de políticas AWS administradas.

> **Note**
>
> La AWSCloudTrail_FullAccesspolítica no está pensada para que se divulgue ampliamente entre todos sus usuarios Cuenta de AWS. Los usuarios con este rol pueden desactivar o reconfigurar las funciones de auditoría más importantes y confidenciales de su Cuentas de AWS. Por este motivo, solo debe aplicar esta política a los administradores de cuentas. Debe controlar y supervisar de cerca el uso de esta política.

- AWSCloudTrail_ReadOnlyAccess— Esta política otorga permisos para ver la CloudTrail consola, incluidos los eventos recientes y el historial de eventos. Esta política también le permite ver los registros de seguimiento, los almacenes de datos de eventos y los canales existentes. Los roles y los usuarios sujetos a esta política pueden descargar el historial de eventos, pero no pueden crear ni actualizar registros de seguimiento, almacenes de datos de eventos ni canales.

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.

Tutorial: Revisa la actividad AWS de la cuenta en el historial de eventos

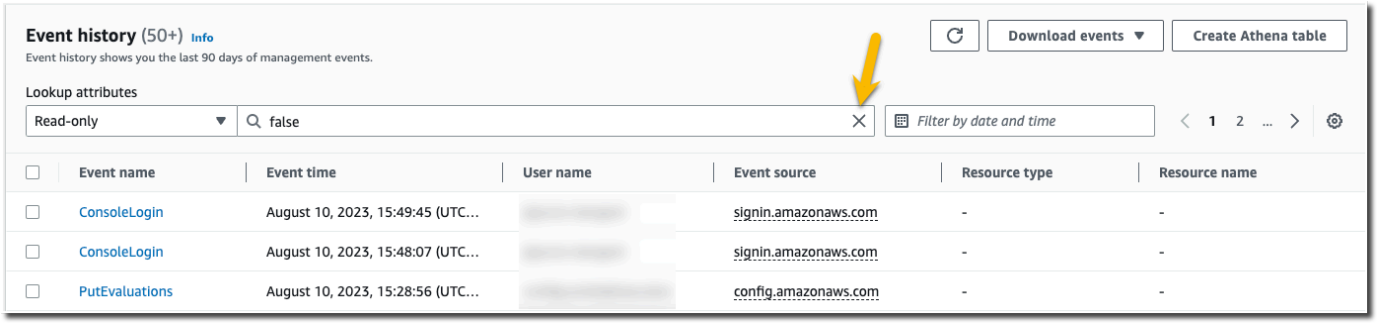
CloudTrail está activo en tu AWS cuenta cuando la creaste. Cuando la actividad de la API admitida (eventos de gestión) se produce en cualquier AWS servicio compatible CloudTrail, esa actividad se registra en un evento CloudTrail de gestión junto con otros eventos de AWS servicio en el historial de eventos. En otras palabras, puede ver, buscar y descargar los eventos de gestión recientes en su AWS cuenta antes de crear un almacén de datos o un registro de eventos, aunque crear un banco de datos o un registro de eventos es importante para registrar y auditar a largo plazo la actividad de su AWS cuenta.

> **Note**
>
> Las limitaciones siguientes son aplicables al Historial de eventos.
>
> - La página del historial de eventos de la CloudTrail consola solo muestra los eventos de gestión. No muestra eventos de datos ni de Insights.
> - El Historial de eventos está limitado a los últimos 90 días. Para tener un registro continuo de tus eventos Cuenta de AWS, crea un almacén de datos de eventos o una ruta.
> - El Historial de eventos no proporciona la agregación de eventos a nivel de organización. Para registrar los eventos de su organización, cree un almacén de datos de eventos o un registro de seguimiento de la organización.
> - La búsqueda en el historial de eventos se limita a una sola Cuenta de AWS, solo devuelve los eventos de una sola Región de AWS y no puede consultar varios atributos.
>
>   Puede crear un banco de datos de eventos de CloudTrail Lake para consultar varios atributos y Regiones de AWS. También puede realizar consultas Cuentas de AWS en varios elementos de una AWS Organizations organización. En CloudTrail Lake, puede consultar varios tipos de eventos, incluidos los eventos de administración, los eventos de datos, los elementos de AWS Config configuración, las pruebas de Audit Manager y las que no son AWS eventos. CloudTrail Las consultas de Lake ofrecen una visión más profunda y personalizable de los eventos que las simples búsquedas de claves y valores en el historial de eventos o en ejecución. `LookupEvents` Para más información, consulte Trabajando con AWS CloudTrail Lake y Cree un banco de datos de CloudTrail eventos para eventos.

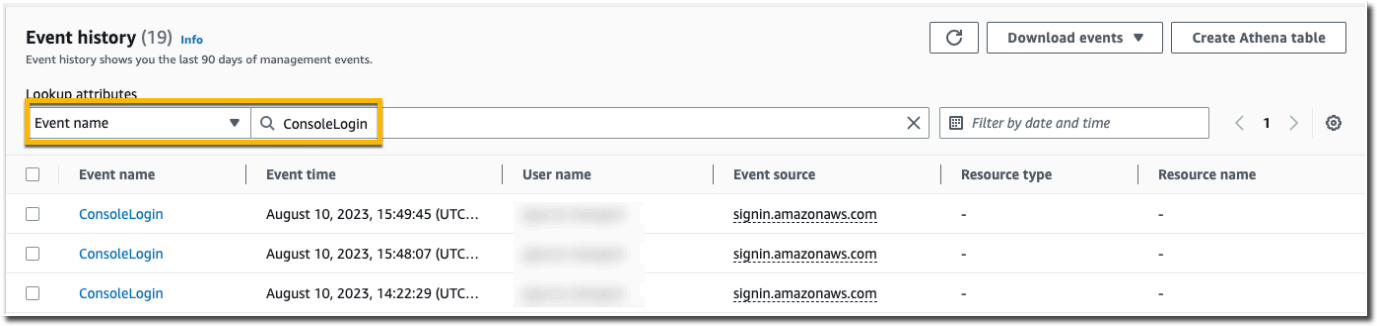
- No puede excluir AWS KMS ni los eventos de la API de datos de Amazon RDS del historial de eventos; los ajustes que aplique a un almacén de datos de eventos o senderos no se aplican al historial de eventos.

Para ver el Historial de eventos

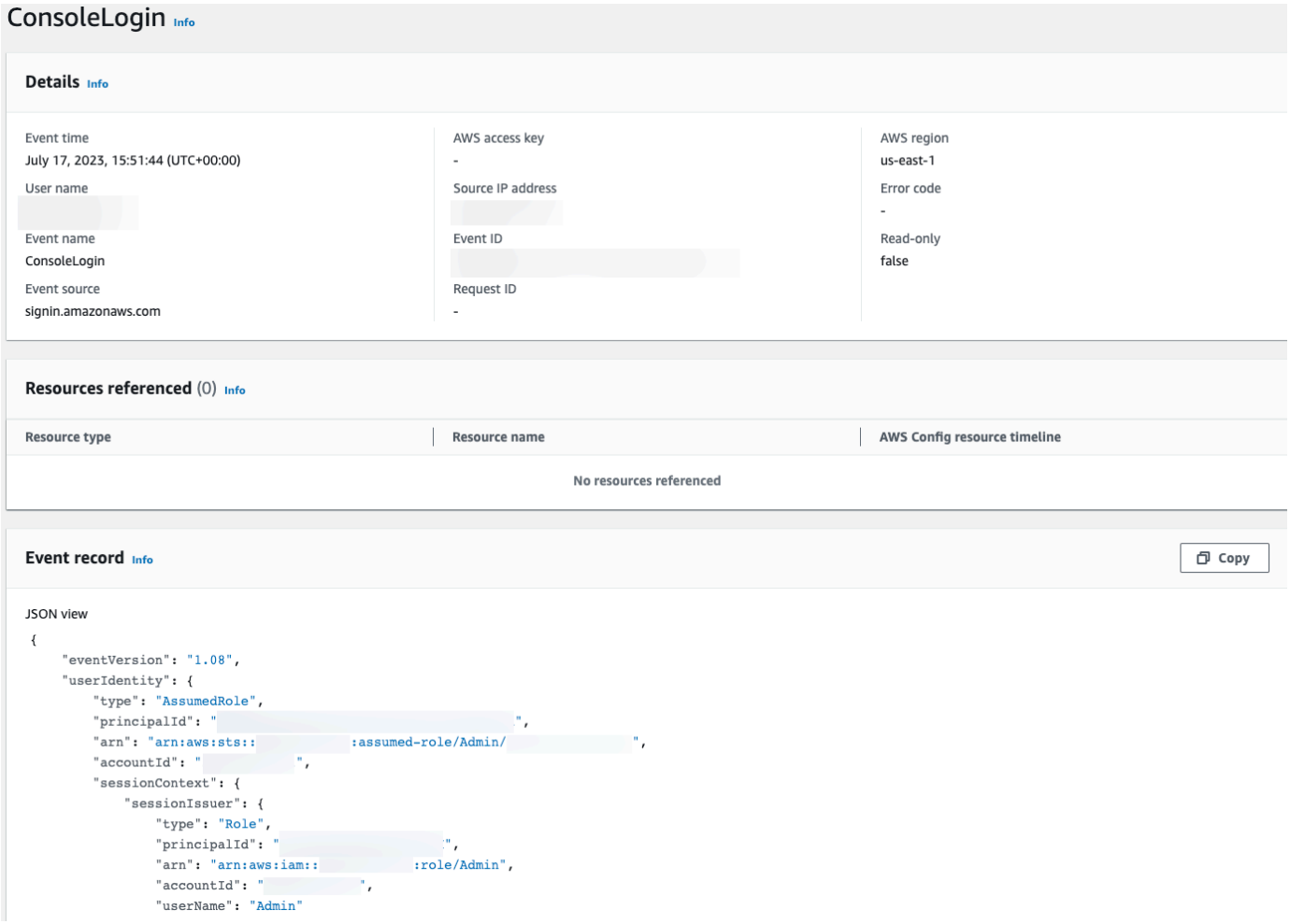
1. Inicia sesión en la CloudTrail consola AWS Management Console y ábrela en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, elija Event history (Historial de eventos). Verá una lista filtrada de eventos, con los últimos eventos en primer lugar. El filtro predeterminado de eventos es Read only (Solo lectura), con el valor false. Puede borrar ese filtro, al elegir X a la derecha del filtro. Puede buscar eventos en el Historial de eventos filtrando los eventos en un solo atributo



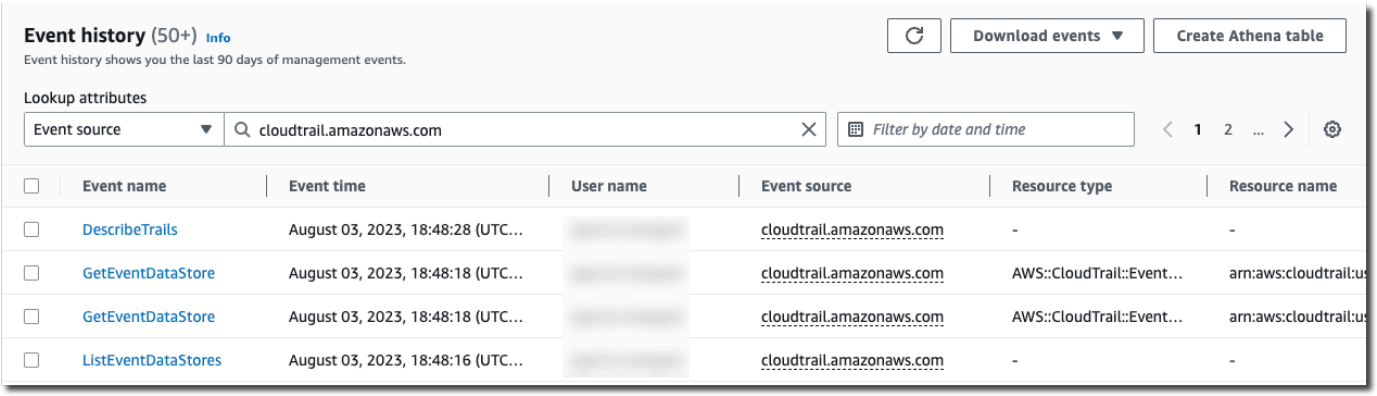
3. Si se quita el filtro predeterminado, se muestran muchos más eventos. Puede filtrar los eventos de muchas formas. Por ejemplo, para ver todos los eventos de inicio de sesión en la consola, puede elegir el filtro de nombre del evento y especificarlo. ConsoleLogin Elija los filtros que desee.



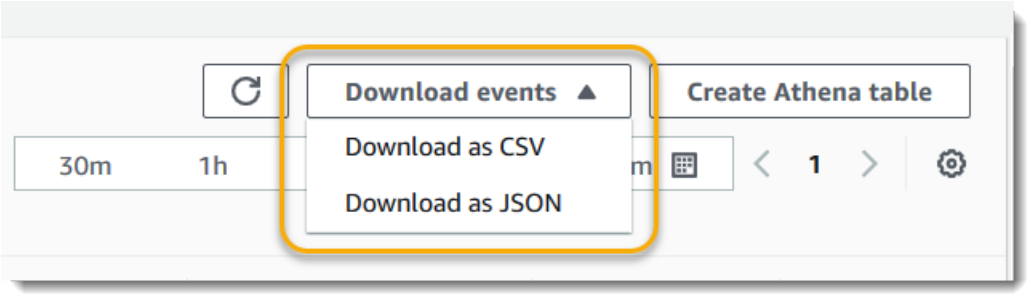
4. Para ver un evento de administración específico, seleccione el nombre del evento. En la página de detalles del evento, puede ver los detalles del evento, ver los recursos a los que se hace referencia y ver el registro del evento.



5. Para ver los eventos de administración recientes de un servicio, filtre según el origen del evento.



6. Puede guardar el historial de eventos descargándolo como un archivo con formato CSV o JSON. Descargar el historial de eventos puede demorar unos minutos.



Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Tutorial: Crear un registro de seguimiento

Si bien los eventos proporcionados en el historial de eventos de la CloudTrail consola son útiles para revisar la actividad reciente de los eventos de gestión, se limitan a la actividad reciente y no incluyen todos los eventos posibles que se pueden registrar CloudTrail, como los datos y los eventos de Insights. Además, la visualización de los eventos en la consola se limita a la AWS región en la que has iniciado sesión. Para crear un registro continuo de la actividad en tu AWS cuenta que recoja la información de todas AWS las regiones, puedes crear una ruta. De forma predeterminada, al crear una ruta en la CloudTrail consola, la ruta registra todos los Regiones de AWS eventos de la AWS partición en la que está trabajando. Registrar eventos en todas las regiones de su cuenta es una práctica recomendada.

Para tu primera ruta, te recomendamos crear una ruta que registre todos los eventos de gestión en todas AWS las regiones y no registre ningún evento de datos. Por ejemplo, son eventos de administración los eventos de seguridad, como `CreateUser` y `AttachRolePolicy` de IAM, los eventos de recursos como `RunInstances` y `CreateBucket`, etc. Creará un depósito de Amazon S3 en el que almacenará los archivos de registro de la ruta como parte de la creación de la ruta en la CloudTrail consola.

> **Note**
>
> En este tutorial, se presupone que está creando su primer registro de seguimiento. En función de la cantidad de rutas que tenga en su AWS cuenta y de cómo estén configuradas esas rutas, el siguiente procedimiento podría implicar gastos o no. CloudTrail almacena los archivos de registro en un bucket de Amazon S3, lo que conlleva costes. Para obtener más información sobre los precios, consulte Precios de AWS CloudTrail y Precios de Amazon S3.

Para crear un registro de seguimiento

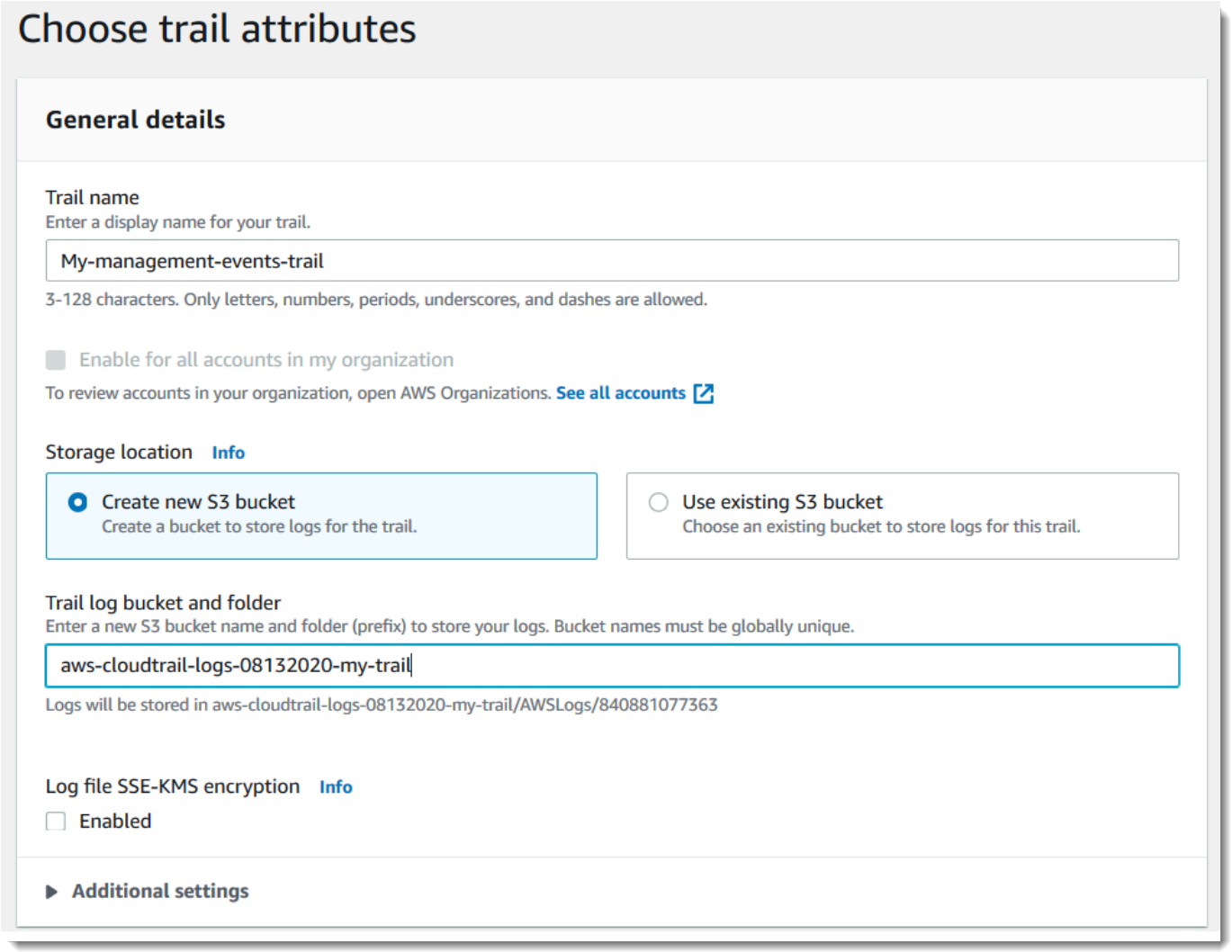
1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el selector de regiones, elige la AWS región en la que quieres que se cree tu ruta. Esta es la región principal del registro de seguimiento.

   > **Note**
   >
   > La región de origen es la única AWS región en la que puedes ver y actualizar la ruta una vez creada, incluso si la ruta registra los eventos en todas AWS las regiones.

3. En la página CloudTrail de inicio del servicio, en la página de senderos o en la sección Rutas de la página del panel de control, selecciona Crear ruta.
4. En Trail name (Nombre del registro de seguimiento), indique el nombre del registro de seguimiento, como, por ejemplo, *`My-Management-Events-Trail`*. Como práctica recomendada, utilice un nombre que identifique rápidamente el propósito del registro de seguimiento. En este caso, está creando un registro de seguimiento que registra eventos de administración.
5. Deje la configuración predeterminada en Activar para todas las cuentas de mi organización. No podrá cambiar esta opción a menos que tenga cuentas configuradas en Organizations.
6. En Storage location (Ubicación del almacenamiento), elija Create new S3 bucket (Crear un bucket de S3 nuevo) para crear un bucket. Al crear un segmento, CloudTrail crea y aplica las políticas del segmento requeridas. Dale un nombre a tu depósito, como *`my-bucket-for-storing-cloudtrail-logs`*.

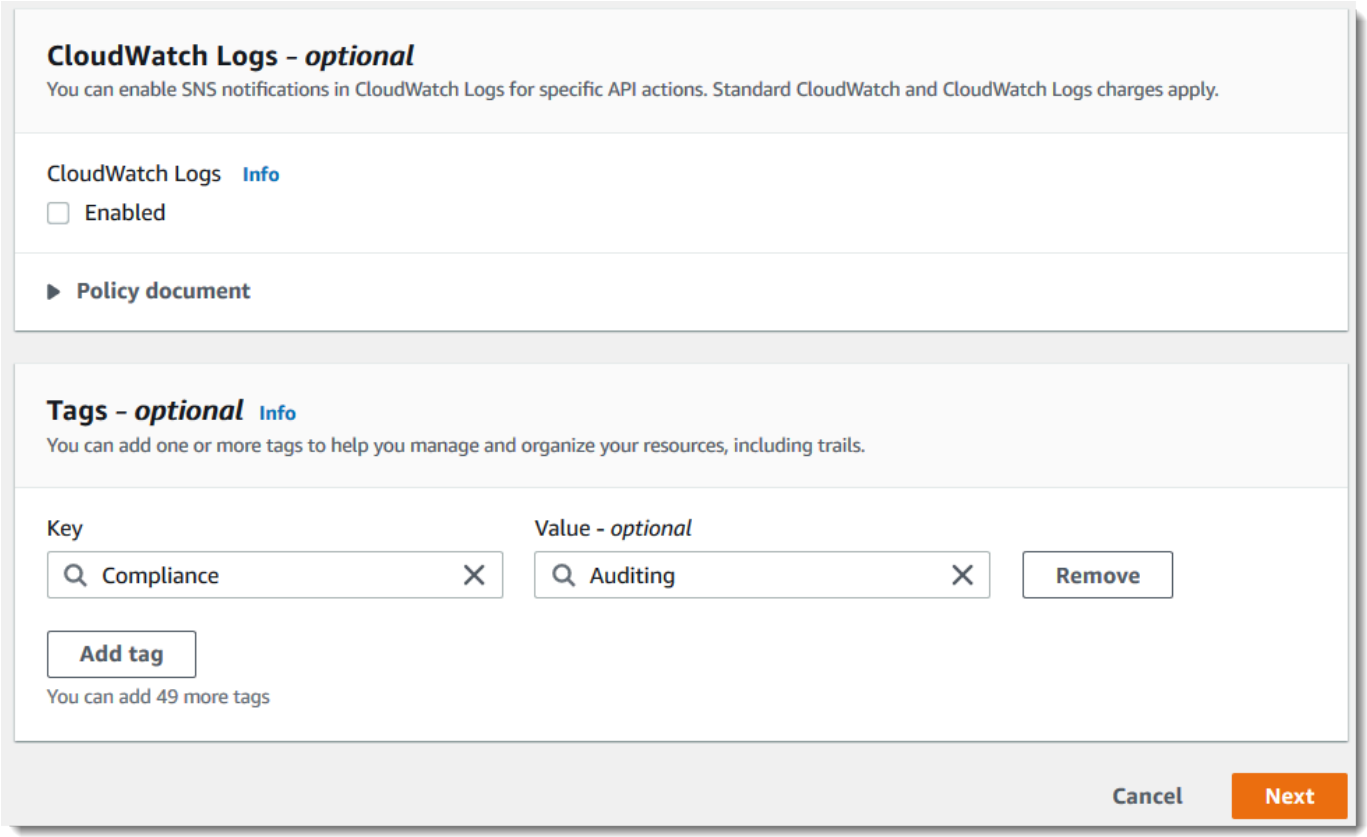
   Para que sea más fácil encontrar tus registros, crea una nueva carpeta (también conocida como prefijo) en un depósito existente para almacenar tus registros. CloudTrail

   > **Note**
   >
   > El nombre del bucket de Amazon S3 debe ser único de forma global. Para obtener más información, consulte Reglas de nomenclatura de buckets en la Guía del usuario de Amazon Simple Storage Service.



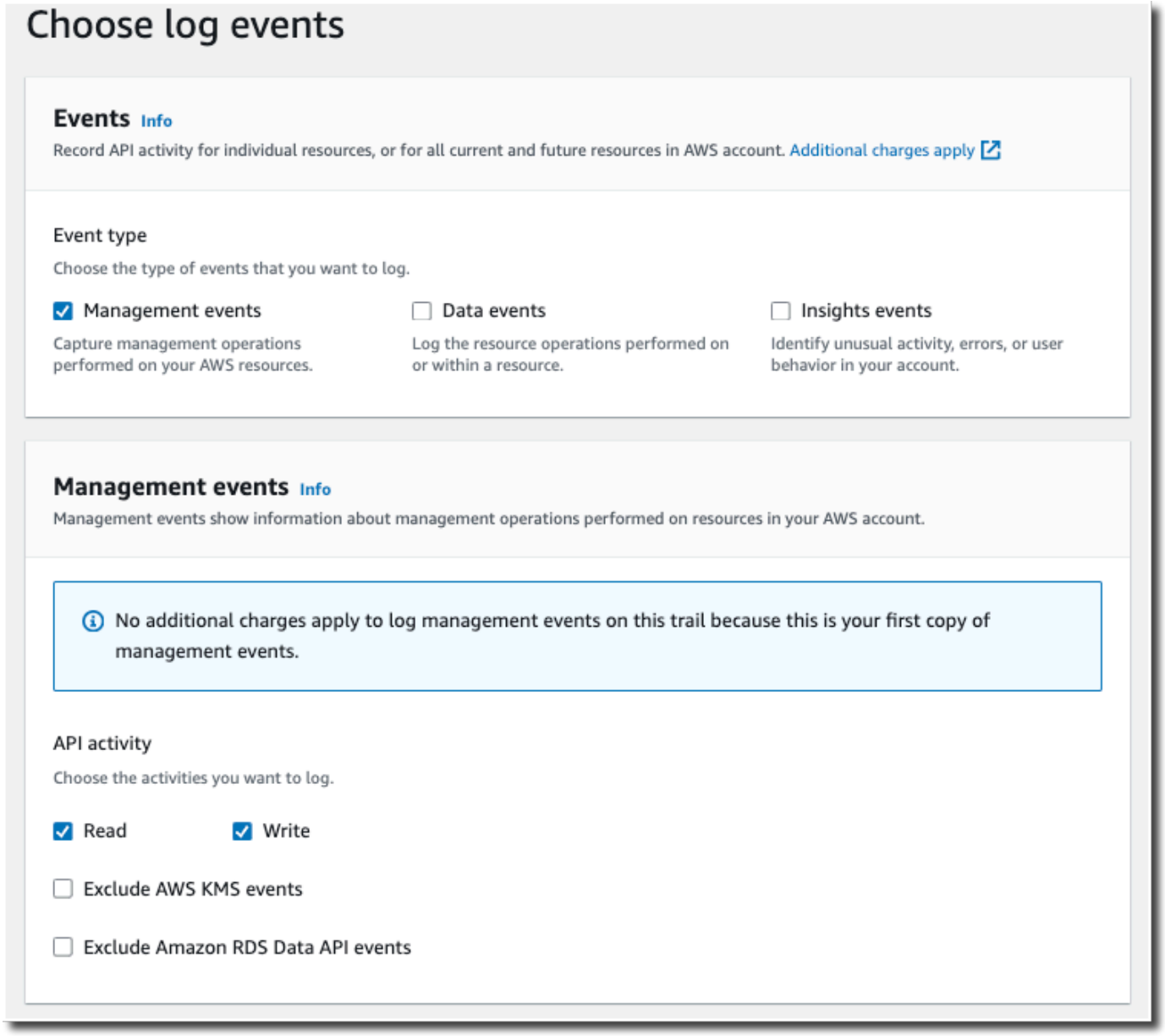
7. Desactive la casilla de verificación para deshabilitar el cifrado con SSE-KMS del archivo de registros. De forma predeterminada, los archivos de registros se cifran con el SSE de S3. Para obtener más información sobre esta configuración, consulte Protección de los datos mediante el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3).
8. Mantenga la configuración predeterminada de los Ajustes adicionales.
9. Deja la configuración predeterminada para los CloudWatch registros. Por ahora, no envíes registros a Amazon CloudWatch Logs.
10. (Opcional) En Etiquetas, agregue una o más etiquetas personalizadas (pares clave-valor) a su registro de seguimiento. Las etiquetas pueden ayudarle a identificar sus CloudTrail rutas y otros recursos, como los depósitos de Amazon S3 que contienen archivos de CloudTrail registro. Por ejemplo, podría adjuntar una etiqueta con el nombre **`Compliance`** y el valor **`Auditing`**.

> **Note**
>
> Aunque puede añadir etiquetas a las rutas al crearlas en la CloudTrail consola y puede crear un bucket de Amazon S3 para almacenar sus archivos de registro en la CloudTrail consola, no puede añadir etiquetas al bucket de Amazon S3 desde la CloudTrail consola. Para obtener más información sobre cómo ver y cambiar las propiedades de un bucket de Amazon S3, incluida la adición de etiquetas a un bucket, consulte la Guía del usuario de Amazon S3.

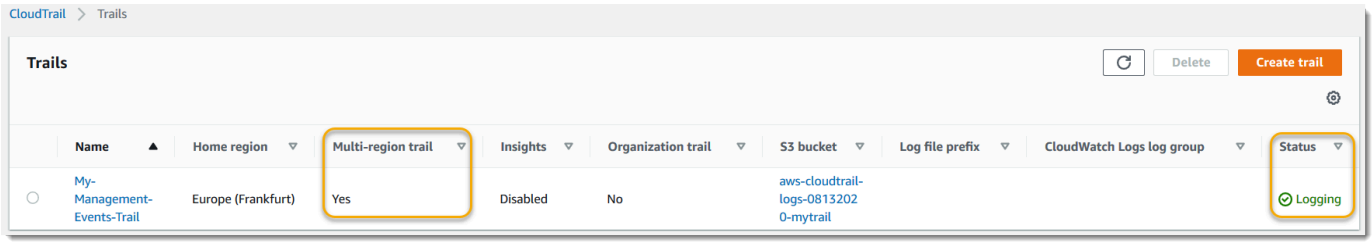


Cuando haya terminado de crear las etiquetas, seleccione Next (Siguiente).

11. En la página Choose log events (Elegir eventos de registro), seleccione los tipos de eventos que desea registrar. Para este registro de seguimiento mantenga el valor predeterminado, Eventos de administración. En la zona de Management events (Eventos de administración), elija registrar tanto los eventos de Read (Lectura) como los eventos de Write (Escritura), si aún no están seleccionados. Deje vacías las casillas Excluir AWS KMS eventos y Excluir eventos de la API de datos de Amazon RDS para registrar todos los eventos de administración.



12. Mantenga la configuración predeterminada para Eventos de datos y Eventos de Insights. Esta ruta no registrará ningún dato ni evento de CloudTrail Insights. Elija Siguiente.
13. En la página Review and create (Revisar y crear), revise la configuración que ha elegido para el registro de seguimiento. Elija Edit (Editar) para una sección a fin de retroceder y realizar cambios. Cuando esté listo para crear el registro de seguimiento, elija Create trail (Crear registro de seguimiento).
14. La página Trails (Registros de seguimiento) muestra el nuevo registro de seguimiento en la tabla. Tenga en cuenta que el registro de seguimiento está establecido de forma predeterminada como Multi-region trail (Registro de seguimiento de varias regiones) y está activado para el registro de seguimiento de forma predeterminada.



Tutorial: Ver los archivos de registro

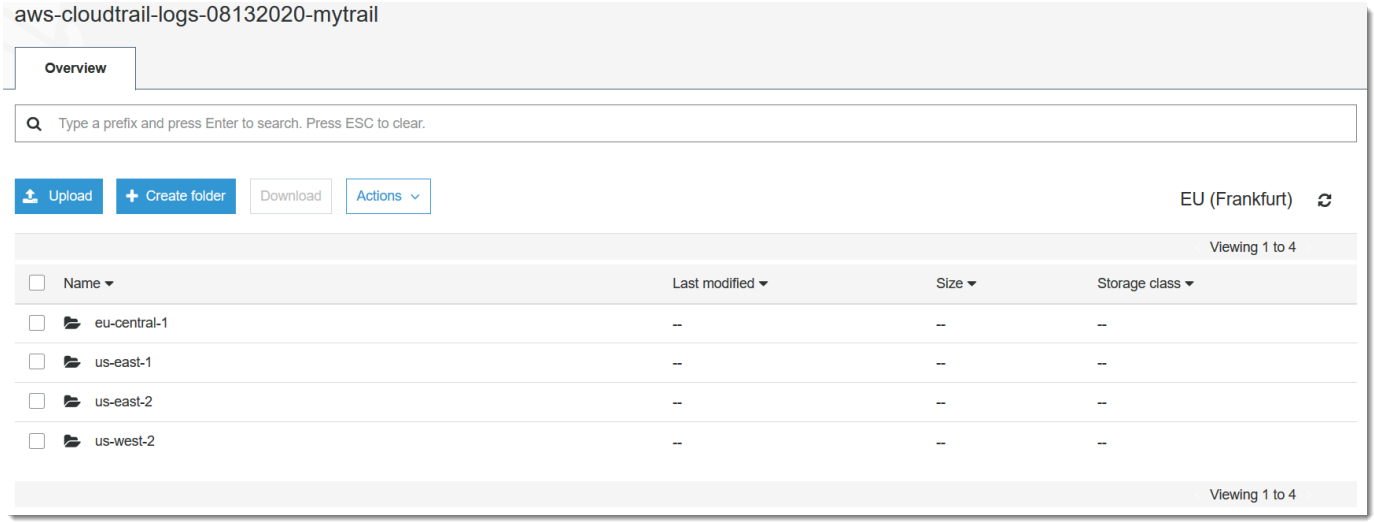
En un promedio de unos 5 minutos desde la creación de la primera ruta, CloudTrail entrega el primer conjunto de archivos de registro al bucket de Amazon S3 de la ruta. Puede ver estos archivos y analizar la información que contienen.

> **Note**
>
> CloudTrail Por lo general, entrega los registros en una media de unos 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el Acuerdo de nivel de servicios de AWS CloudTrail.
> Si configuras mal la ruta (por ejemplo, si no se puede acceder al depósito de S3), CloudTrail intentarás volver a enviar los archivos de registro a tu depósito de S3 durante 30 días. Estos attempted-to-deliver eventos estarán sujetos a los cargos estándar. CloudTrail Para evitar que se le cobre por un registro de seguimiento mal configurado, debe eliminarlo.

Para ver los archivos de registro

1. Inicie sesión en la consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/. CloudTrail
2. En el panel de navegación, seleccione Trails. En la página Trails (Registros de seguimiento), busque el nombre del registro de seguimiento que acaba de crear (en el ejemplo, *My-Management-Events-Trail*).
3. En la fila de la ruta, elige el valor del segmento S3 (en el ejemplo, *aws-cloudtrail-logs-08132020-mytrail*).
4. La consola de Amazon S3 se abre y muestra ese bucket, en el nivel superior de los archivos de registro. Como ha creado un registro que registra los eventos en todas AWS las regiones, la pantalla se abre en el nivel que muestra cada carpeta de la región. *La jerarquía de la navegación por buckets de Amazon S3 en este nivel es bucket-name/AWS*

Logs/ account-id/. CloudTrail Elija la carpeta de la AWS región en la que desee revisar los archivos de registro. Por ejemplo, si desea examinar los archivos de registros de la región EE. UU. Este (Ohio), elija us-este-2.



5. Desplácese por la estructura de carpetas del bucket hasta el año, el mes y el día cuyos registros de actividad desea examinar en esa región. En ese día, hay una serie de archivos. El nombre de los archivos comienza con el ID de su AWS cuenta y termina con la extensión `.gz`. *Por ejemplo, si tu ID de cuenta es 123456789012, verás archivos con nombres similares a los siguientes: 123456789012 _ us-east-2 _ 20190610t1255abcdeexample .json.gz. CloudTrail*

   Para ver estos archivos, puede descargarlos, descomprimirlos y, a continuación, verlos en un editor de texto sin formato o en un visor de archivos JSON. Algunos navegadores también permiten visualizar archivos .gz y JSON directamente. Te recomendamos usar un visor JSON, ya CloudTrail que facilita el análisis de la información de los archivos de registro.

   A medida que navega por el contenido del archivo, es posible que comience a preguntarse qué está viendo. CloudTrail registra los eventos de todos los AWS servicios que estaban activos en esa AWS región en el momento en que ocurrió el evento. En otras palabras, los eventos de AWS los distintos servicios se combinan en función únicamente del tiempo. Para obtener más información sobre los elementos con los que se registra un AWS servicio específico CloudTrail, incluidos ejemplos de entradas en los archivos de registro de las llamadas a la API de ese servicio, consulta la lista de servicios compatibles y lee el tema sobre la CloudTrail integración de ese servicio. CloudTrail También puede obtener más información sobre el contenido y la estructura de los archivos de CloudTrail registro consultando laReferencia de eventos de registro de CloudTrail.

También es posible que se dé cuenta de lo que no está viendo en los archivos de registros de EE. UU. Este (Ohio). En concreto, no verá los eventos de inicio de sesión en la consola, aunque sepa que ha iniciado sesión en la consola. Esto se debe a que el inicio de sesión en la consola y los eventos de IAM son eventos de servicio globales que, por lo general, se registran en una región específica AWS . En este caso, se registran en EE. UU. Este (Norte de Virginia) y se encuentran en la carpeta de us-east-1. Abra esa carpeta y el año, mes y día que le interese. Examine los archivos de registro y busque los eventos `ConsoleLogin` que tengan un aspecto similar al siguiente:

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "userName": "Mary_Major"
    },
    "eventTime": "2019-06-10T17:14:09Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.67",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101
 Firefox/60.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?state=hashArgs
%23&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "2681fc29-EXAMPLE",
    "eventType": "AwsConsoleSignIn",
    "recipientAccountId": "123456789012"
}
```

Esta entrada de archivo de registro le indica algo más que la identidad del usuario de IAM que ha iniciado sesión (`Mary_Major`), la fecha y la hora en que ha iniciado sesión y que el inicio de sesión se ha llevado a cabo correctamente. También puede ver la dirección IP desde la que ha iniciado sesión, el sistema operativo y el software del navegador del equipo que ha utilizado, y que no estaba utilizando la autenticación multifactor.

Planificar los pasos siguientes

Ahora que tienes un registro, tienes acceso a un registro continuo de los eventos y actividades de tu AWS cuenta. Este registro continuo le ayuda a satisfacer las necesidades de auditoría y contabilidad de su cuenta de AWS . Sin embargo, hay muchas más cosas que puedes hacer con CloudTrail los CloudTrail datos.

- Añade seguridad adicional a los datos de tus senderos. CloudTrailaplica automáticamente un cierto nivel de seguridad al crear un sendero. Sin embargo, hay más medidas que puede adoptar para ayudar a mantener los datos seguros.
  - De forma predeterminada, el depósito de Amazon S3 que creó como parte de la creación de una ruta tiene aplicada una política que permite CloudTrail escribir archivos de registro en ese depósito. El bucket no es de acceso público, pero es posible que otros usuarios de su AWS cuenta puedan acceder a él si tienen permisos para leer y escribir en los buckets de su AWS cuenta. Revise la política del bucket y, si es necesario, haga cambios para restringir el acceso. Para obtener más información, consulte la documentación de seguridad de Amazon S3 y la explicación de ejemplo para proteger un bucket.
  - Los archivos de registro que envía CloudTrail a tu bucket se cifran mediante el cifrado del lado del servidor de Amazon con claves de cifrado gestionadas por Amazon S3 (SSE-S3). Para proporcionar una capa de seguridad que se pueda administrar directamente, puede utilizar el cifrado del lado del servidor con claves administradas AWS KMS(SSE-KMS) para sus archivos de registro. CloudTrail Para usar SSE-KMS CloudTrail, debe crear y administrar una clave KMS, también conocida como. AWS KMS key Para obtener más información, consulte Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS).
  - Para una planificación de seguridad adicional, consulte las prácticas recomendadas de seguridad de. CloudTrail
- Crear un registro de seguimiento para registrar los eventos de datos. Si le interesa registrar cuándo se añaden, recuperan y eliminan objetos en uno o más buckets de Amazon S3, cuando se añaden, cambian o eliminan elementos en las tablas de DynamoDB o cuando se invoca una o

AWS Lambda más funciones, se trata de eventos de datos. El registro de seguimiento de eventos de administración que creó anteriormente en este tutorial no registra estos tipos de eventos. Puede crear un registro independiente específico para registrar los eventos de datos de algunos o todos los tipos de recursos compatibles. Para obtener más información, consulte Eventos de datos.

> **Note**
>
> Se aplican cargos adicionales para registrar eventos de datos. Para obtener más información, consulte AWS CloudTrail Precios.

- Registra los eventos de CloudTrail Insights en tu ruta. AWS CloudTrail Gracias al análisis continuo de los eventos de CloudTrail gestión, Insights ayuda a AWS los usuarios a identificar y responder a las actividades inusuales asociadas a las llamadas a las API y a las tasas de error de las API. CloudTrail Insights utiliza modelos matemáticos para determinar los niveles normales de actividad de las API y los eventos de servicio de una cuenta. Identifica comportamientos que se encuentran fuera de los patrones normales, genera eventos de Insights y entrega esos eventos a una carpeta `/CloudTrail-Insight` en el bucket de S3 de destino elegido para el registro de seguimiento. Para obtener más información sobre CloudTrail Insights, consulteRegistro de eventos de Insights.

  > **Note**
  >
  > Se aplican cargos adicionales por registrar eventos de Insights. Para obtener más información, consulte AWS CloudTrail Precios.

- Configure las alarmas de CloudWatch Logs para que le avisen cuando se produzcan determinados eventos. CloudWatch Los registros le permiten monitorear y recibir alertas sobre eventos específicos capturados por CloudTrail. Por ejemplo, puede supervisar los principales eventos de administración y seguridad relacionados con la red, como los cambios en los grupos de seguridad, los errores de inicio de AWS Management Console sesión o los cambios en las políticas de IAM. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.
- Utilice herramientas de análisis para identificar las tendencias en sus registros. CloudTrail Aunque los filtros del historial de eventos le ayudan a encontrar eventos o tipos de eventos específicos en su actividad reciente, no proporcionan la capacidad de realizar búsquedas durante periodos de tiempo de actividad más largos. Para realizar análisis más detallados y sofisticados, puede utilizar Amazon Athena. Para obtener más información, consulte Consulta de AWS CloudTrail registros en la Guía del usuario de Amazon Athena.

Tutoriales para Lake CloudTrail

Si bien puedes buscar eventos en el historial de eventos, estás limitado a uno solo Cuenta de AWS, solo puedes devolver los eventos de uno Región de AWS y no puedes consultar varios atributos. Por el contrario, al crear un CloudTrail banco de datos de eventos de Lake, puede ejecutar consultas SQL complejas en varios campos de eventos y también puede consultar eventos en varios Regiones de AWS y Cuentas de AWS. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción Precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción Precio de retención de siete años. Puede crear un banco de datos de eventos para recopilar eventos CloudTrail de administración y datos, elementos de AWS Config configuración, AWS Audit Manager pruebas o no relacionados con AWS eventos. Puede crear almacenes de datos de eventos mediante la consola AWS CLI, la o la CloudTrail API.

CloudTrail Los almacenes de datos y las consultas de eventos de Lake conllevan cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Cuando ejecuta consultas en Lake, paga según la cantidad de datos escaneados. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Los siguientes tutoriales le muestran cómo realizar tareas comunes de CloudTrail Lake en la consola. Para obtener más información sobre CloudTrail Lake, consulteTrabajando con AWS CloudTrail Lake.

Temas

- Tutorial: Creación de un almacén de datos de eventos para eventos de administración
- Tutorial: Creación de un almacén de datos de eventos para eventos de datos de S3
- Tutorial: Copia los eventos del sendero a CloudTrail Lake
- Tutorial: Ver los paneles de Lake
- Tutorial: Ver y ejecutar consultas de ejemplo
- Tutorial: Guardar los resultados de las consultas en un bucket de Amazon S3

Tutorial: Creación de un almacén de datos de eventos para eventos de administración

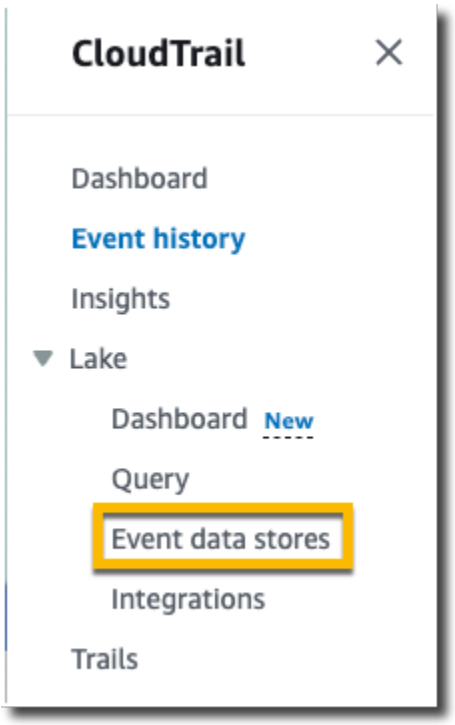
Puede crear un banco de datos de eventos para registrar CloudTrail eventos (eventos de administración, eventos de datos), eventos de CloudTrail Insights, AWS Audit Manager pruebas, elementos de AWS Config configuración o no AWS eventos.

En este tutorial, se muestra cómo crear un banco de datos de eventos que registre todos los eventos de gestión en todas AWS las regiones y no registre ningún evento de datos. Por ejemplo, son eventos de administración los eventos de seguridad, como `CreateUser` y `AttachRolePolicy` de IAM, los eventos de recursos como `RunInstances` y `CreateBucket`, etc.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Para crear un almacén de datos de eventos para eventos de administración

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.



3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configurar el almacén de datos de eventos, en Detalles generales, asigne un nombre al almacén de datos de eventos, por ejemplo `my-management-events-eds`. Como práctica recomendada, utilice un nombre que identifique rápidamente el propósito del almacén de datos de eventos. Para obtener información sobre los requisitos de CloudTrail nomenclatura, consulteRequisitos de nomenclatura.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

   - Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
     - Periodo de retención predeterminado: 366 días.

- Periodo máximo de retención: 3653 días.

- Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
  - Periodo de retención predeterminado: 2557 días.
  - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

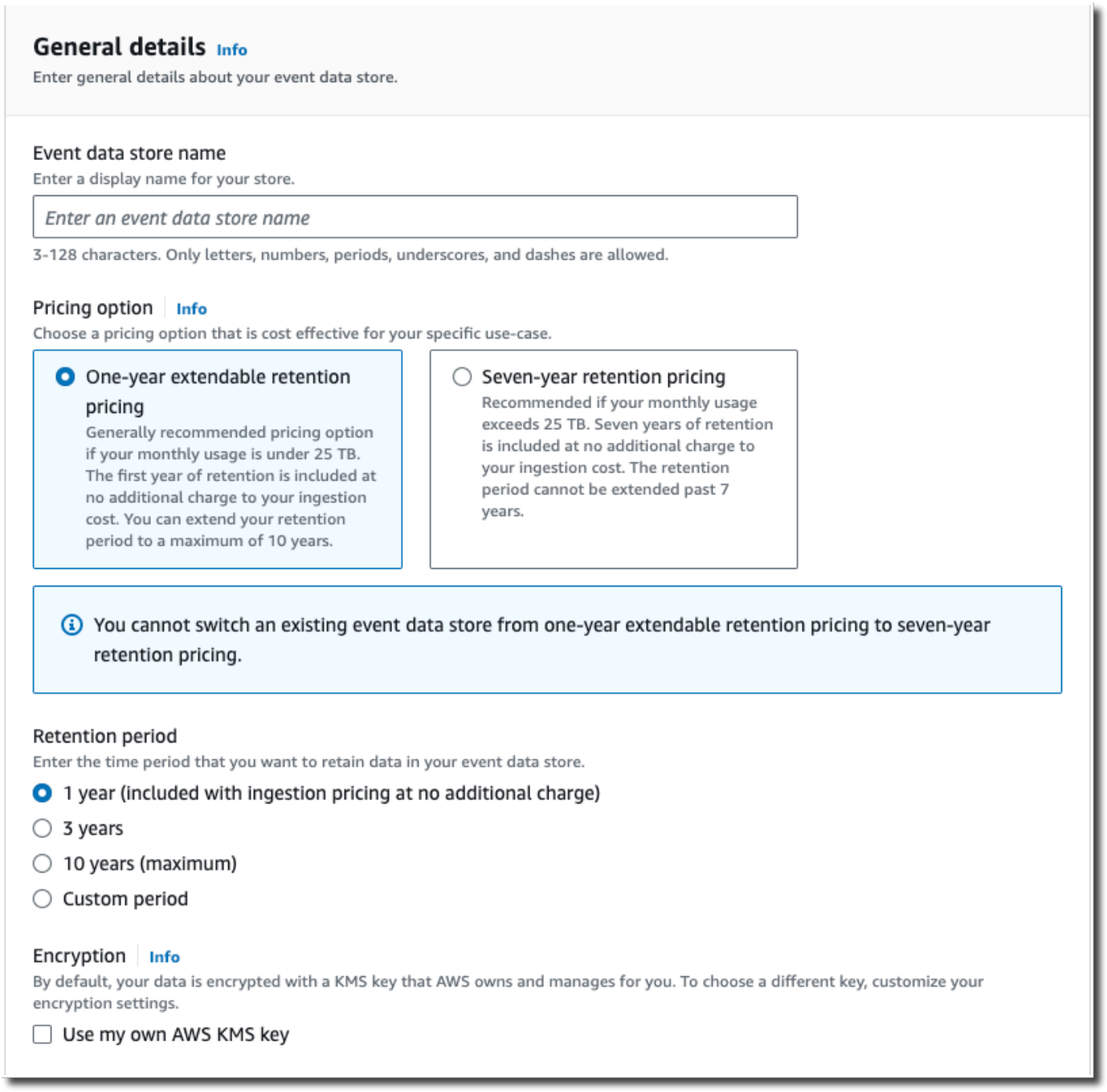
   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

7. (Opcional) En Cifrado, seleccione si quiere cifrar el almacén de datos de eventos con su propia clave de KMS. De forma predeterminada, todos los eventos de un almacén de datos de eventos se cifran CloudTrail mediante una clave de KMS que le AWS pertenece y administra por usted.

   Para habilitar el cifrado con su propia clave de KMS, seleccione Usar mi propia AWS KMS key. Elija Nuevo para que se AWS KMS key cree una por usted, o bien elija Existente para usar una clave de KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

> **Note**
>
> Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.



8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

   Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

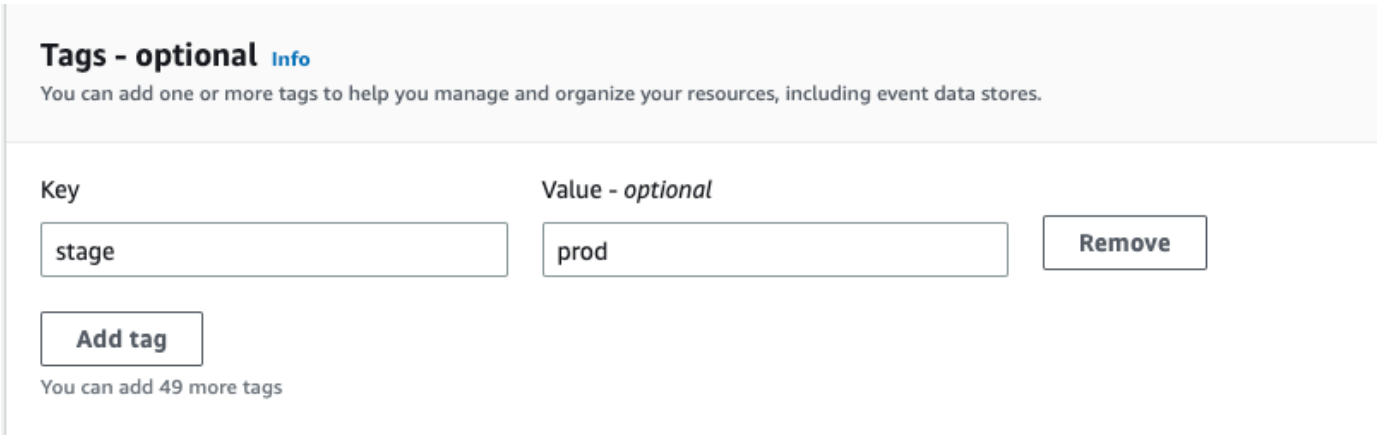
   a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

   b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

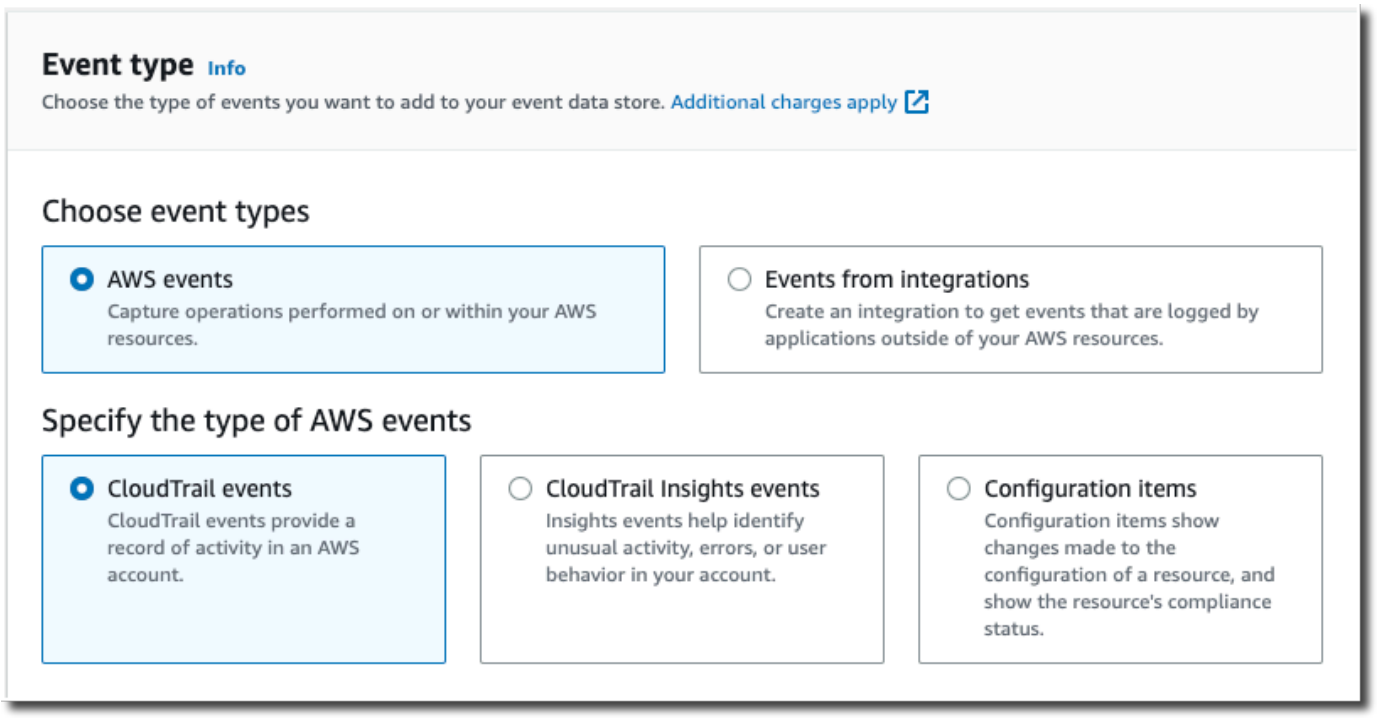
   c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En Etiquetas, agregue una o más etiquetas personalizadas (pares clave-valor) a su almacén de datos de eventos. Las etiquetas pueden ayudarle a identificar los almacenes de datos de sus CloudTrail eventos. Por ejemplo, podría adjuntar una etiqueta con el nombre **`stage`** y el valor **`prod`**. Puede utilizar etiquetas para limitar el acceso al almacén de datos de eventos. También puede utilizar etiquetas para hacer un seguimiento de los costos de consulta e ingesta del almacén de datos de eventos.

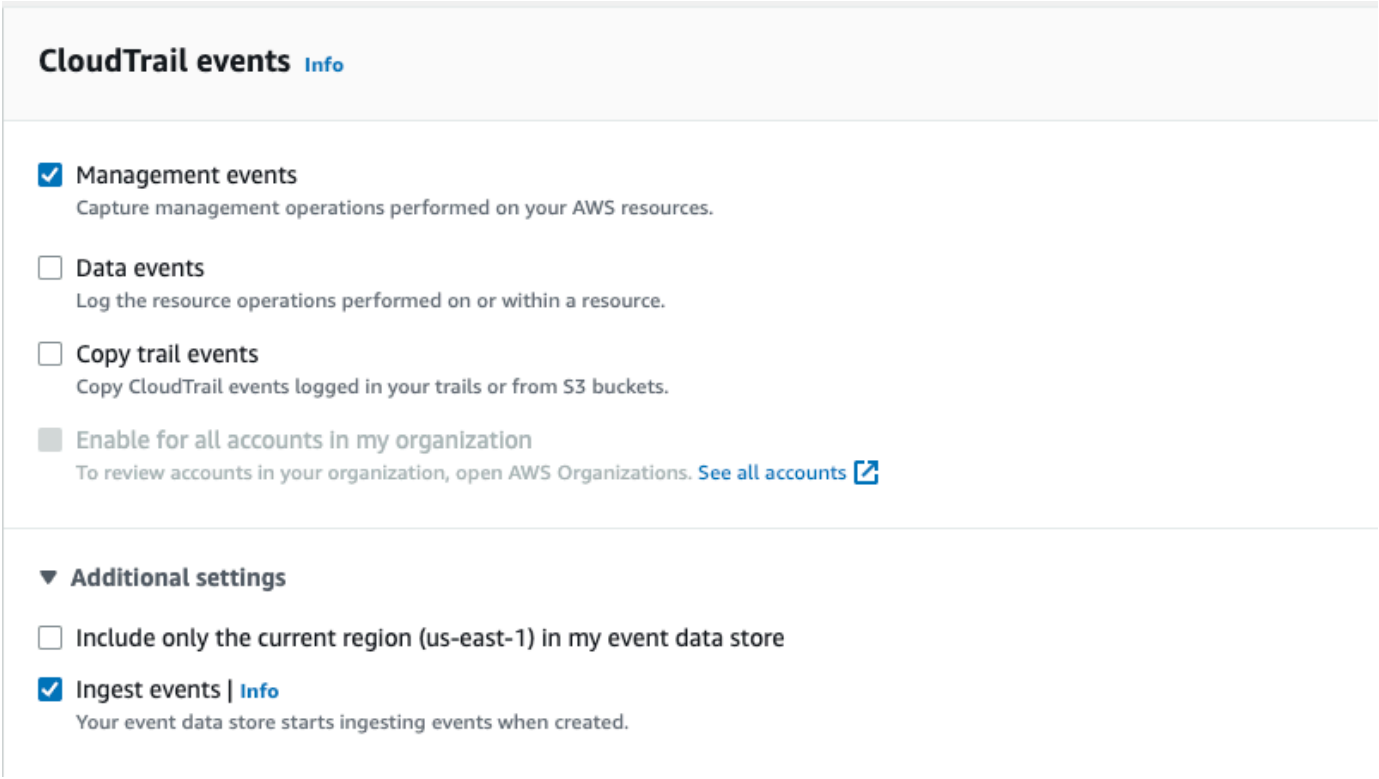
   Para obtener más información acerca de cómo usar etiquetas para hacer un seguimiento de los costos, consulte Creación de etiquetas de asignación de costes definidas por el usuario para los almacenes de datos de eventos de CloudTrail Lake. Para obtener información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener información sobre cómo puede utilizar las etiquetas en AWS, consulte AWS los recursos de etiquetado en. Referencia general de AWS



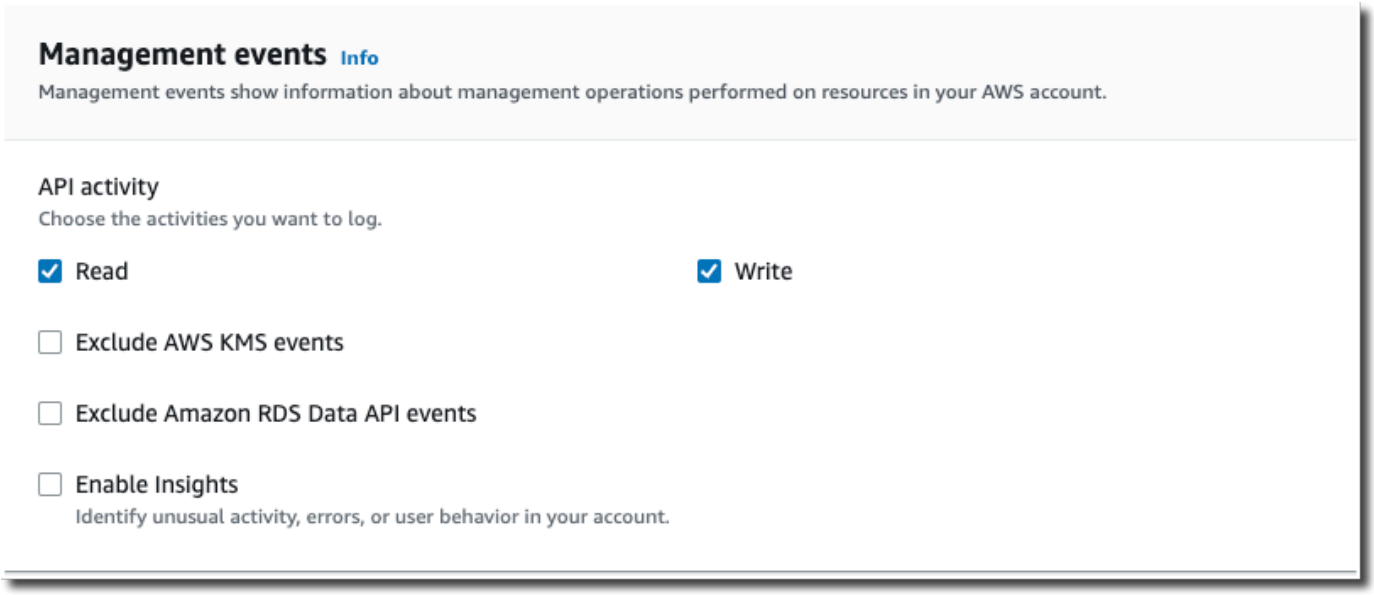
10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
11. En la página Seleccionar eventos, deje las selecciones predeterminadas en Tipo de evento.



12. Para CloudTrail los eventos, deje las selecciones predeterminadas. De forma predeterminada, los almacenes de datos de CloudTrail eventos recopilan eventos de administración y no recopilan eventos de datos. Para obtener más información sobre los eventos de administración, consulte Registro de eventos de administración. Para obtener más información sobre los eventos de datos, consulte Registro de eventos de datos.

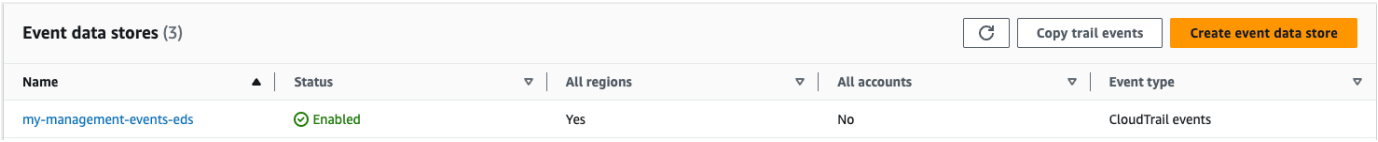


13. Deje la configuración predeterminada para Copiar eventos de los registros de seguimiento. Utilizaría esta opción para copiar los eventos de los registros de seguimiento existentes en el almacén de datos de eventos. Para obtener más información, consulte Copiar eventos de registro de seguimiento en un almacén de datos de eventos.
14. Deje la configuración predeterminada en Activar para todas las cuentas de mi organización. No podrá cambiar esta opción a menos que tenga cuentas configuradas en AWS Organizations.
15. En Configuración adicional, deje las selecciones predeterminadas. De forma predeterminada, un banco de datos de eventos recopila los eventos de todos Regiones de AWS y comienza a incorporarlos cuando se crea.
16. En Eventos de administración, elija recopilar los eventos de lectura y escritura. Deje vacías las casillas Excluir AWS KMS eventos y Excluir eventos de la API de datos de Amazon RDS para recopilar todos los eventos de administración. Deje vacía la casilla de verificación Habilitar eventos de Insights.



17. Elija Next (Siguiente) para revisar las opciones seleccionadas.
18. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).
19. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

    A partir de este momento, el almacén de datos de eventos captura los eventos que coinciden con sus selectores de eventos avanzados. Los eventos que ocurrieron antes de que creara el almacén de datos de eventos no estarán en el almacén de datos de eventos, a menos que opte por copiar los eventos de registro de seguimiento existentes.



Ahora puede ejecutar consultas en su almacén de datos de eventos. Para obtener más información acerca de cómo ver y ejecutar consultas de ejemplo, consulte Tutorial: Ver y ejecutar consultas de ejemplo.

Tutorial: Creación de un almacén de datos de eventos para eventos de datos de S3

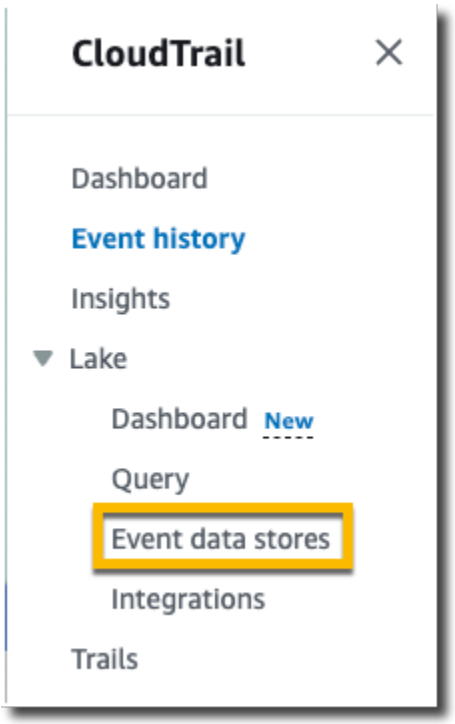
Al crear un banco de datos de eventos para eventos de datos, elige los Servicios de AWS tipos de recursos para los que quiere registrar los eventos de datos. Para obtener información sobre Servicios de AWS los eventos de datos de registro, consulteEventos de datos.

En este tutorial se muestra cómo crear un almacén de datos de eventos para los eventos de datos de Amazon S3. En este tutorial, en lugar de registrar todos los eventos de datos de Amazon S3, seleccionaremos una plantilla de selector de registros personalizada para registrar los eventos solo cuando se elimine un objeto de un bucket de S3 específico.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Para crear un almacén de datos de eventos para eventos de datos de S3

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.



3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configurar el almacén de datos de eventos, en Detalles generales, asigne un nombre al almacén de datos de eventos, como `s3- data-events-eds`. Como práctica recomendada, utilice un nombre que identifique rápidamente el propósito del almacén de datos de eventos. Para obtener información sobre los requisitos de CloudTrail nomenclatura, consulteRequisitos de nomenclatura.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

   - Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
     - Periodo de retención predeterminado: 366 días.

- Periodo máximo de retención: 3653 días.

- Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
  - Periodo de retención predeterminado: 2557 días.
  - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

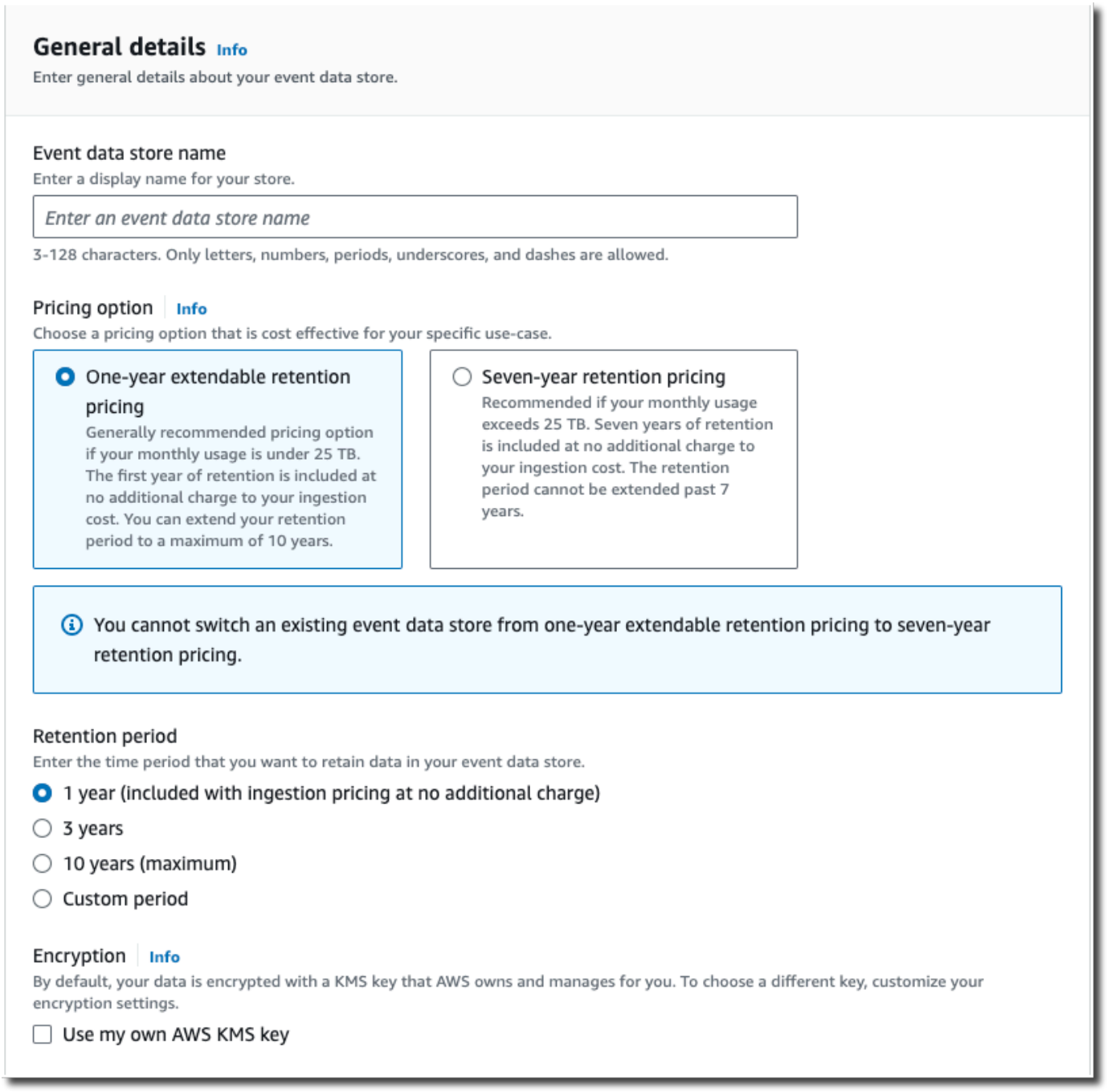
   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

7. (Opcional) En Cifrado, seleccione si quiere cifrar el almacén de datos de eventos con su propia clave de KMS. De forma predeterminada, todos los eventos de un almacén de datos de eventos se cifran CloudTrail mediante una clave de KMS que le AWS pertenece y administra por usted.

   Para habilitar el cifrado con su propia clave de KMS, seleccione Usar mi propia AWS KMS key. Elija Nuevo para que se AWS KMS key cree una por usted, o bien elija Existente para usar una clave de KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

> **Note**
>
> Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.



8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

   Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

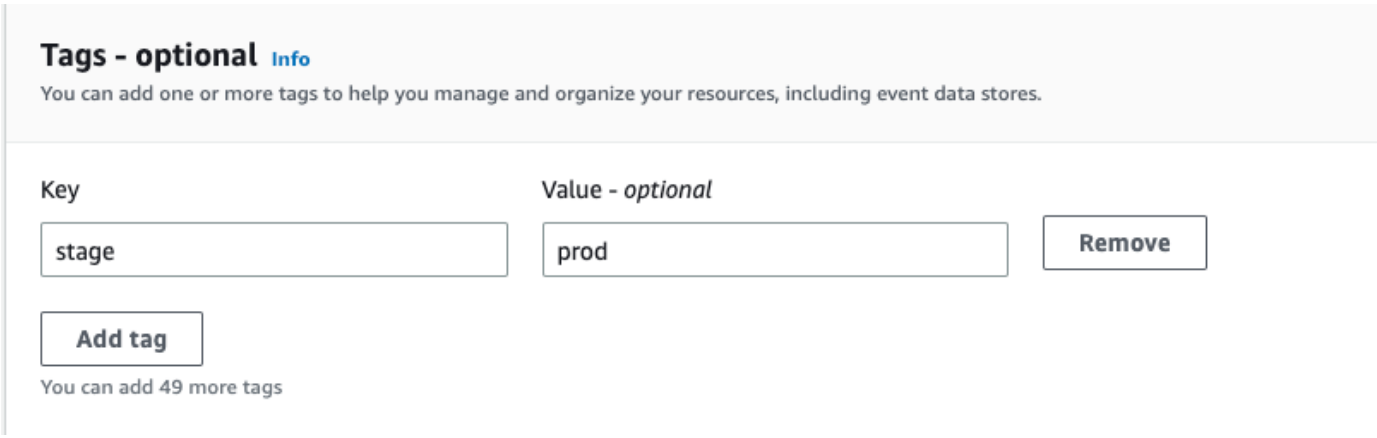
   a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

   b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

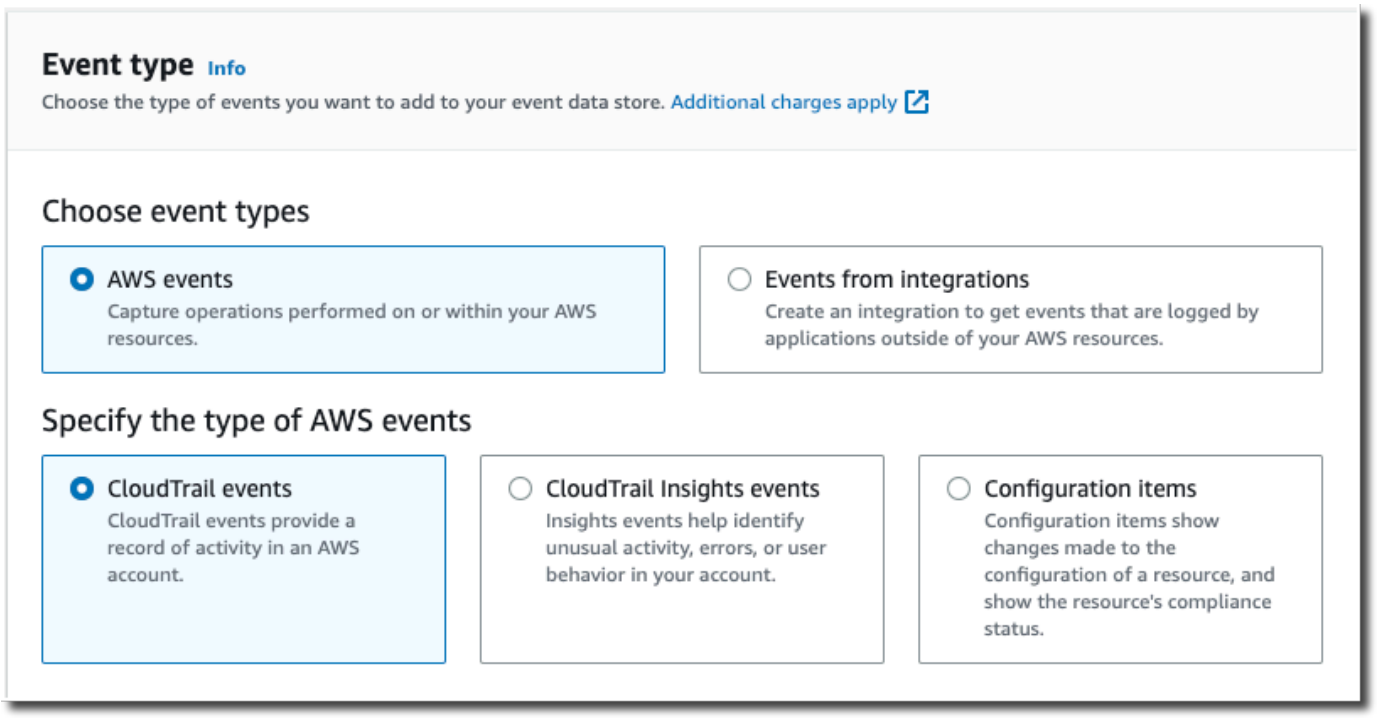
   c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En Etiquetas, agregue una o más etiquetas personalizadas (pares clave-valor) a su almacén de datos de eventos. Las etiquetas pueden ayudarle a identificar los almacenes de datos de sus CloudTrail eventos. Por ejemplo, podría adjuntar una etiqueta con el nombre **`stage`** y el valor **`prod`**. Puede utilizar etiquetas para limitar el acceso al almacén de datos de eventos. También puede utilizar etiquetas para hacer un seguimiento de los costos de consulta e ingesta del almacén de datos de eventos.

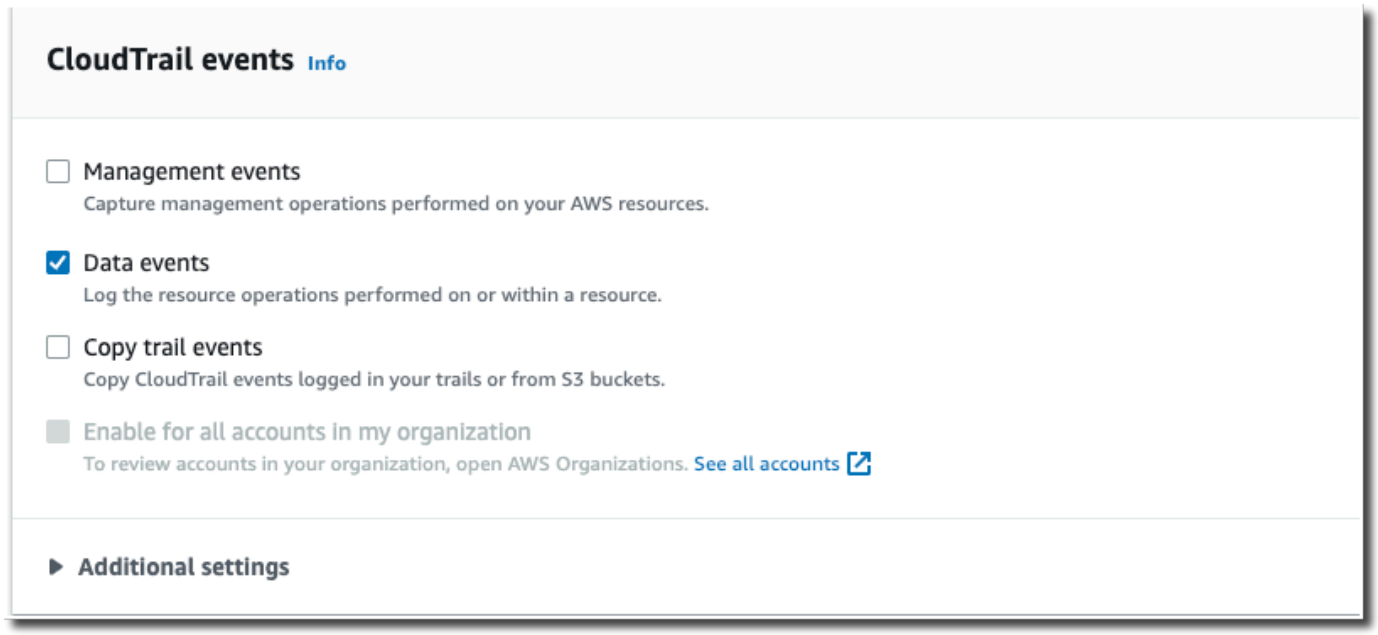
   Para obtener más información acerca de cómo usar etiquetas para hacer un seguimiento de los costos, consulte Creación de etiquetas de asignación de costes definidas por el usuario para los almacenes de datos de eventos de CloudTrail Lake. Para obtener información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener información sobre cómo puede utilizar las etiquetas en AWS, consulte AWS los recursos de etiquetado en. Referencia general de AWS



10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
11. En la página Seleccionar eventos, deje las selecciones predeterminadas en Tipo de evento.



12. Para CloudTrail los eventos, elija Eventos de datos y deseleccione los eventos de administración. Para obtener más información sobre los eventos de datos, consulte Registro de eventos de datos.

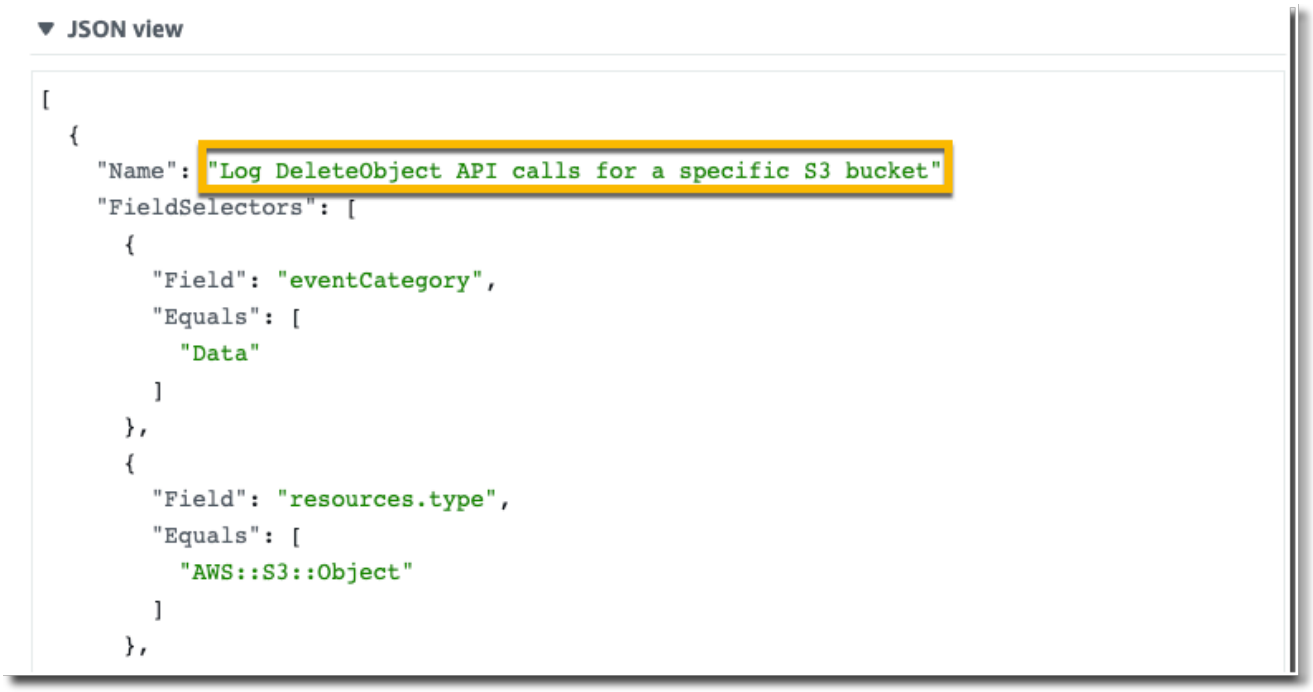


13. Deje la configuración predeterminada para Copiar eventos de los registros de seguimiento. Utilizaría esta opción para copiar los eventos de los registros de seguimiento existentes en el almacén de datos de eventos. Para obtener más información, consulte Copiar eventos de registro de seguimiento en un almacén de datos de eventos.
14. Deje la configuración predeterminada en Activar para todas las cuentas de mi organización. No podrá cambiar esta opción a menos que tenga cuentas configuradas en AWS Organizations.
15. En Configuración adicional, deje las selecciones predeterminadas. De forma predeterminada, un banco de datos de eventos recopila los eventos de todos Regiones de AWS y comienza a ingerirlos cuando se crea.
16. En Eventos de datos, lleve a cabo las siguientes selecciones:

    a. En Tipo de evento de datos, seleccione S3. El tipo de evento de datos identifica el Servicio de AWS recurso en el que se registran los eventos de datos.

    b. En Plantilla de selector de registros, seleccione Personalizado. Si selecciona Personalizado, puede definir un selector de eventos personalizado para filtrar los campos `eventName`, `resources.ARN` y `readOnly`. Para obtener información sobre estos campos, consulte AdvancedFieldSelectorla referencia de la AWS CloudTrail API.

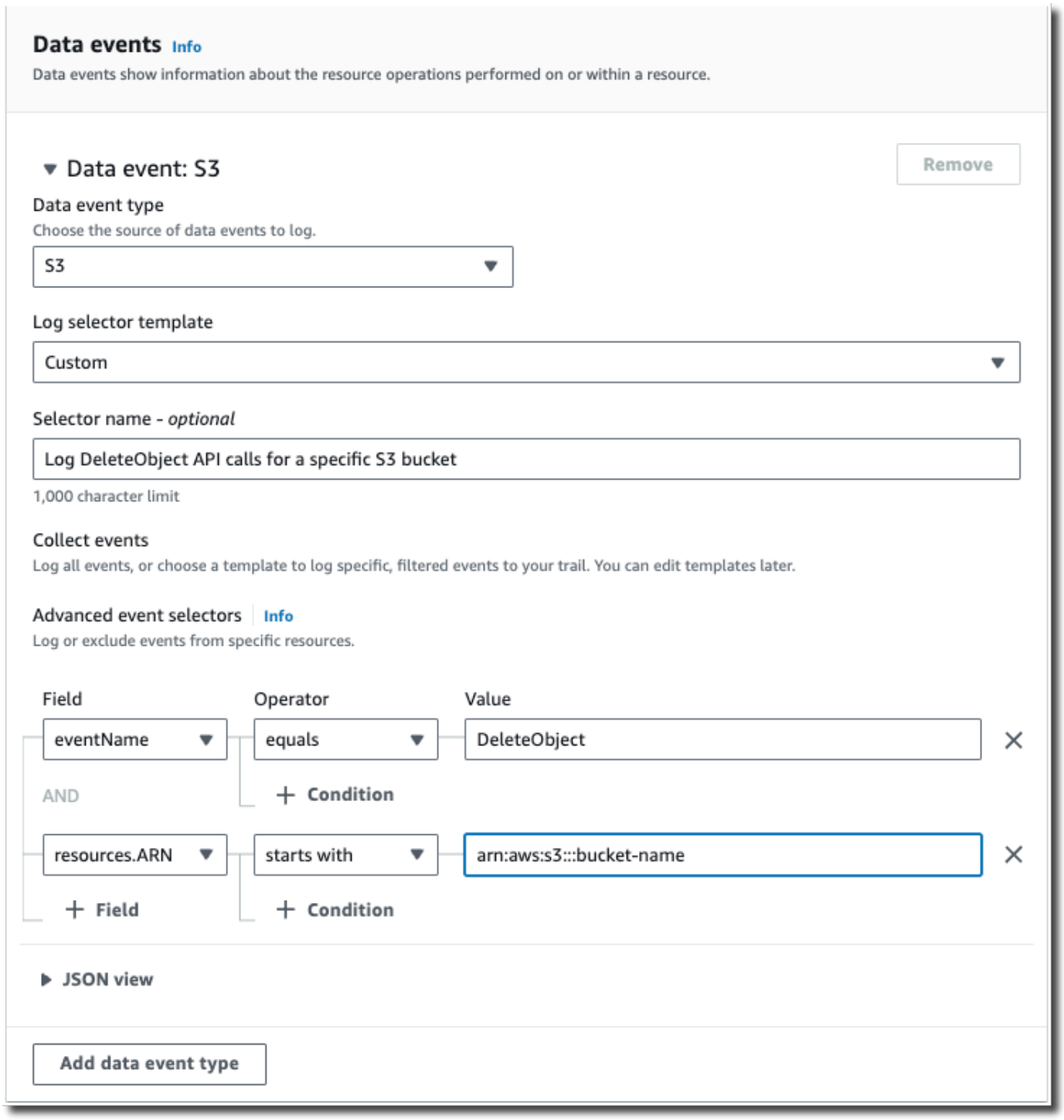
    c. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo para un selector de eventos avanzado, como «Registrar las llamadas a la DeleteObject API para un segmento de S3 específico». El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.



d. En los selectores de eventos avanzados, crearemos un selector de eventos personalizado para filtrar los `resources.ARN` campos `eventName` y. Los selectores de eventos avanzados para un almacén de datos de eventos funcionan igual que los selectores de eventos avanzados que se aplican a un registro de seguimiento. Para obtener más información sobre cómo crear selectores de eventos avanzados, consulte Registrar eventos de datos con selectores de eventos avanzados.

   i. En Campo, seleccione eventName. En Operador, seleccione equals. En Valor, introduzca **`DeleteObject`**. Selecciona + Campo para filtrar por otro campo.

   ii. En Campo, seleccione resources.ARN. En Operador, elija StartsWith. En Valor, introduzca el ARN de su bucket (por ejemplo, *`arn:aws:s3:::bucket-name`*). Para obtener información acerca de cómo obtener el ARN, consulte Recursos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.



17. Elija Next (Siguiente) para revisar las opciones seleccionadas.
18. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).

19. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

    A partir de este momento, el almacén de datos de eventos captura los eventos que coinciden con sus selectores de eventos avanzados. Los eventos que ocurrieron antes de que creara el almacén de datos de eventos no estarán en el almacén de datos de eventos, a menos que opte por copiar los eventos de registro de seguimiento existentes.

Ahora puede ejecutar consultas en su almacén de datos de eventos. Para obtener más información acerca de cómo ver y ejecutar consultas de ejemplo, consulte Tutorial: Ver y ejecutar consultas de ejemplo.

Tutorial: Copia los eventos del sendero a CloudTrail Lake

Este tutorial le muestra cómo copiar los eventos de los senderos a un nuevo banco de datos de eventos de CloudTrail Lake para su análisis histórico. Para obtener más información acerca de cómo copiar eventos de registros de seguimiento, consulte Copiar eventos de registro de seguimiento en un almacén de datos de eventos.

CloudTrail Los almacenes de datos de eventos lacustres conllevan cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Cuando copias los eventos de los senderos a un banco de datos de eventos de CloudTrail Lake, incurres en cargos en función de la cantidad de datos sin comprimir que ingiera el almacén de datos de eventos.

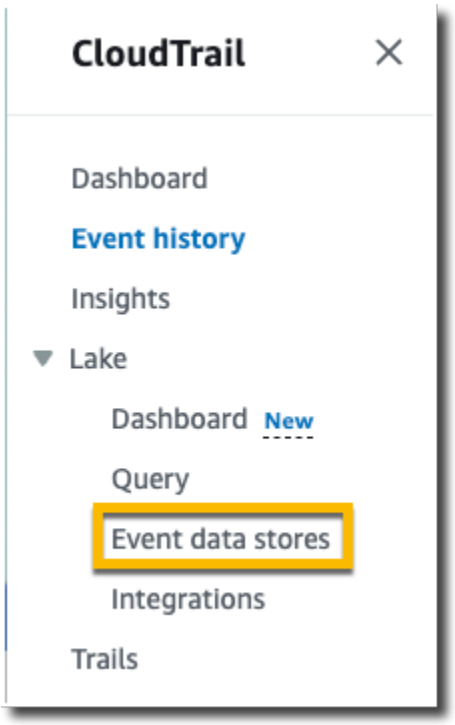
Al copiar los eventos de los senderos en CloudTrail Lake, se CloudTrail descomprimen los registros almacenados en formato gzip (comprimido) y, a continuación, se copian los eventos contenidos en los registros en el almacén de datos de eventos. El tamaño de los datos sin comprimir podría ser mayor que el tamaño real del almacenamiento de S3. Para obtener una estimación general del tamaño de los datos sin comprimir, puede multiplicar por 10 el tamaño de los registros del bucket de S3.

Puede reducir los costos especificando un intervalo de tiempo más reducido para los eventos copiados. Si planea usar solo el almacén de datos de eventos para consultar los eventos copiados,

puede desactivar la ingesta de eventos para evitar generar cargos por eventos futuros. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

Para copiar eventos de registros de seguimiento en un almacén de datos de eventos nuevo

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.



3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configurar el almacén de datos de eventos, en Detalles generales, asigne un nombre al almacén de datos de eventos, por ejemplo `my-management-events-eds`. Como práctica recomendada, utilice un nombre que identifique rápidamente el propósito del almacén de datos de eventos. Para obtener información sobre los requisitos de CloudTrail nomenclatura, consulteRequisitos de nomenclatura.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

- Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
  - Periodo de retención predeterminado: 366 días.
  - Periodo máximo de retención: 3653 días.
- Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
  - Periodo de retención predeterminado: 2557 días.
  - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

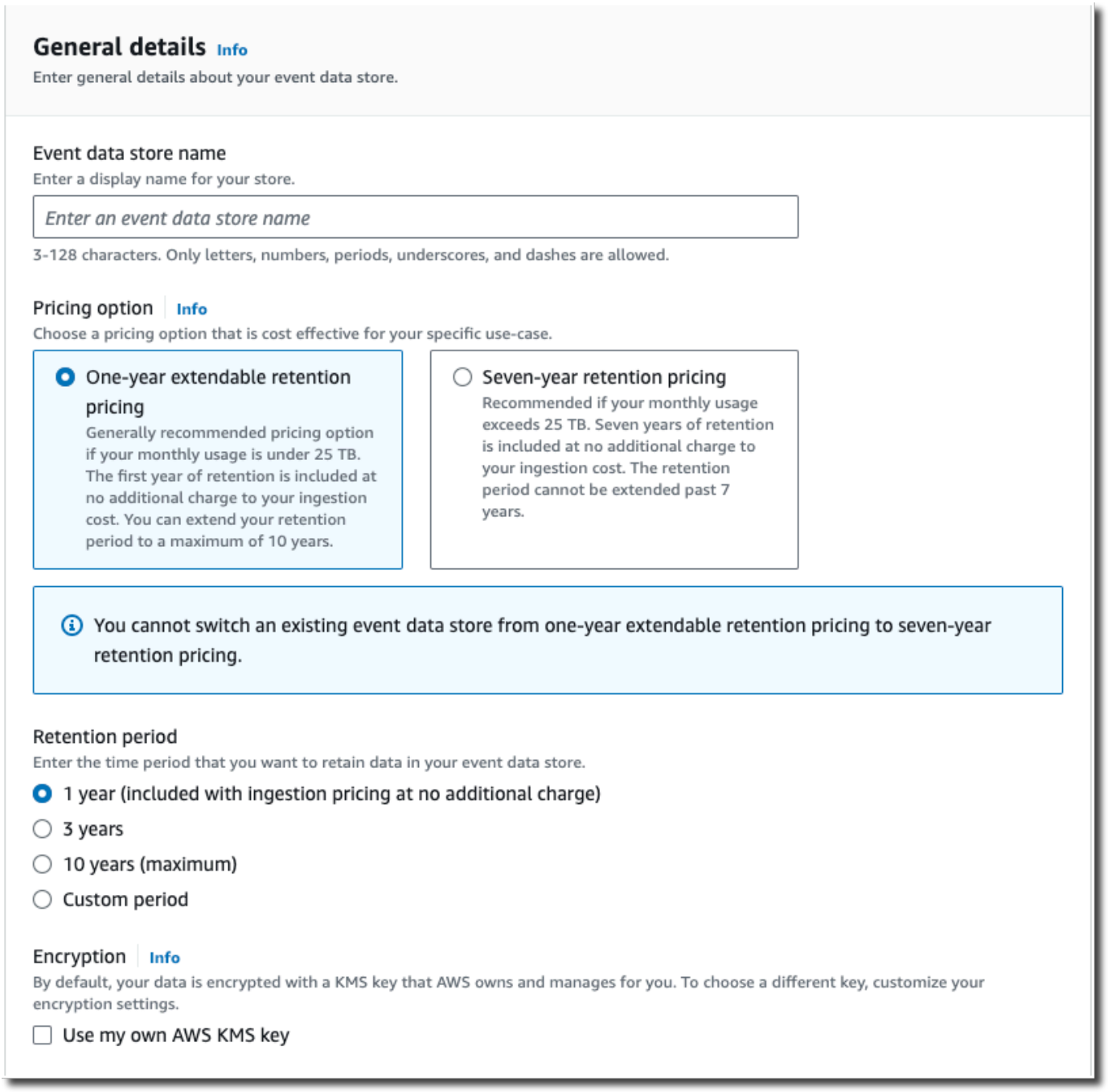
   > **Note**
   >
   > CloudTrail no copiará un evento si `eventTime` es anterior al período de retención especificado.
   > Le recomendamos que, al elegir un periodo de retención, tenga en cuenta tanto la antigüedad de los eventos que desea copiar como el tiempo que desea conservar los eventos copiados en su almacén de datos de eventos. Por ejemplo, si copia los eventos de registros de seguimiento que tienen 5 años y especifica un periodo de retención de 7 años, el almacén de datos de eventos retendrá esos eventos durante dos años.

7. (Opcional) En Cifrado, seleccione si quiere cifrar el almacén de datos de eventos con su propia clave de KMS. De forma predeterminada, todos los eventos de un almacén de datos de eventos se cifran CloudTrail mediante una clave de KMS que le AWS pertenece y administra por usted.

   Para habilitar el cifrado con su propia clave de KMS, seleccione Usar mi propia AWS KMS key. Elija Nuevo para que se AWS KMS key cree una por usted, o bien elija Existente para usar una clave de KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

   > **Note**
   >
   > Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.



8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar,

leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

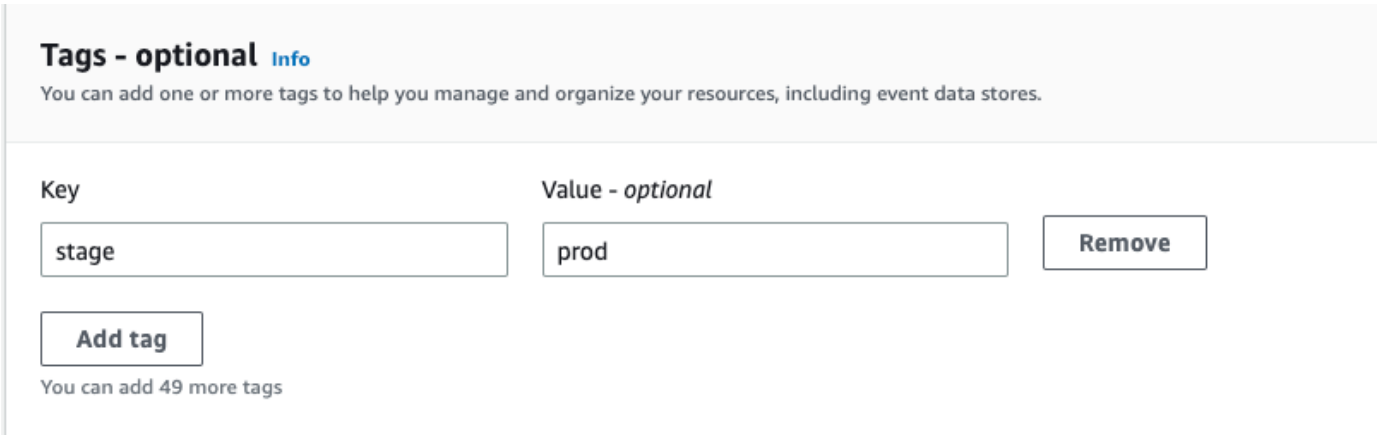
a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

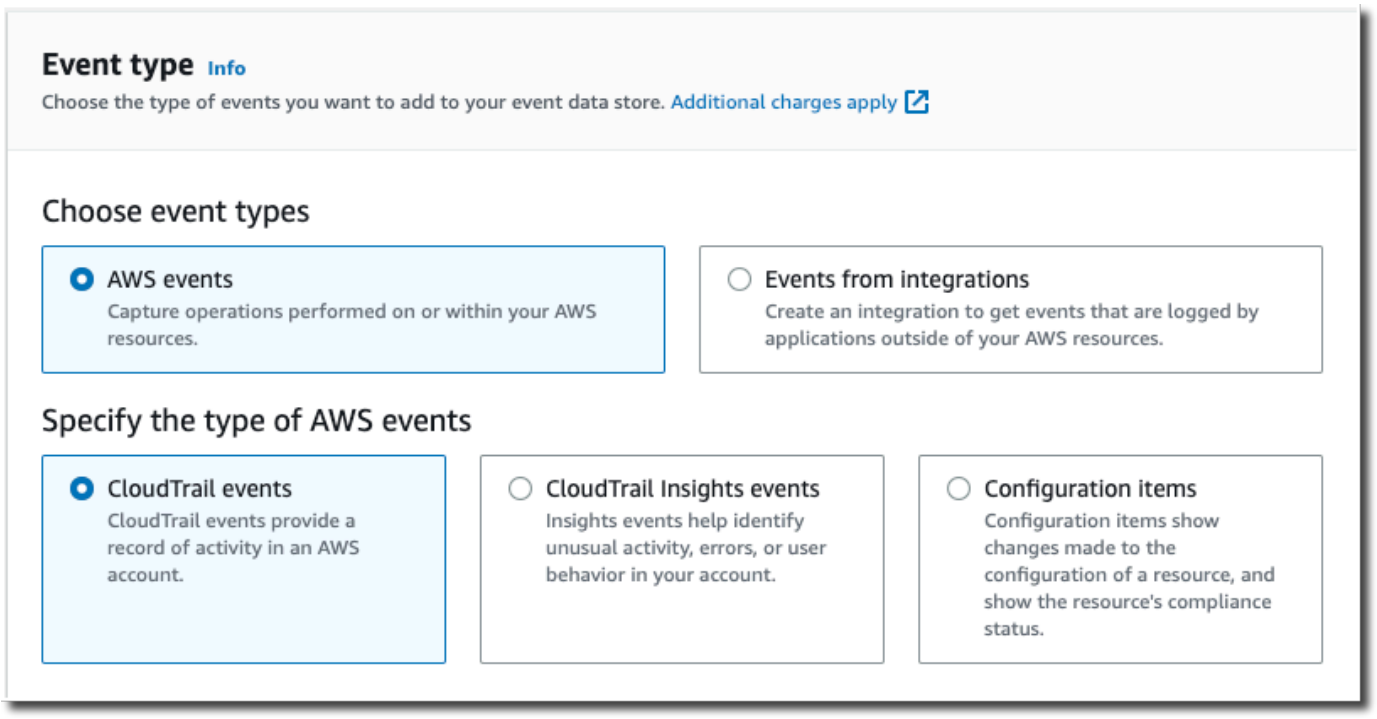
c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En Etiquetas, agregue una o más etiquetas personalizadas (pares clave-valor) a su almacén de datos de eventos. Las etiquetas pueden ayudarle a identificar los almacenes de datos de sus CloudTrail eventos. Por ejemplo, podría adjuntar una etiqueta con el nombre **`stage`** y el valor **`prod`**. Puede utilizar etiquetas para limitar el acceso al almacén de datos de eventos. También puede utilizar etiquetas para hacer un seguimiento de los costos de consulta e ingesta del almacén de datos de eventos.

   Para obtener más información acerca de cómo usar etiquetas para hacer un seguimiento de los costos, consulte Creación de etiquetas de asignación de costes definidas por el usuario para los almacenes de datos de eventos de CloudTrail Lake. Para obtener información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener información sobre cómo puede utilizar las etiquetas en AWS, consulte AWS los recursos de etiquetado en. Referencia general de AWS

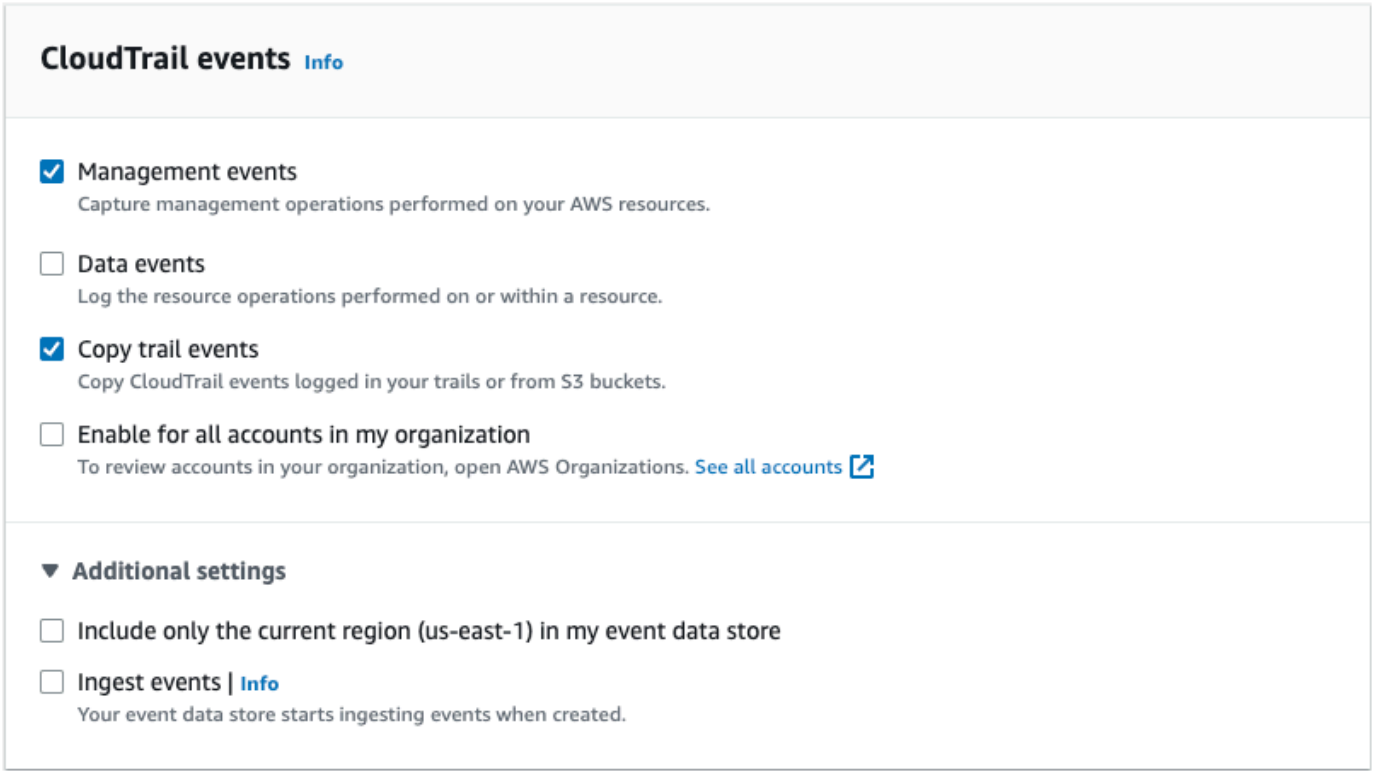


10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
11. En la página Seleccionar eventos, deje las selecciones predeterminadas en Tipo de evento.



12. En el CloudTrail caso de los eventos, dejaremos seleccionada la opción Gestión de eventos y seleccionaremos Copiar eventos de seguimiento. En este ejemplo, no nos preocupan los tipos de eventos porque solo utilizamos el almacén de datos de eventos para analizar eventos pasados y no ingerimos eventos futuros.

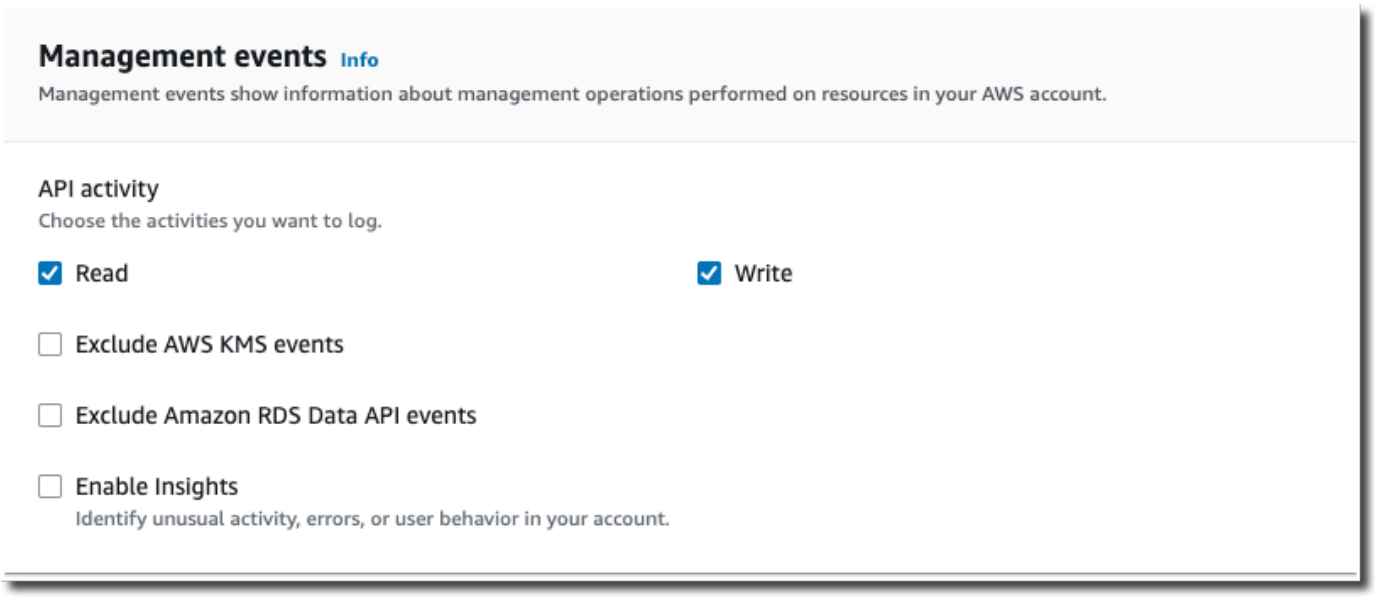
    Si va a crear un almacén de datos de eventos para reemplazar un registro de seguimiento existente, seleccione los mismos selectores de eventos que el registro de seguimiento para asegurarse de que el almacén de datos de eventos tenga la misma cobertura de eventos.



13. Seleccione Activar para todas las cuentas de mi organización si se trata de un almacén de datos de eventos de la organización. No podrá cambiar esta opción a menos que tenga cuentas configuradas en AWS Organizations.

> **Note**
>
> Si va a crear un almacén de datos de eventos de la organización, debe iniciar sesión con la cuenta de administración de la organización, ya que solo la cuenta de administración puede copiar los eventos de registros de seguimiento en un almacén de datos de eventos de la organización.

14. En Configuración adicional, desmarcaremos Ingerir eventos, ya que en este ejemplo no queremos que el almacén de datos de eventos ingiera ningún evento futuro, ya que solo nos interesa consultar los eventos copiados. De forma predeterminada, un almacén de datos de eventos recopila los eventos de todos Regiones de AWS y comienza a incorporarlos cuando se crea.
15. En Eventos de administración, dejaremos la configuración predeterminada.



16. En el área Copiar eventos de registros de seguimiento, complete los siguientes pasos.

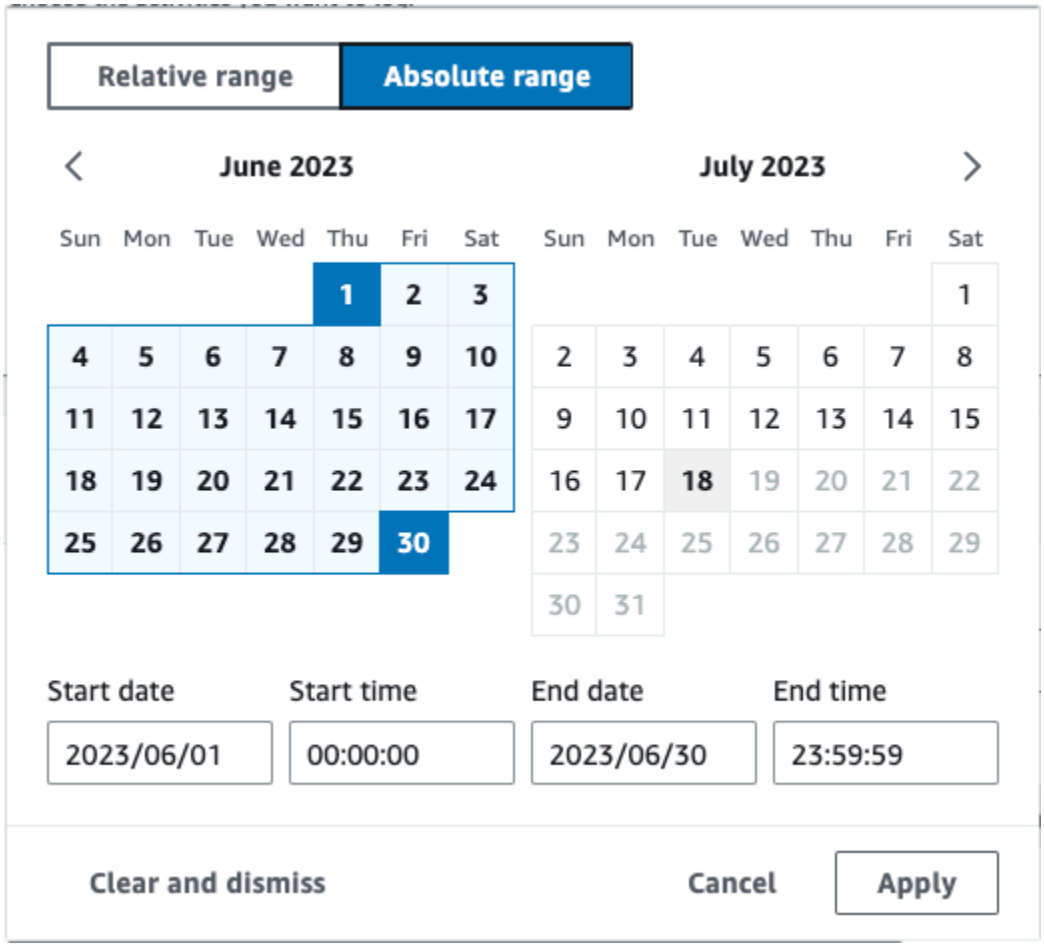
    a. Elija el registro de seguimiento que desea copiar. En este ejemplo, seleccionaremos un registro de seguimiento llamado *`management-events`*.

       De forma predeterminada, CloudTrail solo copia CloudTrail los eventos contenidos en el `CloudTrail` prefijo del bucket de S3 y los prefijos incluidos en el `CloudTrail` prefijo, y no comprueba los prefijos de otros servicios. AWS Si desea copiar CloudTrail los eventos contenidos en otro prefijo, seleccione Introducir el URI de S3 y, a continuación, elija Examinar S3 para buscar el prefijo. Si el depósito de S3 de origen de la ruta utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS CloudTrail permita descifrar los datos. Si el bucket de S3 de origen utiliza varias claves KMS, debe actualizar la política de cada clave CloudTrail para poder descifrar los datos del bucket. Para obtener más información sobre la actualización de la política de claves KMS, consulte Política de claves KMS para descifrar datos en el bucket de S3 de origen.

    b. Elige un intervalo de tiempo para copiar los eventos. CloudTrail comprueba el prefijo y el nombre del archivo de registro para comprobar que el nombre contiene una fecha entre la fecha de inicio y la de finalización elegidas antes de intentar copiar los eventos de seguimiento. Puede elegir un intervalo relativo o un intervalo absoluto. Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de tiempo que sea anterior a la creación del almacén de datos de eventos.

- Si selecciona Rango relativo, puede optar por copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un rango personalizado. CloudTrail copia los eventos registrados en el período de tiempo elegido.
- Si elige Rango absoluto, puede elegir una fecha de inicio y finalización específica. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y finalización elegidas.

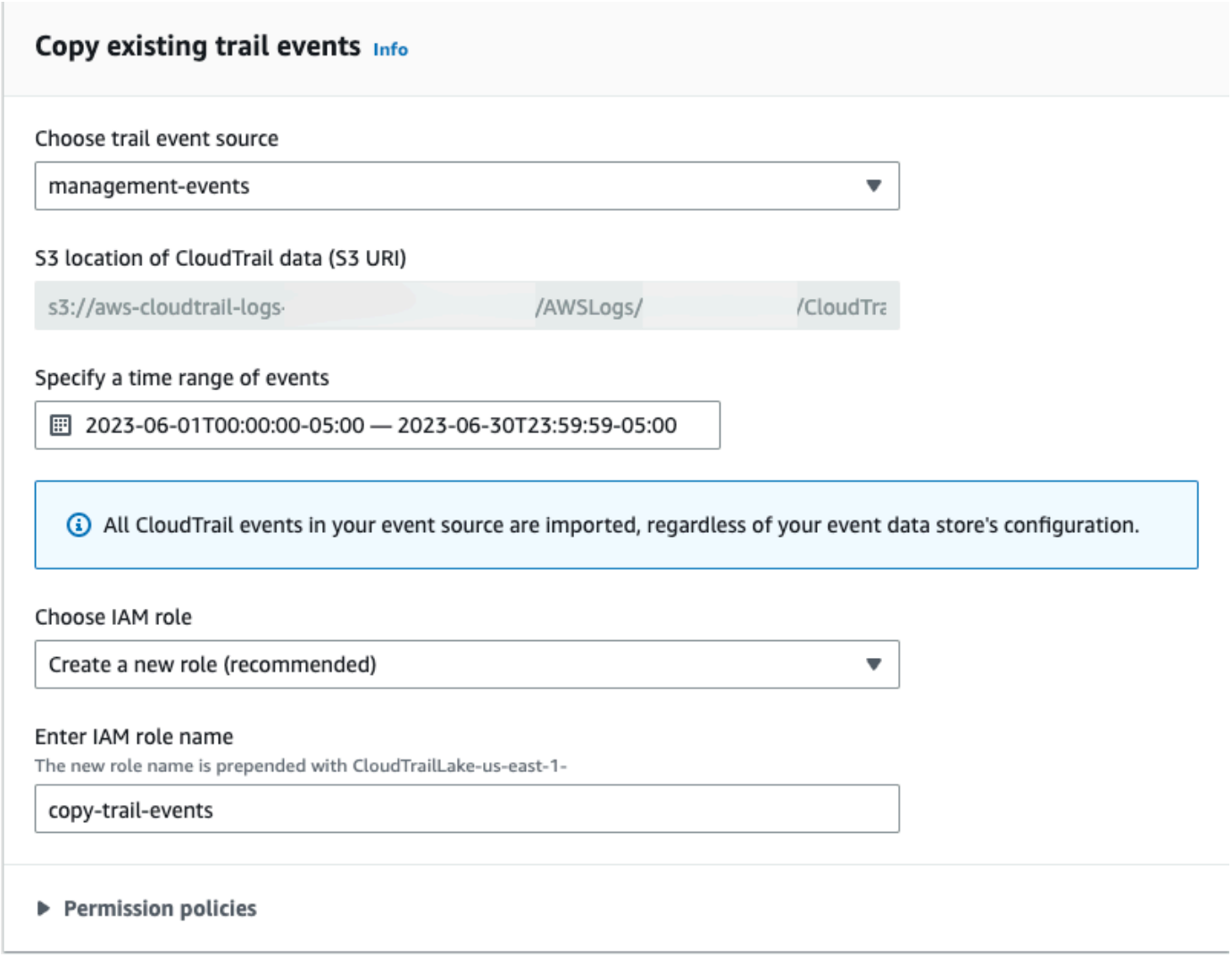
En este ejemplo, seleccionaremos Intervalo absoluto y seleccionaremos todo el mes de junio.



c. Para Permissions (Permisos), elija una de las siguientes opciones de rol de IAM. Si elige un rol de IAM existente, verifique que la política de roles de IAM proporcione los permisos necesarios. Para obtener más información acerca de la actualización de los permisos de rol de IAM, consulte Permisos de IAM para copiar eventos de registro de seguimiento.

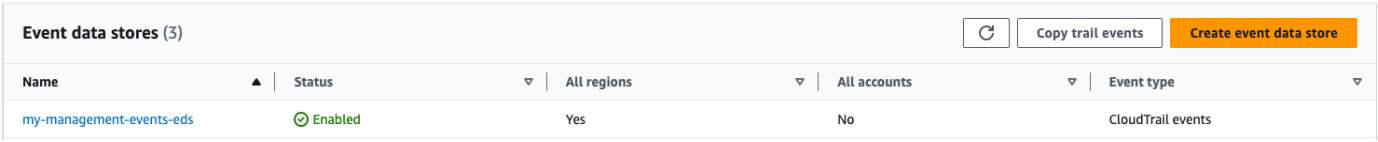
- Elija Create a new role (recommended) (Crear un nuevo rol [recomendado]) para crear un nuevo rol de IAM. En Introducir el nombre del rol de IAM, introduzca un nombre para el rol. CloudTrail crea automáticamente los permisos necesarios para este nuevo rol.
- Elija Usar un ARN de rol de IAM personalizado para usar un rol de IAM personalizado que no aparezca en la lista. En Enter IAM role ARN (Ingresar ARN del rol de IAM), escriba el ARN de IAM.
- Elija un rol de IAM existente de la lista desplegable.

En este ejemplo, seleccionaremos Crear un nuevo rol (recomendado) y proporcionaremos el nombre **`copy-trail-events`**.



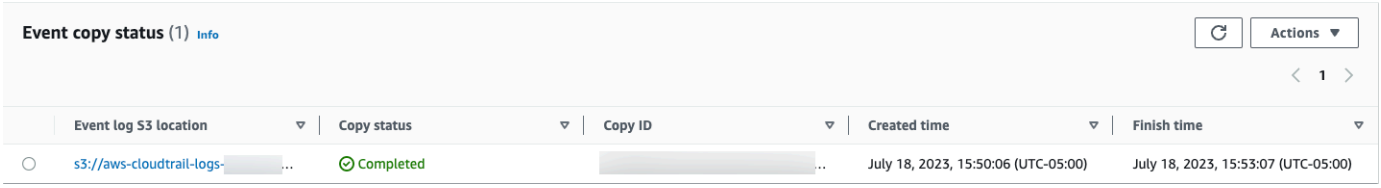
17. Elija Next (Siguiente) para revisar las opciones seleccionadas.

18. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).
19. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

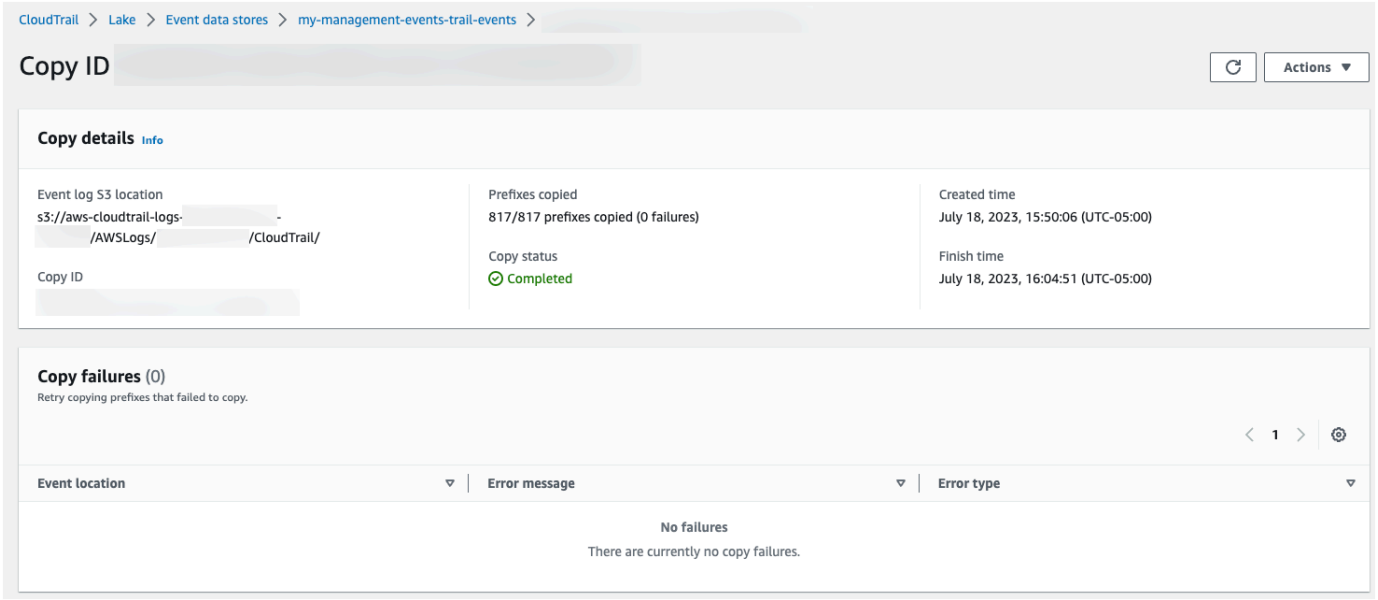


20. Seleccione el nombre del almacén de datos de eventos para ver su página de detalles. En la página de detalles, se muestran los detalles del almacén de datos de eventos y el estado de la copia. El estado de la copia de eventos se muestra en el área Estado de la copia de eventos.

    Cuando se completa la copia de un evento de registro de seguimiento, el campo Copy status (Estado de la copia) se establece en Completed (Completa), si no hubo errores, o Failed (Error), si hubo errores.



21. Para ver más detalles sobre la copia, seleccione el nombre de la copia en la columna Ubicación de S3 del registro de eventos o seleccione la opción Ver detalles en el menú Acciones. Para obtener más información sobre cómo ver los detalles de la copia de un evento de registro de seguimiento, consulte Detalles de la copia del evento.



22. En el área Errores de copia, se muestra cualquier error que se haya producido al copiar los eventos del registro de seguimiento. Si Copy status (Estado de la copia) está establecido en Failed (Error), corrija los errores que aparecen en Copy failures (Errores de la copia) y, a continuación, elija Retry copy (Volver a copiar). Al volver a intentar una copia, la CloudTrail reanuda en la ubicación en la que se produjo el error.

Tutorial: Ver los paneles de Lake

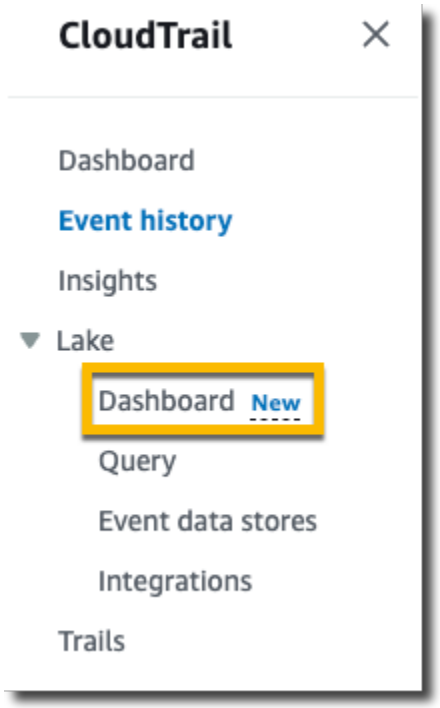
En este tutorial se muestra cómo ver los paneles de Lake. CloudTrail Los paneles de Lake le permiten visualizar los eventos en su almacén de datos de eventos y ver las tendencias, como los principales usuarios y los principales errores.

Cada panel consta de varios widgets y cada widget representa una consulta SQL. Para rellenar el panel, CloudTrail ejecuta consultas generadas por el sistema. Las consultas generan cargos según la cantidad de datos que se analizan.

> **Note**
>
> Actualmente, los paneles solo están disponibles para los almacenes de datos de eventos que recopilan eventos CloudTrail de administración y eventos de datos de Amazon S3.

Para ver los paneles de Lake

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, seleccione Lake y, a continuación, Panel.



3. La primera vez que vea la página de paneles, CloudTrail le pedirá que confirme los costes asociados a la ejecución de consultas. Elija Acepto para reconocer el costo de ejecutar las consultas. Esta es una confirmación única. Para obtener más información sobre CloudTrail los precios, consulte CloudTrailPrecios.
4. Seleccione el almacén de datos de eventos de la lista y, a continuación, seleccione el tipo de panel que desee ver.

   Los tipos de paneles posibles son los siguientes:

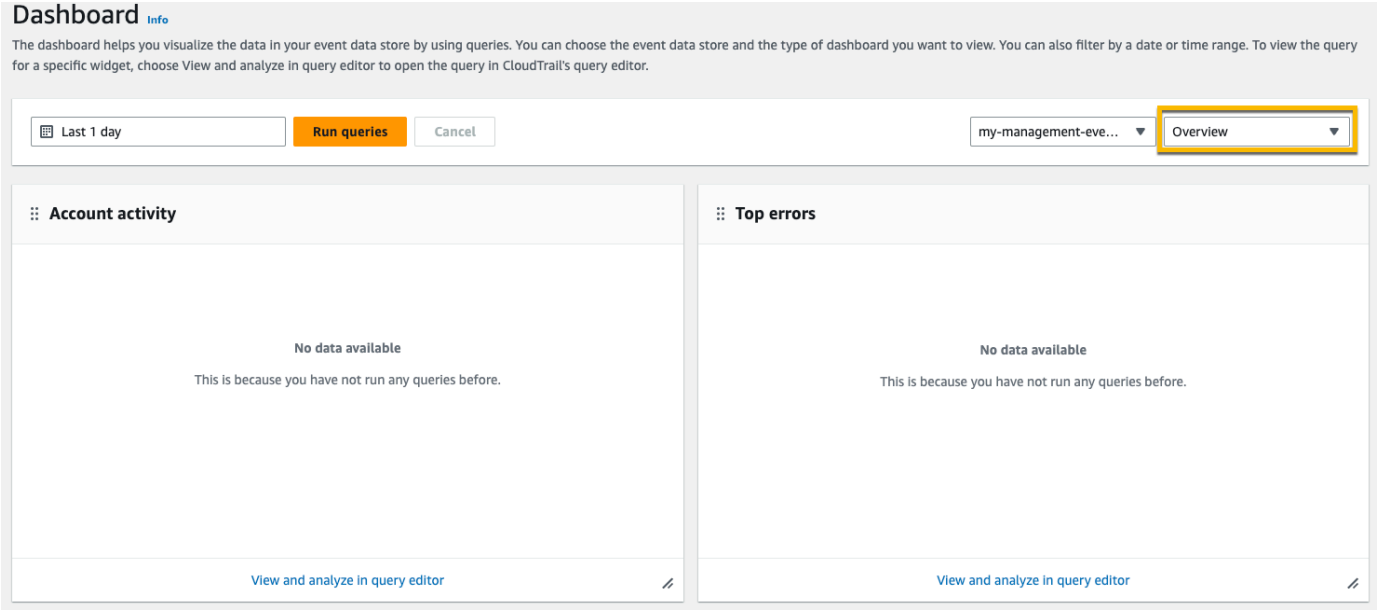
   - Panel de información general: muestra los usuarios más activos y Servicios de AWS por número de eventos. Regiones de AWS También puede ver información sobre la actividad de los eventos de administración de `read` y `write`, los eventos con más limitación y los principales errores. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración.
   - Panel Eventos de administración: muestra los eventos de inicio de sesión en la consola, los eventos de acceso denegado, las acciones destructivas y los principales errores por usuario. También puede ver información sobre las versiones de TLS y las llamadas de TLS obsoletas por usuario. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración.
   - Panel Eventos de datos de S3: muestra la actividad de la cuenta de S3, los objetos de S3 a los que más se ha accedido, los principales usuarios de S3 y las principales acciones de S3.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos de Amazon S3.

- Panel de eventos de Insights: muestra la proporción total de eventos de Insights por tipo de Insights, la proporción de eventos de Insights por tipo de Insights para los principales usuarios y servicios, y el número de eventos de Insights por día. El panel también incluye un widget que muestra hasta 30 días de eventos de Insights. Este panel solo está disponible para los almacenes de datos de eventos que recopilan eventos de Insights.

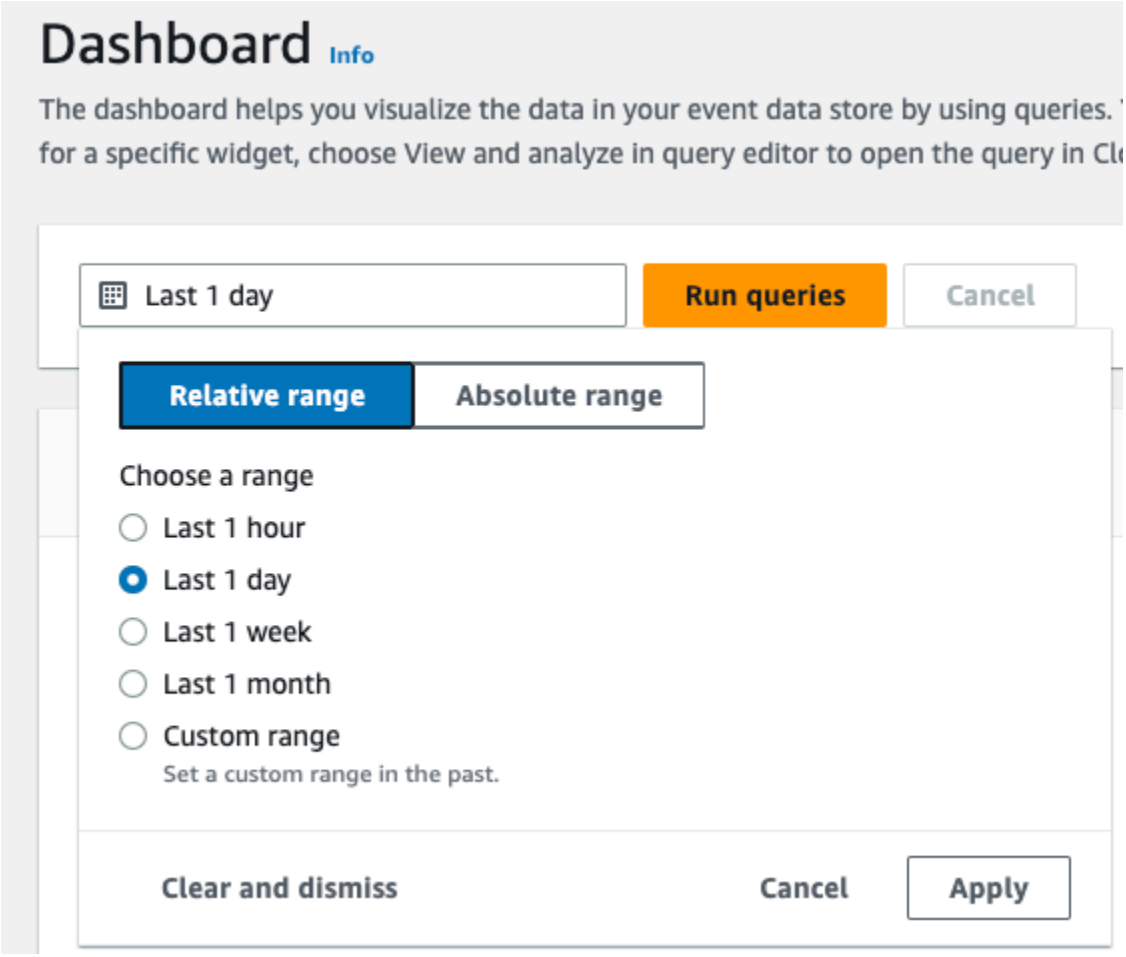
> **Note**
>
> - Tras activar CloudTrail Insights por primera vez en el almacén de datos de eventos de origen, el primer evento de Insights puede tardar hasta 7 días en publicarse si se detecta una actividad inusual. CloudTrail Para obtener más información, consulte Descripción de la entrega de eventos de Insights.
> - El panel Eventos de Insights solo muestra información sobre los eventos de Insights recopilados por el almacén de datos de eventos seleccionado, que viene determinada por la configuración del almacén de datos de eventos de origen. Por ejemplo, si configura el almacén de datos de eventos de origen para habilitar los eventos de Insights en `ApiCallRateInsight`, pero no en `ApiErrorRateInsight`, no verá la información sobre los eventos de Insights en `ApiErrorRateInsight`.

En este ejemplo, hemos seleccionado el panel Información general.



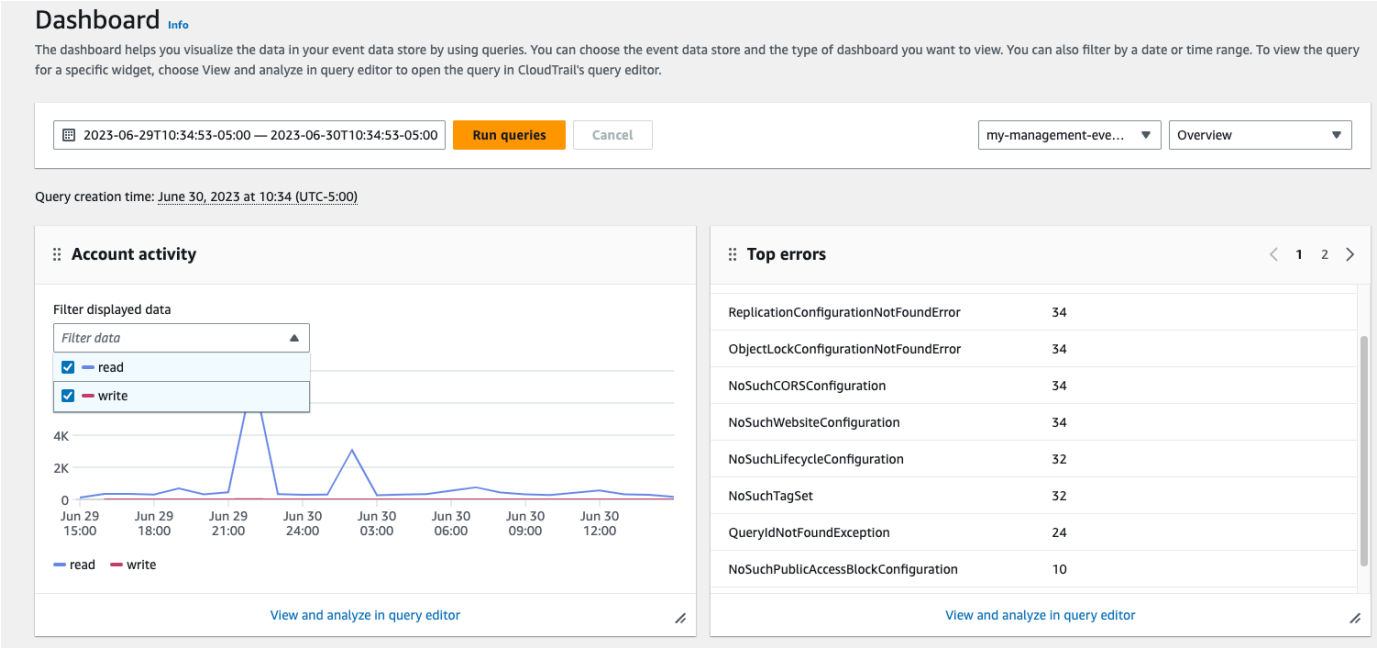
5. Seleccione el campo de fecha para filtrar por un intervalo de tiempo y, a continuación, seleccione Aplicar. Elija Intervalo absoluto para seleccionar un intervalo de fechas y horas específico. Elija Intervalo relativo para seleccionar un intervalo de tiempo predefinido o personalizado. De forma predeterminada, el panel muestra los datos de eventos de las últimas 24 horas.

> **Note**
>
> Como CloudTrail las consultas se cobran en función de la cantidad de datos escaneados, puede reducir los costes filtrando en un intervalo de tiempo más reducido.

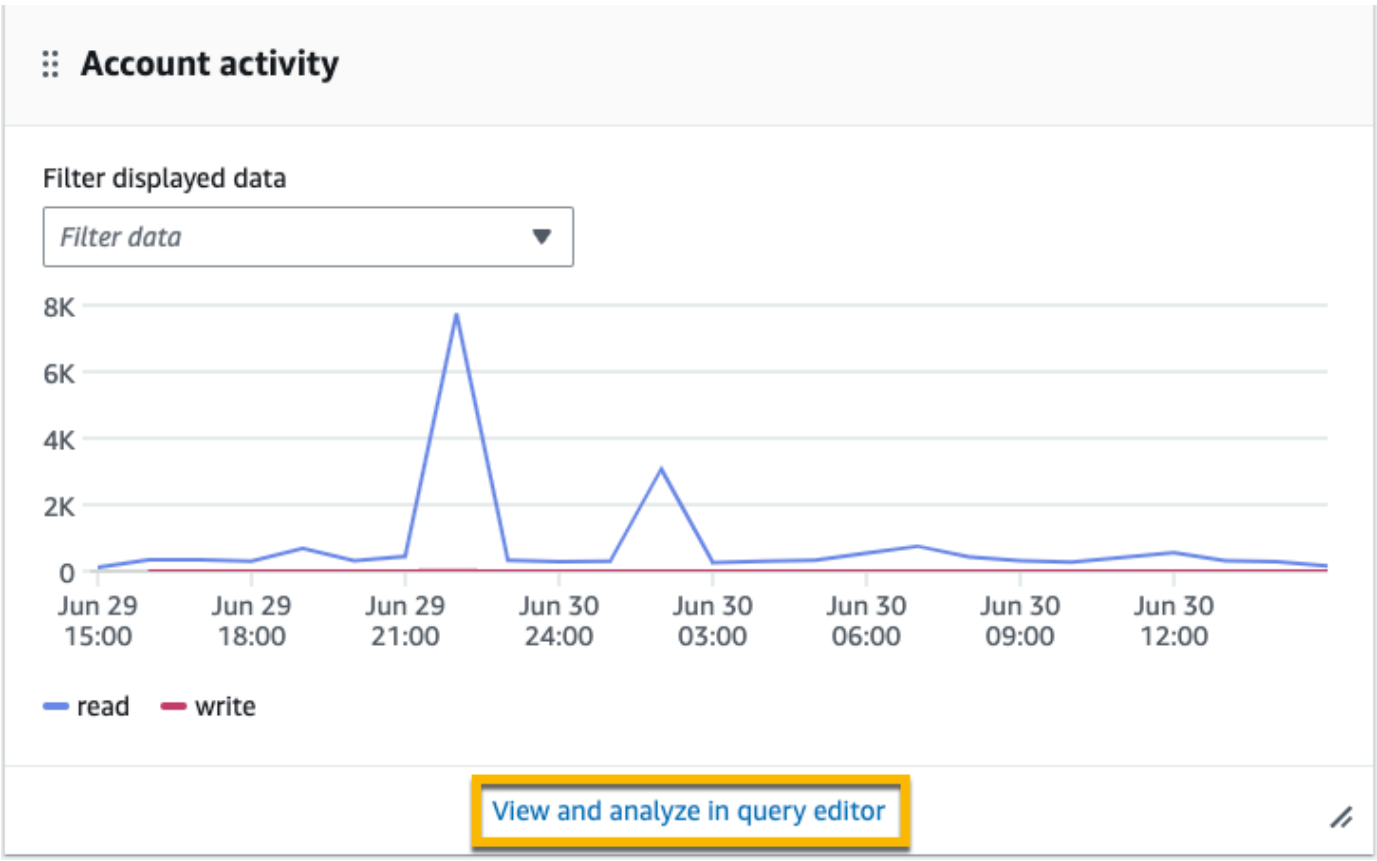


6. Seleccione Ejecutar consultas para rellenar el panel. En cada widget se muestra el estado de la consulta asociada y se presentan los datos cuando se completa la consulta.

   Puede llevar a cabo un filtrado adicional en algunos widgets, como Actividad de la cuenta, que le permite filtrar por la actividad de los eventos de `read` y `write`.

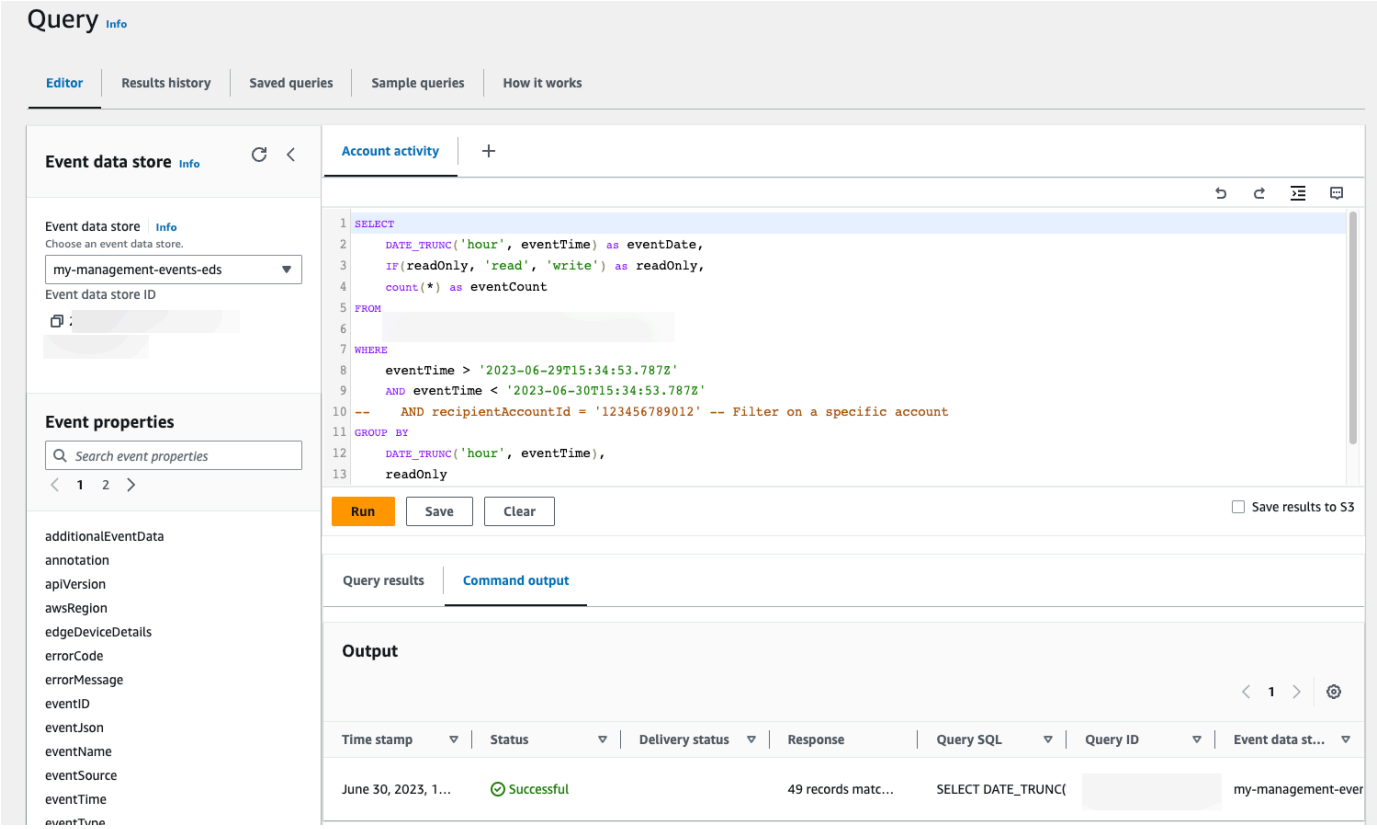


7. Para ver la consulta de un widget, seleccione Ver y analizar en el editor de consultas.



Si selecciona Ver y analizar en el editor de consultas, se abre la consulta en el editor de consultas de CloudTrail Lake, lo que le permite analizar más a fondo los resultados de la

consulta fuera del panel de control. Para obtener más información sobre la edición de una consulta, consulte Creación o edición de una consulta. Para obtener más información sobre cómo ejecutar una consulta y guardar los resultados, consulte Ejecutar una consulta y guardar los resultados de la consulta.



Para obtener más información acerca de los paneles, consulte Ver los paneles de Lake.

Tutorial: Ver y ejecutar consultas de ejemplo

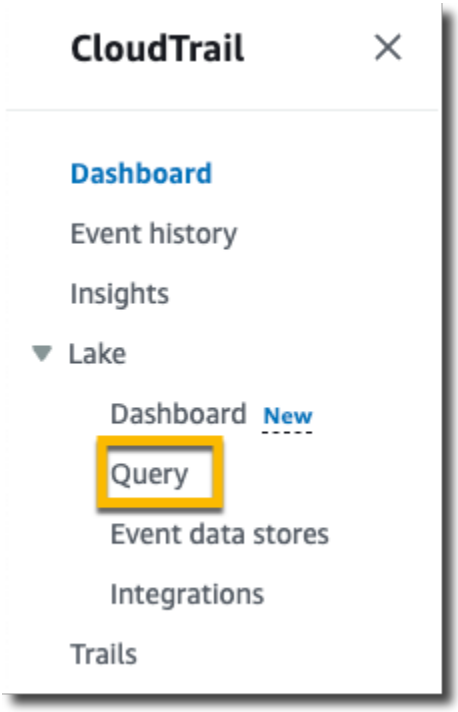
CloudTrail Lake proporciona una serie de ejemplos de consultas que pueden ayudarle a empezar a escribir sus propias consultas. En este tutorial se muestra cómo seleccionar y ejecutar una consulta de ejemplo.

Las consultas de CloudTrail Lake se crean en SQL. Puede crear una consulta en la pestaña CloudTrail Lake Editor escribiéndola en SQL desde cero o abriendo una consulta guardada o de muestra y editándola. No puede sobrescribir una consulta de muestra ya incluida con sus cambios, pero puede guardarla como una nueva consulta. Para obtener más información acerca del lenguaje de consulta SQL permitido, consulte CloudTrail Restricciones de Lake SQL.

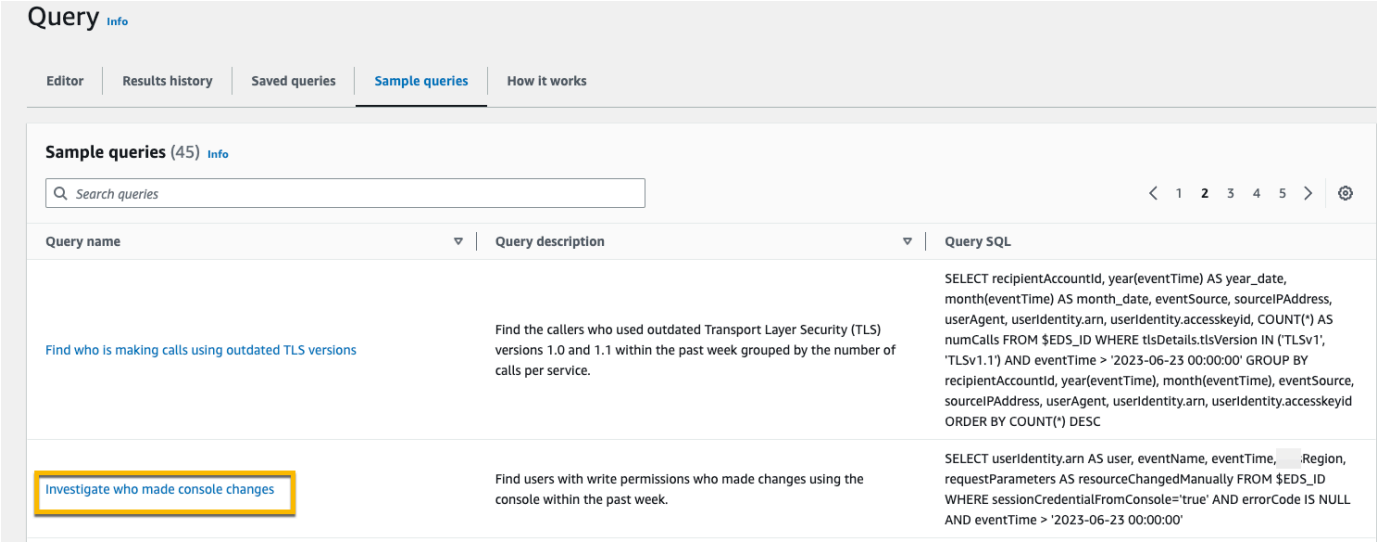
CloudTrail las consultas incurren en cargos en función de la cantidad de datos escaneados. Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales `eventTime` de inicio y finalización a las consultas. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Para ver y ejecutar una consulta de muestra

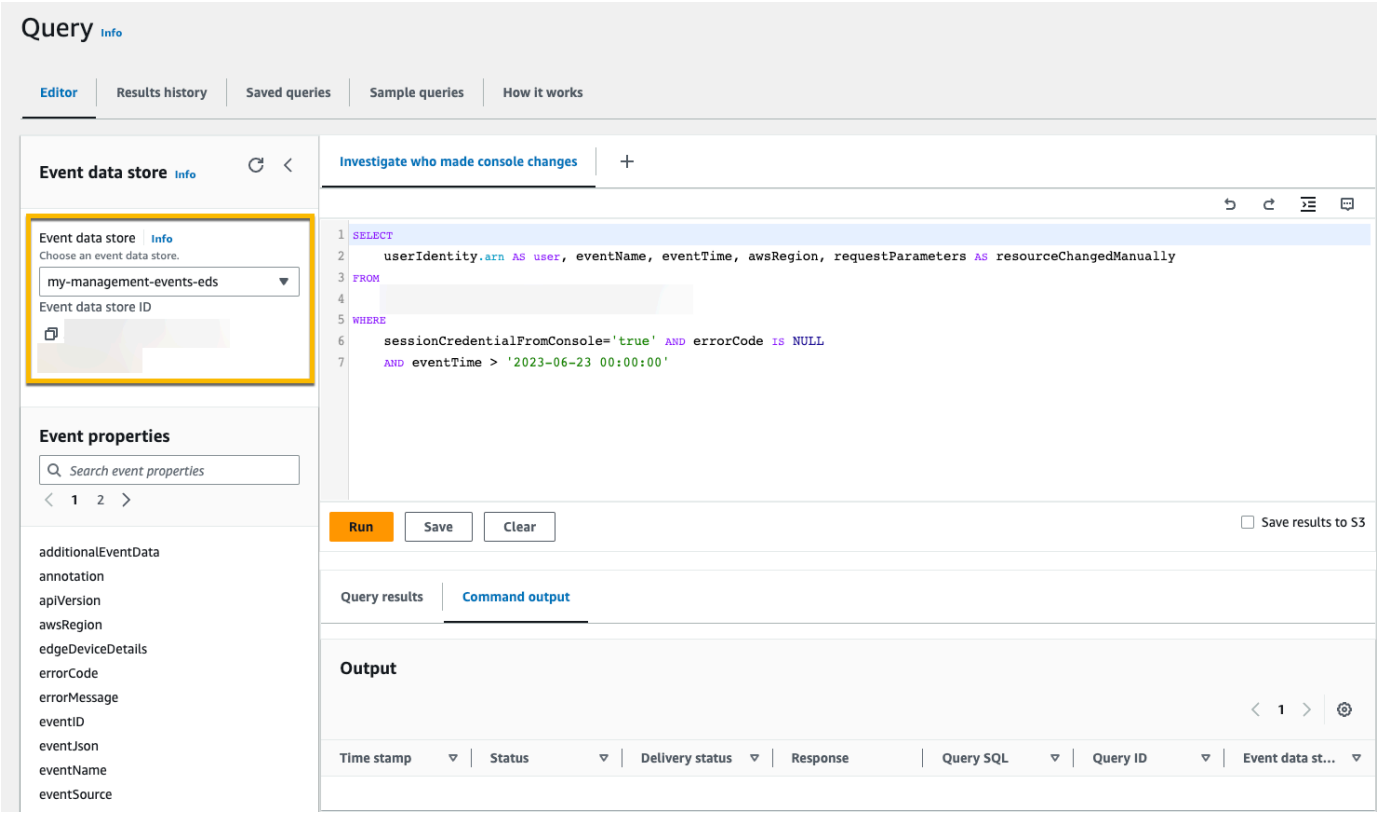
1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Consulta.



3. En la página Query (Consultas), elija la pestaña Sample queries (Consultas de ejemplo).
4. Seleccione un ejemplo de consulta de la lista o busque la consulta para filtrar la lista. En este ejemplo, abriremos la consulta Investigar quién realizó los cambios en la consola eligiendo el nombre de la consulta. Esto abre la consulta en la pestaña Editor.

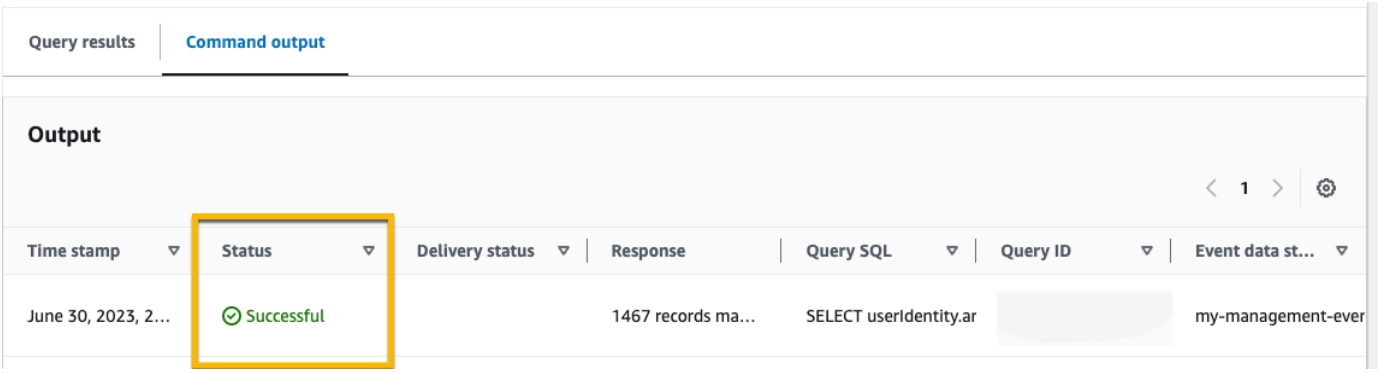


5. En la pestaña Editor, seleccione el almacén de datos de eventos para el que desee ejecutar la consulta. Al elegir el banco de datos de eventos de la lista, rellena CloudTrail automáticamente el ID del banco de datos de eventos en la `FROM` línea del editor de consultas.

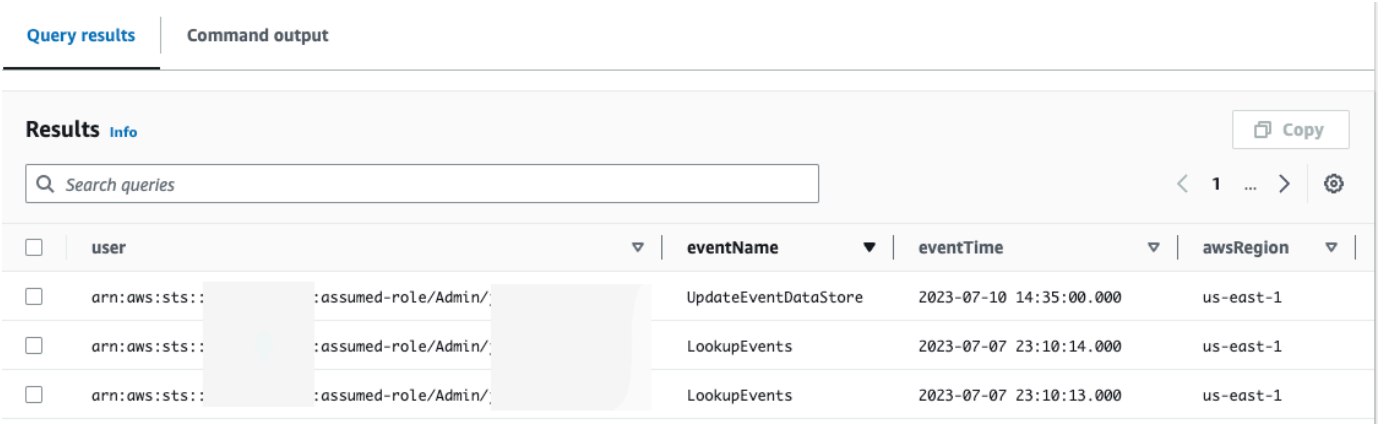


6. Seleccione Ejecutar para ejecutar la consulta.

En la pestaña Resultado del comando, se muestran los metadatos sobre la consulta, por ejemplo, si la consulta se ha hecho correctamente, el número de registros coincidentes y el tiempo de ejecución de la consulta.



En la pestaña Resultados de la consulta, se muestran los datos de eventos del almacén de datos de eventos seleccionado que coinciden con la consulta.



Para obtener más información sobre la edición de una consulta, consulte Creación o edición de una consulta. Para obtener más información sobre cómo ejecutar una consulta y guardar los resultados, consulte Ejecutar una consulta y guardar los resultados de la consulta.

Tutorial: Guardar los resultados de las consultas en un bucket de Amazon S3

En este tutorial se muestra cómo guardar los resultados de las consultas en un bucket de S3 y, a continuación, descargar los resultados de las consultas.

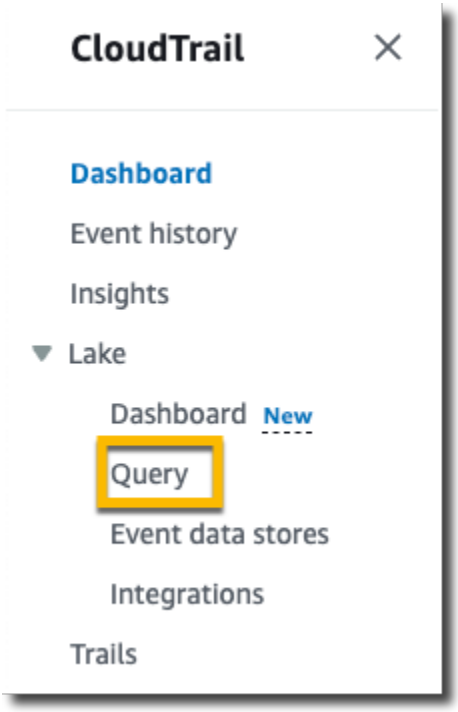
Cuando realizas consultas en CloudTrail Lake, incurres en cargos en función de la cantidad de datos escaneados por la consulta. No hay cargos adicionales de CloudTrail Lake por guardar los

resultados de las consultas en un depósito de S3; sin embargo, sí hay cargos de almacenamiento de S3. Para obtener más información acerca de los precios de S3, consulte Precios de Amazon S3.

Al guardar los resultados de la consulta, es posible que los resultados de la consulta se muestren en la CloudTrail consola antes de que se puedan ver en el depósito de S3, ya que se muestran los resultados de la consulta CloudTrail una vez finalizado el escaneo de la consulta. Si bien la mayoría de las consultas se completan en unos minutos, según el tamaño del banco de datos de eventos, la entrega de los resultados de las consultas CloudTrail al bucket de S3 puede tardar mucho más tiempo. CloudTrail entrega los resultados de la consulta al depósito de S3 en formato gzip comprimido. De media, una vez que se complete el escaneo de la consulta, puede esperar una latencia de 60 a 90 segundos por cada GB de datos que se entregue al bucket de S3.

Para guardar los resultados de las consultas en un bucket de Amazon S3

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Consulta.



3. En las pestañas Consultas guardadas o Consultas guardadas, seleccione el nombre de la consulta para seleccionar una consulta para que se ejecute. En este ejemplo, seleccionaremos la consulta de ejemplo denominada Investigar acciones de usuarios.
4. En la pestaña Editor (Editor), para Event data store (Almacén de datos de eventos), seleccione un almacén de datos de eventos de la lista desplegable. Al elegir el banco de datos del evento

de la lista, rellena CloudTrail automáticamente el ID del banco de datos del evento en la `From` línea.

5. En esta consulta de ejemplo, editaremos el valor de `userIdentity.ARN` para especificar un usuario llamado `Admin` y dejaremos los valores predeterminados para `eventTime`. Al ejecutar una consulta, se le cobra por la cantidad de datos que se analizan. Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales `eventTime` de inicio y finalización a las consultas.

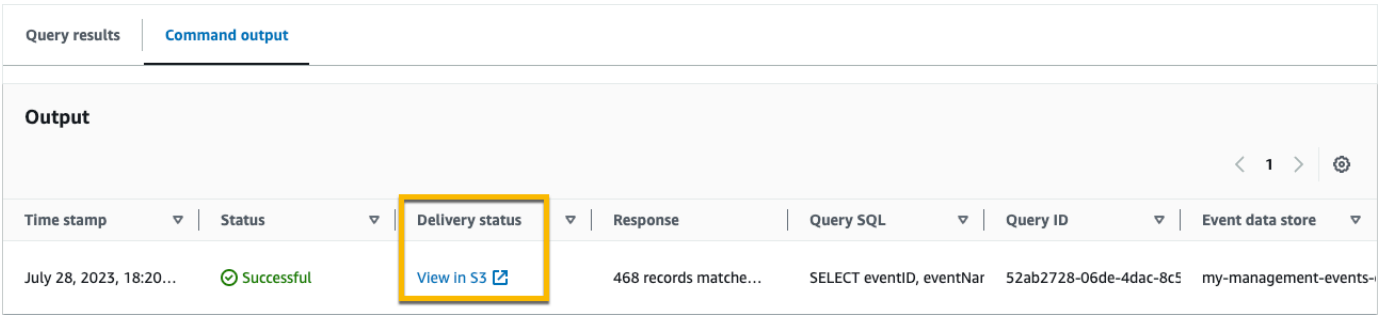
6. Seleccione Guardar resultados en S3 para guardar los resultados de la consulta en un bucket de S3. Al elegir el bucket de S3 predeterminado, CloudTrail crea y aplica las políticas de bucket requeridas. Para obtener más información sobre cómo guardar los resultados de consultas, consulte Información adicional sobre los resultados de consultas guardados. En este ejemplo, utilizaremos el bucket de S3 predeterminado.

> **Note**
>
> Para usar un bucket diferente, especifique un nombre de bucket o elija Browse S3 (Examinar S3) para elegir un bucket. La política del bucket debe conceder CloudTrail permiso para entregar los resultados de las consultas al bucket. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake.

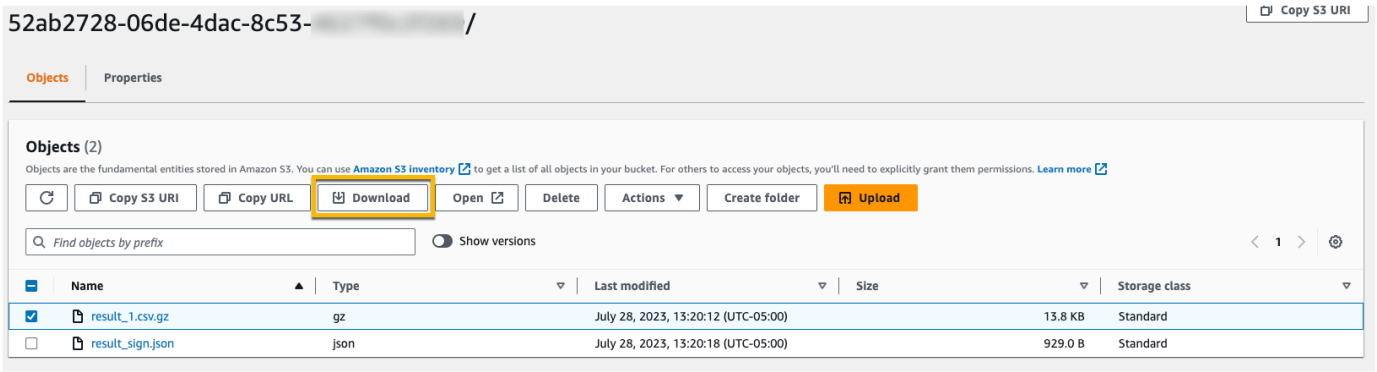
7. Elija Ejecutar. Dependiendo del tamaño de su almacén de datos de eventos y del número de días de datos que incluya, una consulta puede tardar varios minutos en ejecutarse. La pestaña Command output (Resultado del comando) muestra el estado de una consulta y si la consulta ha terminado de ejecutarse. Cuando una consulta haya terminado de ejecutarse, abra Query results (Resultados de la consulta) para ver una tabla de resultados de la consulta activa (la consulta que se muestra actualmente en el editor).
8. Cuando CloudTrail termine de enviar los resultados de las consultas guardadas a su bucket de S3, la columna de estado de entrega proporciona un enlace al bucket de S3 que contiene los archivos de resultados de las consultas guardadas, así como un archivo de firma que puede usar para verificar los resultados de las consultas guardadas. Seleccione Ver en S3 para ver los archivos de resultados de las consultas y los archivos de firma del bucket de S3.

> **Note**
>
> Al guardar los resultados de la consulta, es posible que los resultados de la consulta se muestren en la CloudTrail consola antes de que se puedan ver en el bucket de S3, ya que muestran los resultados de la consulta CloudTrail una vez finalizado el escaneo de la consulta. Si bien la mayoría de las consultas se completan en unos minutos, según el tamaño del banco de datos de eventos, la entrega de los resultados de las consultas CloudTrail al bucket de S3 puede tardar bastante más tiempo. CloudTrail entrega los resultados de la consulta al depósito de S3 en formato gzip comprimido. De media, una

vez que se complete el escaneo de la consulta, puede esperar una latencia de 60 a 90 segundos por cada GB de datos que se entregue al bucket de S3.



9. Para descargar los resultados de la consulta, seleccione el archivo de resultados de la consulta (en este ejemplo, `result_1.csv.gz`) y, a continuación, seleccione Descargar.



Para obtener información sobre la validación de resultados de consultas guardados, consulte Validación de los resultados de consultas guardados.

Trabajar con el historial de CloudTrail eventos

CloudTrail está activado de forma predeterminada en su AWS cuenta y usted tiene acceso automático al historial de CloudTrail eventos. El Historial de eventos proporciona un registro visible e inmutable, que se puede buscar y descargar, de los últimos 90 días de eventos de administración en una Región de AWS. Estos eventos capturan la actividad realizada a través de los AWS Management Console AWS Command Line Interface, y AWS los SDK y las API. El historial de eventos registra los eventos en el Región de AWS lugar donde ocurrió el evento. La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Puede consultar los eventos relacionados con la creación, modificación o eliminación de recursos (como usuarios de IAM o instancias de Amazon EC2) por región en Cuenta de AWS CloudTrail la consola consultando la página Historial de eventos. También puede buscar estos eventos ejecutando el comando aws cloudtrail lookup-events o utilizando la API `LookupEvents`.

Puede utilizar la página del historial de eventos de la CloudTrail consola para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en su infraestructura. AWS Para personalizar la vista del Historial de eventos en la consola, seleccione cuántos eventos mostrar en cada página y qué columnas mostrar u ocultar. También puede comparar los detalles de los eventos en el historial de eventos side-by-side. Puedes buscar eventos mediante programación mediante los AWS SDK o. AWS Command Line Interface

> **Note**
>
> Con el tiempo, Servicios de AWS podría añadir eventos adicionales. CloudTrail registra estos eventos en el historial de eventos, pero un registro completo de actividad de 90 días que incluya los eventos agregados no estará disponible hasta 90 días después de agregar los eventos.
>
> El Historial de eventos es independiente de los registros de seguimiento o almacenes de datos de eventos que cree para su cuenta. Los cambios que haga en los almacenes de datos de eventos o en los registros de seguimiento no afectan al Historial de eventos.

En las secciones siguientes se describe cómo buscar los eventos de gestión recientes mediante la CloudTrail consola y el AWS CLI, y se describe cómo descargar un archivo de eventos. Para obtener información sobre el uso de la `LookupEvents` API para recuperar información de CloudTrail los eventos, consulta LookupEventsla referencia de la AWS CloudTrail API.

Temas

- Limitaciones del Historial de eventos
- Visualización CloudTrail de eventos de administración recientes en la CloudTrail consola
- Visualización CloudTrail de eventos de gestión recientes con AWS CLI

Limitaciones del Historial de eventos

Las limitaciones siguientes son aplicables al Historial de eventos.

- La página del historial de eventos de la CloudTrail consola solo muestra los eventos de administración. No muestra eventos de datos ni de Insights.
- El Historial de eventos está limitado a los últimos 90 días. Para tener un registro continuo de tus eventos Cuenta de AWS, crea un almacén de datos de eventos o una ruta.
- Al descargar eventos desde la página del historial de eventos de la CloudTrail consola, puede descargar hasta 200 000 eventos en un solo archivo. Si alcanzas el límite de 200 000 eventos, la CloudTrail consola te ofrecerá la opción de descargar archivos adicionales.
- El Historial de eventos no proporciona la agregación de eventos a nivel de organización. Para registrar los eventos de su organización, cree un almacén de datos de eventos o un registro de seguimiento de la organización.
- La búsqueda en el historial de eventos se limita a una sola Cuenta de AWS, solo devuelve los eventos de una sola Región de AWS vez y no puede consultar varios atributos. Solo puede aplicar un filtro de atributo y un filtro de intervalo de tiempo.

  Puede crear un banco de datos de eventos de CloudTrail Lake para consultar varios atributos y Regiones de AWS. También puede realizar consultas Cuentas de AWS en varios elementos de una AWS Organizations organización. En CloudTrail Lake, puede consultar varios tipos de eventos, incluidos los eventos de administración, los eventos de datos, los eventos de Insights, los elementos de AWS Config configuración, las pruebas de Audit Manager y las que no son AWS eventos. CloudTrail Las consultas de Lake ofrecen una visión más profunda y personalizable de los eventos que las simples búsquedas de claves y valores en el historial de eventos o en ejecución. `LookupEvents` Para más información, consulte Trabajando con AWS CloudTrail Lake y Cree un banco de datos de CloudTrail eventos para eventos.
- No puede excluir AWS KMS ni los eventos de la API de datos de Amazon RDS del historial de eventos; los ajustes que aplique a un almacén de datos de eventos o senderos no se aplican al historial de eventos.

Visualización CloudTrail de eventos de administración recientes en la CloudTrail consola

Puede utilizar la página del historial de eventos de la CloudTrail consola para ver los últimos 90 días de los eventos de gestión de una Región de AWS. También puede descargar un archivo con dicha información, o un subconjunto de información en función del filtro y el intervalo de tiempo que elija. Puede personalizar la vista del Historial de eventos seleccionando cuántos eventos mostrar en cada página y qué columnas mostrar en la consola. También puede buscar eventos y filtrarlos en función de los tipos de recursos disponibles en un determinado servicio. Puedes seleccionar hasta cinco eventos en el historial de eventos y comparar sus detalles side-by-side.

El Event history (Historial de eventos) no muestra eventos de los datos. Para ver los eventos de datos, cree un almacén de datos de eventos o un registro de seguimiento.

Transcurridos 90 días, los eventos ya no se muestran en Event history (Historial de eventos). No puede eliminar manualmente eventos del Event history (Historial de eventos).

Para obtener más información sobre cómo se CloudTrail registran los eventos de un servicio específico, consulte la documentación de ese servicio. Para obtener más información, consulte AWS temas de servicio para CloudTrail.

> **Note**
>
> Para mantener un registro continuo de la actividad y de los eventos, cree un almacén de datos de eventos o un registro de seguimiento.
> La creación de un almacén de datos de eventos le permite aprovechar las siguientes características:
>
> - Puede crear un almacén de datos de eventos para recopilar eventos CloudTrail de administración y datos, elementos de AWS Config configuración, AWS Audit Manager pruebas o no relacionados con AWS eventos de las integraciones. Para más información, consulte Trabajando con AWS CloudTrail Lake y Creación de un almacén de datos de eventos.
> - Analice su actividad AWS de servicio con las consultas de CloudTrail Lake. CloudTrail Las consultas de Lake ofrecen una visión más profunda y personalizable de los eventos que las simples búsquedas de claves y valores en el historial de eventos o en curso. `LookupEvents` La búsqueda en el historial de eventos se limita a una sola Cuenta de AWS, solo devuelve los eventos de una sola vez Región de AWS y no puede consultar

varios atributos. Por el contrario, los usuarios de CloudTrail Lake pueden ejecutar consultas SQL complejas en varios campos de eventos. Para más información, consulte Creación o edición de una consulta y Visualización de consultas de ejemplo en la consola de CloudTrail.

- Vea los paneles de CloudTrail Lake para visualizar los datos de sus almacenes de datos de eventos. Para obtener más información, consulte Ver los paneles de Lake.
- Un almacén de datos de eventos le permite excluir AWS Key Management Service (AWS KMS) o eventos de la API de datos de Amazon Relational Database Service. AWS KMS acciones como `EncryptDecrypt`, y `GenerateDataKey` suelen generar un gran volumen (más del 99%) de eventos. Los eventos no se pueden excluir del Historial de eventos.

La creación de un registro de seguimiento le permite aprovechar las siguientes integraciones:

- Un registro te permite registrar los eventos de CloudTrail Insights, lo que puede ayudarte a identificar y responder a las actividades inusuales asociadas a las llamadas a `write` la API de administración. Para obtener más información, consulte Registro de eventos de Insights.
- Analice su actividad AWS de servicio con consultas en Amazon Athena. Para obtener más información, consulte Creación de una tabla para CloudTrail registros en la CloudTrail consola en la Guía del usuario de Amazon Athena o elija la opción de crear una tabla directamente desde el historial de eventos de la CloudTrail consola.
- Supervisa tus registros de rutas y recibe notificaciones cuando se produzca una actividad específica con Amazon CloudWatch Logs. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.
- Un registro le permite excluir eventos de la API de datos de Amazon Relational Database Service AWS Key Management Service (AWS KMS) o Amazon Relational Database Service. AWS KMS acciones como `EncryptDecrypt`, y `GenerateDataKey` suelen generar un gran volumen (más del 99%) de eventos. Los eventos no se pueden excluir del Historial de eventos.

Para ver los CloudTrail eventos recientes en la consola

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/home/.
2. En el panel de navegación, elija Event history (Historial de eventos).

Aparecerá una lista filtrada de eventos en el panel de contenido con el último evento en primer lugar. Desplácese hacia abajo para ver más eventos.

3. Para comparar eventos, seleccione hasta cinco para completar las casillas de verificación en el margen izquierdo de la tabla Event history (Historial de eventos). Consulta los detalles de los eventos seleccionados side-by-side en la tabla de comparación de detalles de eventos.

La visualización predeterminada de los eventos en Event history (Historial de eventos) utiliza un filtro de atributos para excluir los eventos de solo lectura de la lista de eventos mostrados. Para eliminar este filtro, o para aplicar otros, cambie su configuración. Para obtener más información, consulte Filtrar CloudTrail eventos.

Contenido

- Navegación entre páginas
- Personalización de la pantalla
- Filtrar CloudTrail eventos
- Ver los detalles de un evento
- Descarga de eventos
- Ver los recursos a los que se hace referencia AWS Config

Navegación entre páginas

Para navegar entre las páginas del Historial de eventos, puede seleccionar la página que desea ver. También puede ver la página siguiente y la anterior en el Historial de eventos.

Seleccione **<** para ver la página anterior del Historial de eventos.

Seleccione **>** para ver la página siguiente del Historial de eventos.

Personalización de la pantalla

Puede personalizar la vista del historial de eventos en la CloudTrail consola seleccionando una de las siguientes preferencias.

- Tamaño de página: elija si desea que se muestren 10, 25 o 50 eventos en cada página.

- Ajustar líneas: permite ajustar el texto para que pueda ver todo el texto de cada evento.
- Filas a rayas: sombrea una de cada dos filas de la tabla.
- Visualización de la hora del evento: elija si desea que se muestre la hora del evento en UTC o en la zona horaria local.
- Seleccionar las columnas visibles: seleccione las columnas que desea que se muestren. De forma predeterminada, se muestran las siguientes columnas:
  - Nombre de evento
  - Hora del evento
  - Nombre de usuario
  - Origen del evento
  - Tipo de recurso
  - Nombre del recurso

> **Note**
>
> No puede cambiar el orden de las columnas ni eliminar manualmente eventos del Event history (Historial de eventos).

Para personalizar la pantalla

1. Inicia sesión en la CloudTrail consola AWS Management Console y ábrela en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, elija Event history (Historial de eventos).
3. Seleccione el icono de la rueda.
4. En Tamaño de página, seleccione el número de eventos que se van a mostrar en una página.
5. Seleccione Ajustar líneas para ver todo el texto de cada evento.
6. Seleccione Filas a rayas para sombrear una de cada dos filas de la tabla.
7. En Visualización de la hora del evento, seleccione si desea que se muestra la hora del evento en UTC o en la zona horaria local. De forma predeterminada, se ha seleccionado UTC.
8. En Select visible columns (Seleccionar las columnas visibles), seleccione las columnas que desea mostrar. Desactive las columnas que no desea mostrar.
9. Cuando haya terminado de hacer los cambios, seleccione Confirmar.

Filtrar CloudTrail eventos

La visualización predeterminada de los eventos en Event history (Historial de eventos) utiliza un filtro de atributos para excluir los eventos de solo lectura de la lista de eventos mostrados. Este filtro de atributos se llama Read-only (Solo lectura) y está configurado como false (falso). Puede eliminar este filtro para visualizar tanto los eventos de lectura como los de escritura. Si desea ver solo los eventos de Read (Lectura), puede cambiar el valor del filtro a true (verdadero). También puede filtrar eventos por otros atributos. También puede filtrar por intervalo de tiempo.

> **Note**
>
> Solo puede aplicar un filtro de atributo y un filtro de intervalo de tiempo. No se pueden aplicar varios filtros de atributo.

AWS clave de acceso

: El identificador de la clave de AWS acceso que se utilizó para firmar la solicitud. Si la solicitud se realizó con credenciales de seguridad temporales, este es el ID de clave de acceso de las credenciales temporales.

ID de evento

: El CloudTrail ID del evento. Cada evento tiene un ID único.

Nombre de evento

: El nombre del evento. Por ejemplo, puede filtrar los eventos de IAM, tales como `CreatePolicy`, o los eventos de Amazon EC2, tales como `RunInstances`.

Origen del evento

: El AWS servicio al que se realizó la solicitud, como `iam.amazonaws.com` `os3.amazonaws.com`. Puede desplazarse por una lista de orígenes de eventos después de elegir el filtro Event source.

Solo lectura

: El tipo de lectura del evento. Los eventos se clasifican como eventos de lectura o de escritura. Si se establece en false (falso), los eventos de lectura no se incluyen en la lista de eventos mostrados. De forma predeterminada, se aplica este filtro de atributo y el valor se establece en false (falso).

Nombre del recurso

El nombre o ID del recurso al que hace referencia el evento. Por ejemplo, el nombre del recurso podría ser "auto-scaling-test-group" para un grupo de Auto Scaling o «i-12345678910" para una instancia EC2.

Tipo de recurso

El tipo de recurso al que hace referencia el evento. Por ejemplo, un tipo de recurso puede ser `Instance` para EC2 o `DBInstance` para RDS. Los AWS tipos de recursos varían para cada servicio.

Intervalo de tiempo

El intervalo de tiempo por el que desea filtrar los eventos. Puede seleccionar un intervalo relativo o un intervalo absoluto. Puede filtrar eventos por los últimos 90 días.

Nombre de usuario

La identidad al que hace referencia el evento. Por ejemplo, puede ser un usuario, un nombre de rol o un rol de servicio.

Si no hay eventos registrados para el atributo o el tiempo elegidos, la lista de resultados estará vacía. Solo puede aplicar un filtro de atributo además del intervalo de tiempo. Si elige un atributo diferente, se mantiene el filtro de intervalo de tiempo especificado.

Los siguientes pasos describen cómo filtrar por atributo.

Para filtrar por atributo

1. Para filtrar los resultados por un atributo, elija un atributo en la lista desplegable Lookup attributes (Atributos de búsqueda) y, a continuación, escriba o elija un valor para el atributo en el cuadro de texto.
2. Para eliminar un filtro de atributo, elija la X situada a la derecha del cuadro de filtro de atributo.

Los siguientes pasos describen cómo filtrar por una fecha y una hora de inicio y finalización.

Para filtrar por una fecha y hora de inicio y finalización

1. Para reducir el intervalo de tiempo de los eventos que desea ver, elija un intervalo de tiempo en la barra de intervalo de tiempo. Puede seleccionar un intervalo relativo o un intervalo absoluto.

Seleccione Intervalo relativo para seleccionar un valor preestablecido o seleccione un intervalo personalizado. Los valores preestablecidos son 30 minutos, 1 hora, 12 horas o 1 día. Para especificar un intervalo de tiempo personalizado, elija Custom (Personalizado).

Seleccione Intervalo absoluto para especificar una hora de inicio y finalización específica. También puede cambiar entre la zona horaria local o UTC.

2. Para eliminar un filtro de intervalo de tiempo, seleccione Borrar y descartar en la barra de intervalo de tiempo.

Ver los detalles de un evento

1. Elija un evento de la lista de resultados para mostrar sus detalles.
2. Los recursos a los que se hace referencia en el evento se muestran en la tabla Resources referenced (Recursos referenciados) en la página de detalles del evento.
3. Algunos recursos a los que se hace referencia tienen enlaces. Elija el enlace para abrir la consola de dicho recurso.
4. Desplácese hasta Event record (Registro de eventos) en la página de detalles para ver el registro de eventos JSON, también llamado carga útil del evento.
5. Seleccione Event history (Historial de eventos) en la ruta de navegación de la página para cerrar la página de detalles del evento y volver a Event history (Historial de eventos).

Descarga de eventos

Puede descargar el historial de eventos registrados como un archivo en formato JSON o CSV. Puedes descargar hasta 200 000 eventos en un solo archivo. Si alcanzas el límite de 200 000 eventos, la CloudTrail consola te ofrecerá la opción de descargar archivos adicionales. Utilice filtros e intervalos de tiempo para reducir el tamaño del archivo que descargue.

> **Note**
>
> CloudTrail Los archivos del historial de eventos son archivos de datos que contienen información (como los nombres de los recursos) que los usuarios individuales pueden configurar. Algunos de estos datos podrían ser interpretados como comandos en los programas que se utilizan para leer y analizar esta información (inyección CSV). Por ejemplo, cuando CloudTrail los eventos se exportan a CSV y se importan a un programa de hojas de

cálculo, es posible que ese programa le advierta sobre problemas de seguridad. Debería deshabilitar este contenido para proteger el sistema. Deshabilite siempre los enlaces o las macros de los archivos de historial de eventos descargados.

1. Agregue un filtro y un intervalo de tiempo para los eventos en el Event history (Historial de eventos) que desea descargar. Por ejemplo, puede especificar el nombre del evento, `StartInstances`, y un intervalo de tiempo de los tres últimos días de actividad.
2. Elija Download events (Descargar eventos) y, a continuación, Download as CSV (Descargar como CSV) o Download as JSON (Descargar como JSON). La descarga comienza inmediatamente.

   > **Note**
   >
   > La descarga podría tardar un tiempo en completarse. Antes de iniciar el proceso de descarga, y para obtener resultados más rápidos, utilice un filtro más específico o un intervalo de tiempo más breve para limitar los resultados. Puede cancelar una descarga. Si cancela una descarga, es posible que en el ordenador local haya una descarga parcial que incluya solo algunos datos de eventos. Para descargar el historial de eventos completo, reinicie la descarga.

3. Cuando haya finalizado la descarga, abra el archivo para ver los eventos que ha especificado.
4. Para cancelar la descarga, elija Cancel (Cancelar) y, a continuación, confirme la operación al seleccionar Cancel download (Cancelar la descarga). Si necesita reiniciar una descarga, espere hasta que la anterior termine de cancelarse.

Ver los recursos a los que se hace referencia AWS Config

AWS Config registra los detalles de configuración, las relaciones y los cambios en AWS los recursos.

En el panel Recursos a los que se hace referencia, seleccione la columna

en la cronología del AWS Config recurso para ver el recurso en la AWS Config consola.

Si el

icono está gris, AWS Config no está encendido o no registra el tipo de recurso. Selecciona el icono para ir a la AWS Config consola y activar el servicio o empezar a grabar ese tipo de recurso. Para obtener más información, consulte Configurar el AWS Config uso de la consola en la Guía para AWS Config desarrolladores.

Si en la columna aparece Link not available, significa que el recurso no se puede ver por alguna de las razones siguientes:

- AWS Config no admite este tipo de recurso. Para obtener más información, consulte Recursos, elementos de configuración y relaciones compatibles en la Guía para desarrolladores de AWS Config .
- AWS Config recientemente se agregó compatibilidad con este tipo de recurso, pero aún no está disponible en la CloudTrail consola. Puedes buscar el recurso en la AWS Config consola para ver su cronología.
- El recurso es propiedad de otra persona Cuenta de AWS.
- El recurso es propiedad de otra persona Servicio de AWS, como una política de IAM gestionada.
- El recurso se creó y se eliminó inmediatamente.
- El recurso se ha creado o actualizado recientemente.

Para conceder a los usuarios permisos de solo lectura para ver los recursos de la AWS Config consola, consulte. Otorgar permiso para ver AWS Config información en la consola CloudTrail

Para obtener más información al respecto AWS Config, consulte la Guía para AWS Config desarrolladores.

Visualización CloudTrail de eventos de gestión recientes con AWS CLI

Puede buscar los eventos CloudTrail de administración de los últimos 90 días para los actuales Región de AWS mediante el aws cloudtrail lookup-events comando. El aws cloudtrail lookup-events comando muestra los eventos en el Región de AWS lugar en el que se produjeron.

La búsqueda admite los siguientes atributos para los eventos de administración:

- AWS clave de acceso
- ID de evento

- Nombre de evento
- Origen del evento
- Solo lectura
- Nombre del recurso
- Tipo de recurso
- Nombre de usuario

Todos los atributos son opcionales.

El comando `lookup-events` incluye las siguientes opciones:

- `--max-items` *`<integer>`*: el número total de elementos que se devuelven en la salida del comando. Si el número total de elementos disponible es mayor que el valor especificado, se proporciona un `NextToken` en la salida del comando. Para reanudar la paginación, proporcione el valor de `NextToken` en el argumento starting-token de un comando posterior. No utilice el elemento de respuesta `NextToken` directamente fuera de la AWS CLI.
- `--start-time` *`<timestamp>`*: especifica que solo se devuelvan los eventos que se producen en el tiempo especificado o con posterioridad. Si la fecha de inicio especificada es posterior a la fecha de finalización especificada, se devuelve un error.
- `--lookup-attributes` *`<integer>`*: contiene una lista de atributos de búsqueda. Actualmente, la lista solo puede contener un elemento.
- `--generate-cli-skeleton` *`<string>`*: imprime un esqueleto de JSON en la salida estándar sin enviar una solicitud a la API. Si se proporciona sin ningún valor o sin la entrada del valor, imprime un JSON de entrada de muestra que se puede utilizar como argumento para `--cli-input-json`. Del mismo modo, si se proporciona yaml-input, se imprimirá una entrada YAML de muestra que se puede utilizar con `--cli-input-yaml`. Si se proporciona la salida del valor, valida las entradas del comando y devuelve un JSON de salida de muestra para ese comando. El esqueleto de JSON generado no es estable entre las versiones del AWS CLI y no hay garantías de compatibilidad con versiones anteriores en el esqueleto de JSON generado.
- `--cli-input-json` *`<string>`*: lee los argumentos de la cadena JSON proporcionada. La cadena JSON sigue el formato proporcionado por el parámetro `--generate-cli-skeleton`. Si se proporcionan otros argumentos en la línea de comandos, esos valores anularán los valores proporcionados por el archivo JSON. No es posible pasar valores binarios arbitrarios utilizando un valor proporcionado por el archivo JSON, ya que la cadena se interpretará literalmente. Es posible que no se especifique junto con el parámetro `--cli-input-yaml`.

Para obtener información general sobre el uso de la interfaz de línea de AWS comandos, consulte la Guía del AWS Command Line Interface usuario.

Contenido

- Requisitos previos
- Obtener ayuda de la línea de comandos
- Buscar eventos
- Especificar el número de eventos que se devuelven
- Buscar eventos por intervalo de tiempo
- Buscar eventos por atributo
  - Ejemplos de búsqueda de atributos
- Especificar la siguiente página de resultados
- Obtener datos de entrada JSON de un archivo
- Campos de resultados de búsqueda

Requisitos previos

- Para ejecutar AWS CLI comandos, debe instalar el AWS CLI. Para obtener más información, consulte Instalación de la interfaz de línea de AWS comandos.
- Asegúrese de que su AWS CLI versión sea posterior a la 1.6.6. Para comprobar la versión de la CLI, ejecute aws --version en la línea de comandos.
- Para configurar la cuenta y el formato de salida predeterminado de una AWS CLI sesión, utilice el aws configure comando. Región de AWS Para obtener más información, consulte Configuración de la interfaz de línea de AWS comandos.

> **Note**
>
> Los CloudTrail AWS CLI comandos distinguen entre mayúsculas y minúsculas.

Obtener ayuda de la línea de comandos

Para ver la ayuda de la línea de comandos de `lookup-events`, escriba el siguiente comando:

```
aws cloudtrail lookup-events help
```

Buscar eventos

> **Important**
>
> La tasa de solicitudes de búsqueda está limitada a dos por segundo, por cuenta y por región. Si se supera este límite, se produce un error de limitación.

Para ver los diez últimos eventos, escriba el siguiente comando:

```
aws cloudtrail lookup-events --max-items 10
```

Un evento devuelto tiene un aspecto similar al siguiente ejemplo ficticio, que se ha formateado para simplificar su lectura:

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
```

```
                        \"MobileVersion\":\"No\",
                        \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                        \"MFAUsed\":\"No\"},
                \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                \"eventType\":\"AwsApiCall\",
                \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```

Para obtener una explicación de los campos relacionados con la búsqueda en el resultado, consulte la sección Campos de resultados de búsqueda más adelante en este documento. Para obtener una explicación de los campos del CloudTrail evento, consulteCloudTrail contenido del registro.

Especificar el número de eventos que se devuelven

Para especificar el número de eventos que se devuelven, escriba el siguiente comando:

```
aws cloudtrail lookup-events --max-items <integer>
```

Los valores posibles comprenden del 1 al 50. El ejemplo siguiente devuelve un solo evento.

```
aws cloudtrail lookup-events --max-items 1
```

Buscar eventos por intervalo de tiempo

Se pueden buscar eventos de los últimos 90 días. Para especificar un intervalo de tiempo, escriba el siguiente comando:

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *`<timestamp>`* especifica, en UTC, que solo se devuelvan los eventos que se producen en el tiempo especificado o con posterioridad. Si la fecha de inicio especificada es posterior a la fecha de finalización especificada, se devuelve un error.

`--end-time` *`<timestamp>`* especifica, en UTC, que solo se devuelvan los eventos que se producen en el tiempo especificado o con anterioridad. Si la fecha de finalización especificada es anterior a la fecha de inicio especificada, se devuelve un error.

La fecha de inicio predeterminada es la primera fecha posible en que los datos están disponibles en los últimos 90 días. La fecha de finalización predeterminada es la fecha del evento que se produjo más cercana a la fecha actual.

Todas las marcas temporales se muestran en UTC.

Buscar eventos por atributo

Para filtrar por un atributo, escriba el siguiente comando:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Solo puede especificar un atributo de pares de clave/valor para cada comando lookup-events. Los siguientes valores son válidos para `AttributeKey`. Los nombres de los valores distinguen entre mayúsculas y minúsculas.

- `AccessKeyId`
- `EventId`
- `EventName`
- `EventSource`
- `ReadOnly`
- `ResourceName`
- `ResourceType`
- `Username`

La longitud máxima para el `AttributeValue` es de 2000 caracteres. Los siguientes caracteres ('_', '', , '\\n') cuentan como dos caracteres dentro del límite de 2000 caracteres.

Ejemplos de búsqueda de atributos

El siguiente comando de ejemplo devuelve los eventos en los que el valor de `AccessKeyId` es `AKIAIOSFODNN7EXAMPLE`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

El siguiente comando de ejemplo devuelve el evento del especificado CloudTrail`EventId`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

El siguiente comando de ejemplo devuelve los eventos en los que el valor de `EventName` es `RunInstances`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

El siguiente comando de ejemplo devuelve los eventos en los que el valor de `EventSource` es `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

El siguiente comando de ejemplo devuelve eventos de escritura. Excluye eventos de lectura como `GetBucketLocation` y `DescribeStream`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

El siguiente comando de ejemplo devuelve los eventos en los que el valor de `ResourceName` es `CloudTrail_CloudWatchLogs_Role`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

El siguiente comando de ejemplo devuelve los eventos en los que el valor de `ResourceType` es `AWS::S3::Bucket`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

El siguiente comando de ejemplo devuelve los eventos en los que el valor de `Username` es `root`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Especificar la siguiente página de resultados

Para obtener la siguiente página de resultados de un comando `lookup-events`, escriba el siguiente comando:

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

donde el valor de *<token>* se obtiene del primer campo del resultado del comando anterior.

Cuando utiliza `--next-token` en un comando, debe utilizar los mismos parámetros que en el comando anterior. Suponga, por ejemplo, que ejecuta el siguiente comando:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Para obtener la siguiente página de resultados, el siguiente comando sería similar al siguiente:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

Obtener datos de entrada JSON de un archivo

AWS CLI Para algunos AWS servicios, tiene dos parámetros `--generate-cli-skeleton` y`--cli-input-json`, que puede usar para generar una plantilla JSON que puede modificar y usar como entrada para el `--cli-input-json` parámetro. En esta sección se describe cómo utilizar estos parámetros con `aws cloudtrail lookup-events`. Para obtener información general, consulte el tema sobre cómo generar parámetros JSON CLI Skeleton y CLI Input.

Para buscar CloudTrail eventos obteniendo la entrada JSON de un archivo

1. Cree una plantilla de entrada para usarla con `lookup-events` redirigiendo el resultado de `--generate-cli-skeleton` a un archivo, como En el ejemplo siguiente.

   ```
   aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
   ```

   El archivo de plantilla generado (en este caso, LookupEvents .txt) tiene el siguiente aspecto:

```
{
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Utilice un editor de texto para modificar los datos JSON según sea necesario. Los datos de entrada JSON solo deben contener los valores que se especifican.

> **Important**
>
> Todos los valores vacíos o null deben eliminarse de la plantilla antes de utilizarla.

El ejemplo siguiente especifica un intervalo de tiempo y un número máximo de resultados que se devuelven.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Para utilizar el archivo editado como entrada, use la sintaxis `--cli-input-json file://<filename>`, como en el ejemplo siguiente:

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> Puede utilizar otros argumentos en la misma línea de comandos como `--cli-input-json`.

Campos de resultados de búsqueda

Eventos

Una lista de eventos de búsqueda en función del atributo de búsqueda y el intervalo de tiempo especificados. La lista de eventos se ordena por tiempo, con el último evento en primer lugar. Cada entrada contiene información sobre la solicitud de búsqueda e incluye una cadena que representa el CloudTrail evento que se recuperó.

Las siguientes entradas describen los campos de cada evento de búsqueda.

CloudTrailEvent

Una cadena JSON que contiene una representación de objeto del evento devuelto. Para obtener información sobre cada uno de los elementos devueltos, consulte la información sobre el contenido del cuerpo del registro.

EventId

Una cadena que contiene el GUID del evento devuelto.

EventName

Una cadena que contiene el nombre del evento devuelto.

EventSource

El AWS servicio al que se realizó la solicitud.

EventTime

La fecha y la hora, en formato de tiempo UNIX, del evento.

Recursos

Una lista de los recursos a los que hace referencia el evento devuelto. Cada entrada de recurso especifica un tipo de recurso y un nombre de recurso.

ResourceName

Una cadena que contiene el nombre del recurso al que hace referencia el evento.

ResourceType

Una cadena que contiene el tipo de recurso al que hace referencia el evento. Cuando el tipo de recurso no se puede determinar, se devuelve null.

Nombre de usuario

Una cadena que contiene el nombre de usuario de la cuenta del evento devuelto.

NextToken

Una cadena para obtener la siguiente página de resultados de un comando `lookup-events` anterior. Para utilizar el token, los parámetros deben ser los mismos que los del comando original. Si no aparece ninguna entrada `NextToken` en la salida, no hay más resultados que devolver.

Trabajando con AWS CloudTrail Lake

AWS CloudTrail Lake te permite ejecutar consultas basadas en SQL en tus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son colecciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción Precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción Precio de retención de siete años. Los selectores que se aplican a un almacén de datos de eventos controlan qué eventos persisten y están disponibles para su consulta. CloudTrail Lake es una solución de auditoría que puede complementar su estrategia de conformidad y ayudarle a solucionar problemas prácticamente en tiempo real.

CloudTrail Almacena datos de eventos en Lake

Cuando crea un almacén de datos de eventos, elige el tipo de eventos que desea incluir en él. Puede crear un banco de datos de eventos para incluir CloudTrail eventos, eventos de CloudTrail Insights, elementos de AWS Config configuración, AWS Audit Manager pruebas o eventos externos AWS. Cada banco de datos de eventos solo puede contener una categoría de eventos específica (por ejemplo, elementos de AWS Config configuración), ya que el esquema de eventos es exclusivo de la categoría de eventos. Puede almacenar los eventos de una organización AWS Organizations en un almacén de datos de eventos de la organización, incluidos los eventos de varias regiones y cuentas. También puede ejecutar consultas SQL en varios almacenes de datos de eventos mediante las palabras clave compatibles con SQL JOIN. Para obtener información acerca de cómo ejecutar consultas en varios almacenes de datos de eventos, consulte Soporte avanzado de consultas en varias tablas.

Puede copiar los eventos de la ruta a un banco de datos de eventos nuevo o existente para crear una point-in-time instantánea de los eventos registrados en la ruta. Para obtener más información, consulte Copiar eventos de registro de seguimiento en un almacén de datos de eventos.

Puede federar un almacén de datos de eventos para ver los metadatos asociados al almacén de datos de eventos en el Catálogo de datos de AWS Glue y ejecutar consultas de SQL sobre los datos de eventos con Amazon Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos

que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

De forma predeterminada, todos los eventos de un almacén de datos de eventos se cifran mediante CloudTrail. Al configurar un banco de datos de eventos, puede optar por utilizar su propia AWS Key Management Service clave. El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

Puede controlar el acceso a las acciones en los almacenes de datos de eventos mediante el uso de una autorización en función de etiquetas. Para obtener más información y ejemplos, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas en esta guía.

Puede usar los paneles de CloudTrail Lake para visualizar los datos de sus almacenes de datos de eventos. Cada panel consta de varios widgets y cada widget representa una consulta SQL. Para obtener más información acerca de los paneles de Lake, consulte Ver los paneles de Lake.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

CloudTrail Lake es compatible con CloudWatch las métricas de Amazon, que proporcionan información sobre los datos ingeridos y los bytes de almacenamiento. Para obtener más información sobre CloudWatch las métricas compatibles, consulteMétricas de CloudWatch compatibles.

> **Note**
>
> CloudTrail normalmente, entrega los eventos en un promedio de unos 5 minutos después de una llamada a la API. No hay garantía de que suceda en este plazo.

CloudTrail Integraciones de Lake

Puede usar las integraciones de CloudTrail Lake para registrar y almacenar datos de actividad de AWS los usuarios desde fuera o desde cualquier fuente en sus entornos híbridos, como aplicaciones

internas o SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores. Después de crear almacenes de datos de eventos en CloudTrail Lake y crear un canal para registrar los eventos de actividad, debe llamar a la `PutAuditEvents` API para incorporar la actividad de su aplicación. CloudTrail Luego, puede usar CloudTrail Lake para buscar, consultar y analizar los datos que se registran desde sus aplicaciones.

Las integraciones también pueden registrar eventos en sus almacenes de datos de eventos de más de una docena de CloudTrail socios. En una integración de socios, crea almacenes de datos de eventos de destino, un canal y una política de recursos. Después de crear la integración, proporciona el ARN del canal al socio. Existen dos tipos de integraciones: directas y de solución. Con las integraciones directas, el socio utiliza la `PutAuditEvents` API para enviar los eventos al almacén de datos de eventos de su AWS cuenta. Con las integraciones de soluciones, la aplicación se ejecuta en su AWS cuenta y la aplicación llama a la `PutAuditEvents` API para enviar los eventos al almacén de datos de eventos de su AWS cuenta.

Para obtener más información sobre las integraciones, consulte Crear una integración con una fuente de eventos externa a. AWS

CloudTrail Consultas de Lake

CloudTrail Las consultas de Lake ofrecen una visión más profunda y personalizable de los eventos que las simples búsquedas de claves y valores en el historial de eventos o en ejecución. `LookupEvents` La búsqueda en el historial de eventos se limita a una sola Cuenta de AWS, solo devuelve los eventos de una sola Región de AWS y no puede consultar varios atributos. Por el contrario, los usuarios de CloudTrail Lake pueden ejecutar consultas SQL complejas en varios campos de eventos. CloudTrail Lake admite todas las `SELECT` instrucciones y funciones de Presto válidas. Para obtener más información acerca de los operadores y funciones SQL compatibles, consulte Funciones y operadores en el sitio web de documentación de Presto.

Puede guardar las consultas de CloudTrail Lake para usarlas en el futuro y ver los resultados de las consultas durante un máximo de siete días. Al ejecutar consultas, puede guardar los resultados de las consultas en un bucket de Amazon S3.

La CloudTrail consola proporciona varios ejemplos de consultas que pueden ayudarle a empezar a escribir sus propias consultas. Para obtener más información, consulte Visualización de consultas de ejemplo en la consola de CloudTrail.

CloudTrail Las consultas de Lake tienen un coste adicional. Cuando ejecuta consultas en Lake, paga según la cantidad de datos escaneados. Para obtener información sobre CloudTrail los precios y

la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Regiones en las que se admite CloudTrail Lake

Actualmente, CloudTrail Lake se admite en las siguientes Regiones de AWS:

Nombre de la región	Región
Este de EE. UU. (Norte de Virginia)	us-east-1
Este de EE. UU. (Ohio)	us-east-2
Oeste de EE. UU. (Norte de California)	us-west-1
Oeste de EE. UU. (Oregón)	us-west-2
Canadá (centro)	ca-central-1
África (Ciudad del Cabo)	af-south-1
Asia-Pacífico (Hong Kong)	ap-east-1
Asia-Pacífico (Bombay)	ap-south-1
Asia-Pacífico (Tokio)	ap-northeast-1
Asia-Pacífico (Seúl)	ap-northeast-2
Asia-Pacífico (Osaka)	ap-northeast-3
Asia Pacífico (Singapur)	ap-southeast-1
Asia-Pacífico (Sídney)	ap-southeast-2
Asia-Pacífico (Yakarta)	ap-southeast-3
Europa (Frankfurt)	eu-central-1
Europa (Estocolmo)	eu-north-1

Nombre de la región	Región
Europa (Irlanda)	eu-west-1
Europa (Londres)	eu-west-2
Europa (París)	eu-west-3
Europa (Milán)	eu-south-1
Medio Oriente (EAU)	me-central-1
Medio Oriente (Baréin)	me-south-1
AWS GovCloud (Este de EE. UU.)	us-gov-este-1
AWS GovCloud (Oeste de EE.UU.)	us-gov-oeste-1
América del Sur (São Paulo)	sa-east-1

Para más información sobre los puntos de conexión del servicio de CloudTrail, consulte Puntos de conexión y cuotas del servicio de AWS CloudTrail.

Para obtener más información sobre la utilización de CloudTrail en la región de AWS GovCloud (EE. UU. Este), consulte Puntos de enlace de AWS GovCloud (EE. UU. Este) en la Guía del usuario de AWS GovCloud (US).

Para obtener más información sobre la utilización de CloudTrail en la región de AWS GovCloud (EE. UU. Oeste), consulte Puntos de enlace de AWS GovCloud (EE. UU. Oeste) en la Guía del usuario de AWS GovCloud (US).

Conceptos y terminología de CloudTrail Lake

En esta sección, se describen los conceptos y términos clave que le ayudarán a utilizar AWS CloudTrail Lake.

Conceptos y términos

- Almacenes de datos de eventos
- Integraciones

- Consultas
- Panel de control

Almacenes de datos de eventos

Los eventos se agregan en almacenes de datos de eventos, que son colecciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados.

Puede crear un almacén de datos de eventos para registrar los eventos de administración y eventos de datos de CloudTrail, los eventos de CloudTrail Insights, las pruebas de AWS Audit Manager, los elementos de configuración de AWS Config o los eventos ajenos a AWS.

Selectores de eventos avanzados

Los selectores de eventos avanzados determinan qué eventos incluir en un almacén de datos de eventos. Los selectores de eventos avanzados le ayudan a controlar los costos al registrar solo aquellos eventos que son importantes para usted.

En el caso de eventos de administración y eventos de datos, puede utilizar selectores de eventos avanzados para filtrar eventos. Por ejemplo, si va a crear un almacén de datos de eventos para recopilar eventos de administración, puede filtrar los eventos de la API de datos de Amazon Relational Database Service (Amazon RDS o AWS Key Management Service (AWS KMS). Por lo general, las acciones de AWS KMS, como `Encrypt`, `Decrypt` y `GenerateDataKey`, generan más del 99 por ciento de los eventos.

En el caso de los elementos de configuración de AWS Config, pruebas de Audit Manager o eventos externos a AWS, se utilizan los selectores de eventos avanzados únicamente para incluir eventos de ese tipo en el almacén de datos de eventos.

Federación

La federación le permite ver los metadatos asociados a un almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL sobre los datos de eventos mediante Amazon Athena. Los metadatos de la tabla almacenados en el Catálogo de datos de AWS Glue permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar.

Cuando habilita la federación de consultas de Lake, CloudTrail crea los recursos federados en su nombre y registra esos recursos con AWS Lake Formation. Una vez habilitada la federación de Lake, puede consultar directamente los datos de su evento en Athena sin necesidad de realizar

ningún paso adicional. Para obtener más información, consulte Federar un almacén de datos de eventos.

Opciones de precios

Cuando crea un almacén de datos de eventos, elige la opción de precio que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre precios, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

Periodo de retención

El periodo de retención de un almacén de datos de eventos determina cuánto tiempo se conservan los datos de eventos en el almacén de datos de eventos. CloudTrail Lake determina si se debe retener un evento. Para ello, comprueba si el valor de `eventTime` del evento se encuentra dentro del periodo de retención especificado. Por ejemplo, si especifica un periodo de retención de 90 días, CloudTrail eliminará los eventos cuando su valor de `eventTime` sea superior a 90 días.

Periodo de retención predeterminado

El periodo de retención predeterminado de un almacén de datos de eventos es el número predeterminado de días que los datos de eventos se conservan en el almacén de datos de eventos. Durante el periodo de retención predeterminado de un almacén de datos de eventos, el almacenamiento se incluye en los precios de incorporación sin costo adicional. Tras el periodo de retención predeterminado, el precio del almacenamiento es de pago por uso.

Periodo de retención máximo

El periodo máximo de retención de un almacén de datos de eventos representa el número máximo de días que puede conservar los datos en un almacén de datos de eventos.

Termination protection

De forma predeterminada, los almacenes de datos de eventos habilitan la protección contra la terminación, que evita que un almacén de datos de eventos se elimine accidentalmente. Para eliminar un almacén de datos de eventos con la protección contra terminación habilitada, seleccione Cambiar la protección contra terminación en el menú Acciones de la página de detalles del almacén de datos de eventos. A continuación, puede continuar con la eliminación del almacén de datos de eventos. Para obtener más información, consulte Cambiar la protección contra la terminación.

Integraciones

Puede usar las integraciones de CloudTrail Lake para registrar y almacenar los datos de actividad de los usuarios de los siguientes orígenes:

- Fuera de AWS
- Cualquier fuente en sus entornos híbridos, como aplicaciones internas o de software como servicio (SaaS) alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores

Una integración requiere un canal para entregar los eventos y un almacén de datos de eventos para recibir los eventos. Después de configurar la integración, llama a la operación de la API PutAuditEvents para incorporar la actividad de su aplicación a CloudTrail. A continuación, puede utilizar CloudTrail Lake para buscar, consultar y analizar los datos que se registran de las aplicaciones. Para obtener más información, consulte Creación de una integración con un origen de eventos externo a AWS.

Tipo de integración

Existen dos tipos de integraciones: directas y de solución. Con las integraciones directas, el socio llama a la operación `PutAuditEvents` de la API para enviar eventos al almacén de datos de eventos de su Cuenta de AWS. Con las integraciones de solución, la aplicación se ejecuta en su Cuenta de AWS y la aplicación llama a la operación `PutAuditEvents` de la API para enviar eventos al almacén de datos de eventos de su Cuenta de AWS.

Canales

Los eventos de actividad de orígenes ajenos a AWS funcionan con canales para incluir eventos a CloudTrail Lake de socios externos que trabajan con CloudTrail o de sus propios orígenes. Cuando crea un canal, elige uno o más almacenes de datos de eventos para almacenar los eventos que llegan del origen del canal. Puede cambiar los almacenes de datos de eventos de destino de un canal según sea necesario, siempre que los almacenes de datos de eventos de destino estén configurados para registrar eventos `eventCategory="ActivityAuditLog"`. Cuando crea un canal para eventos de un socio externo, proporciona un Nombre de recurso de Amazon (ARN) de canal al socio o aplicación de origen.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. La política basada en recursos asociada al canal permite que el origen transmita

eventos a través del canal. Si un canal no tiene una política de recursos, solo el propietario del canal puede llamar a la operación `PutAuditEvents` de la API en el canal. Para obtener más información, consulte Ejemplos de políticas basadas en recursos de AWS CloudTrail.

Consultas

Las consultas de CloudTrail Lake se crean en SQL. Puede crear una consulta en la pestaña Editor de CloudTrail Lake escribiendo la consulta en SQL desde cero o abriendo una consulta guardada o de muestra y editándola. No puede sobrescribir una consulta de muestra ya incluida con sus cambios, pero puede guardarla como una nueva consulta. Para obtener más información, consulte Creación o edición de una consulta.

CloudTrail Lake admite todas las funciones e instrucciones `SELECT` de Presto válidas. Para obtener más información acerca de los operadores y funciones SQL compatibles, consulte Funciones y operadores en el sitio web de documentación de Presto.

Panel de control

Con los paneles de CloudTrail Lake puede visualizar los eventos en un almacén de datos de eventos y ver las tendencias de eventos, como los principales Servicios de AWS, usuarios y los principales errores. Para obtener más información, consulte Ver los paneles de Lake.

Tipo de panel

Los tipos de paneles disponibles para un almacén de datos de eventos dependen de la configuración de los selectores de eventos avanzados del almacén de datos de eventos. Por ejemplo, si un tipo de panel muestra información sobre los eventos de administración de CloudTrail, solo puede seleccionar el panel si el almacén de datos de eventos seleccionado actualmente recopila los eventos de administración de CloudTrail.

Los tipos de paneles disponibles son los siguientes:

- Panel de Información general: muestra los usuarios, las Regiones de AWS y los Servicios de AWS más activos por recuento de eventos. También puede ver información sobre la actividad de los eventos de administración de `read` y `write`, los eventos con más limitación y los principales errores. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración.
- Panel de Eventos de administración: muestra los eventos de inicio de sesión en la consola, los eventos de acceso denegado, las acciones destructivas y los principales errores por usuario.

También puede ver información sobre las versiones de TLS y las llamadas de TLS obsoletas por usuario. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración.

- Panel de Eventos de datos de S3: muestra la actividad de la cuenta de Amazon S3, los objetos de S3 a los que más se accede, los principales usuarios de S3 y las principales acciones de S3. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos de Amazon S3.
- Panel de eventos de Insights: muestra la proporción total de eventos de Insights por tipo de Insights, la proporción de eventos de Insights por tipo de Insights para los principales usuarios y servicios, y el número de eventos de Insights por día. El panel también incluye un widget que muestra hasta 30 días de eventos de Insights. Este panel solo está disponible para los almacenes de datos de eventos que recopilan eventos de Insights.

> **Note**
>
> - Después de que habilite CloudTrail Insights por primera vez en el almacén de datos de eventos de origen, CloudTrail puede tardar hasta 7 días en entregar el primer evento de Insights, si se detecta una actividad inusual. Para obtener más información, consulte Descripción de la entrega de eventos de Insights.
> - El panel Eventos de Insights solo muestra información sobre los eventos de Insights recopilados por el almacén de datos de eventos seleccionado, que viene determinada por la configuración del almacén de datos de eventos de origen. Por ejemplo, si configura el almacén de datos de eventos de origen para habilitar los eventos de Insights en `ApiCallRateInsight`, pero no en `ApiErrorRateInsight`, no verá la información sobre los eventos de Insights en `ApiErrorRateInsight`.

Widgets

Los widgets son los componentes que forman parte de un panel y proporcionan una visualización, como un gráfico de líneas o un gráfico de barras. Cada widget representa una consulta subyacente. Al elegir Ejecutar consultas, CloudTrail ejecuta una consulta generada por el sistema para completar los datos de cada widget.

Creación de un almacén de datos de eventos

Cuando crea un banco de datos de eventos en CloudTrail Lake, elige el tipo de eventos que desea incluir en su banco de datos de eventos. Puede crear un banco de datos de eventos para incluir CloudTrail datos o eventos de administración, eventos de CloudTrail Insights, elementos de AWS Config configuración o eventos externos a AWS. Cada tipo de almacén de datos de eventos solo puede contener categorías de eventos específicas (por ejemplo, elementos de AWS Config configuración), ya que el esquema de eventos es exclusivo de la categoría de eventos. Puede ejecutar consultas SQL en varios almacenes de datos de eventos mediante las palabras clave compatibles SQL JOIN. Para obtener información acerca de cómo ejecutar consultas en varios almacenes de datos de eventos, consulte Soporte avanzado de consultas en varias tablas.

En la siguiente tabla, se muestran las categorías de eventos compatibles con cada tipo de almacén de datos de eventos. En la columna eventCategory, se muestra el valor que se especificaría en los selectores de eventos avanzados para recopilar eventos de ese tipo.

Tipo de evento (consola)	eventCategory (API)	Descripción
CloudTrail eventos	`Management` `Data`	Este tipo de almacén de datos de eventos puede recopilar eventos CloudTrail de administración y datos. Para obtener más información, consulte Crear un banco de datos de CloudTrail eventos para eventos.
CloudTrail Eventos de Insights	`Insight`	Este tipo de almacén de datos de eventos puede recopilar eventos de CloudTrail Insights. Para recibir los eventos de Insights, necesita un banco de datos de eventos de origen que registre los eventos CloudTrail de administr ación y habilite Insights. Para obtener informaci ón sobre cómo crear los bancos de datos de eventos de origen y destino, consulte Crear un banco de datos de eventos para los eventos de CloudTrail Insights.
Elementos de configuración	`Configura tionItem`	Este tipo de almacén de datos de eventos puede recopilar elementos AWS Config de

Tipo de evento (consola)	eventCategory (API)	Descripción
		configuración. Para obtener más información, consulte Crear un banco de datos de eventos para los elementos AWS Config de configuración.
Eventos de integración	`ActivityAuditLog`	Este tipo de almacén de datos de eventos puede recopilar datos no relacionados con AWS eventos de las integraciones. Para obtener más información, consulte Crear un banco de datos de AWS eventos para eventos externos a.

También puede crear un banco de datos de eventos para AWS Audit Manager las pruebas mediante la consola Audit Manager. Para obtener más información sobre la agregación de pruebas en CloudTrail Lake mediante Audit Manager, consulte Cómo funciona el buscador de pruebas con CloudTrail Lake en la Guía del AWS Audit Manager usuario.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

En las siguientes secciones se describe cómo crear, actualizar y eliminar un almacén de datos de eventos mediante la CloudTrail consola. Para obtener información sobre cómo administrar el almacén de datos de eventos mediante el AWS CLI, consulteAdministrar CloudTrail Lake mediante la AWS CLI.

Temas

- Cree un banco de datos de CloudTrail eventos para eventos
- Cree un banco de datos de eventos para los eventos de CloudTrail Insights
- Creación de un almacén de datos de eventos para los elementos de configuración de AWS Config
- Cree un almacén de datos de eventos para eventos ajenos a AWS

- Copiar eventos de registro de seguimiento en un almacén de datos de eventos
- Administración de los ciclos de vida de los almacenes de datos de eventos
- Actualización de un almacén de datos de eventos
- Detener e iniciar la incorporación de eventos
- Federar un almacén de datos de eventos
- Cambiar la protección contra la terminación
- Eliminación de un almacén de datos de eventos
- Restauración de un almacén de datos de eventos
- Almacenes de datos de eventos de la organización

Cree un banco de datos de CloudTrail eventos para eventos

Los almacenes de datos de CloudTrail eventos para eventos pueden registrar eventos CloudTrail de administración y datos. Puede conservar los datos de los eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción Precios de retención ampliables por un año, o hasta 2557 días (unos 7 años) si elige la opción Precios de retención por siete años.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Para crear un almacén de datos de eventos para eventos CloudTrail de administración o de datos

Utilice este procedimiento para crear un banco de datos de eventos que registre los eventos CloudTrail de administración, los eventos de datos o tanto los eventos de administración como de datos.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.

3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configure event data store (Configurar el almacén de datos de eventos), en General details (Detalles generales), ingrese un nombre para el almacén de datos de eventos. El nombre es obligatorio.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

   - Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
     - Periodo de retención predeterminado: 366 días.
     - Periodo máximo de retención: 3653 días.
   - Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
     - Periodo de retención predeterminado: 2557 días.
     - Periodo máximo de retención: 2557 días.
6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

> **Note**
>
> Si está copiando eventos de seguimiento a este almacén de datos de eventos, no CloudTrail copiará ningún evento si `eventTime` es anterior al período de retención especificado. Para determinar el período de retención adecuado, tome la suma del evento más antiguo que desea copiar en días y el número de días que desea conservar los eventos en el almacén de datos del evento (período de retención = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.

7. (Opcional) Para habilitar el cifrado mediante AWS Key Management Service, elija Usar el mío AWS KMS key. Elija Nuevo para que se AWS KMS key cree una para usted, o bien elija Existente para usar una clave KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

   > **Note**
   >
   > Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.

8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar,

leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En la sección Tags (Etiquetas), puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su almacén de datos de eventos y controlar el acceso a él. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo utilizar las etiquetas AWS, consulte Etiquetar AWS los recursos en. Referencia general de AWS
10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
11. En la página Elegir eventos, elija AWS eventos y, a continuación, elija CloudTraileventos.
12. Para CloudTrail los eventos, elige al menos un tipo de evento. De forma predeterminada, se selecciona la opción Management events (Eventos de administración). Puede agregar tanto eventos de administración como de datos a su almacén de datos de eventos. Para obtener más información sobre los eventos de administración, consulte Registro de eventos de administración. Para obtener más información sobre los eventos de datos, consulte Registro de eventos de datos.
13. (Opcional) Elija Copy trail events (Copiar eventos de registros de seguimiento) si desea copiar eventos de un registro de seguimiento existente para ejecutar consultas sobre eventos pasados. Para copiar los eventos de los registros de seguimiento en el almacén de datos de eventos de una organización, debe utilizar su cuenta de administración. La cuenta del administrador delegado no puede copiar los eventos de registro de seguimiento en el almacén de datos de eventos de una organización. Para obtener más información acerca de las consideraciones para

copiar eventos de registro de seguimiento, consulte Consideraciones para copiar eventos de registros de seguimiento.

14. Para que su almacén de datos de eventos recopile eventos de todas las cuentas de una organización de AWS Organizations , seleccione Enable for all accounts in my organization (Activar en todas las cuentas de mi organización). Para crear un almacén de datos de eventos que recopile eventos de una organización, es necesario haber iniciado sesión con la cuenta de administración o la cuenta de administrador delegado de la organización.

> **Note**
>
> Para copiar los eventos de registro de seguimiento o habilitar los eventos de Insights, debe haber iniciado sesión en la cuenta de administración de su organización.

15. Amplíe la configuración adicional para elegir si desea que el banco de datos de eventos recopile los eventos de todos los Regiones de AWS eventos o solo los actuales Región de AWS, y elija si el banco de datos de eventos incluye los eventos. De forma predeterminada, el almacén de datos de eventos recopila los eventos de todas las regiones de la cuenta y comienza a ingerirlos cuando se crea.

    a. Seleccione Incluir solo la región actual en el almacén de datos de eventos para incluir solo los eventos registrados en la región actual. Si no elige esta opción, su almacén de datos de eventos incluirá eventos de todas las regiones.

    b. Anule la selección de Ingerir eventos si no quiere que el almacén de datos de eventos comience a ingerir eventos. Por ejemplo, es posible que desee deseleccionar Ingerir eventos si está copiando eventos de registros de seguimiento y no desea que el almacén de datos de eventos incluya eventos futuros. De forma predeterminada, el almacén de datos de eventos comienza a ingerir eventos cuando se crea.

16. Si el almacén de datos de eventos incluye eventos de administración, puede elegir entre las siguientes opciones. Para obtener más información sobre los eventos de administración, consulte Registro de eventos de administración.

    a. Elija si desea incluir eventos de Lectura, de Escritura o ambos. Se necesita una como mínimo.

    b. Elija si desea excluir AWS Key Management Service o excluir los eventos de la API de datos de Amazon RDS del almacén de datos de eventos.

c. Elija si desea habilitar Insights. Para habilitar Insights, debe configurar un almacén de datos de eventos de destino para recopilar los eventos de Insights en función de la actividad de los eventos de administración en este almacén de datos de eventos.

   Si decide habilitar Insights, haga lo siguiente.

   i. En Habilitar Insights, elija el almacén de eventos de destino que registrará los eventos de Insights. El almacén de datos de eventos de destino recopilará los eventos de Insights en función de la actividad de los eventos de administración en este almacén de datos de eventos. Para obtener información acerca de cómo crear un almacén de datos de eventos de destino, consulte Cómo crear un almacén de datos de eventos de destino que registre los eventos de Insights.

   ii. Elija los tipos de Insights. Puede elegir la tasa de llamadas a la API, la tasa de errores de la API o ambas. Debe registrar los eventos de administración de escritura para registrar los eventos de Insights para calcular la tasa de llamadas a la API. Debe registrar los eventos de administración de lectura o escritura para registrar los eventos de Insights para calcular la tasa de errores de la API.

17. Para incluir eventos de datos en su almacén de datos de eventos, haga lo siguiente.

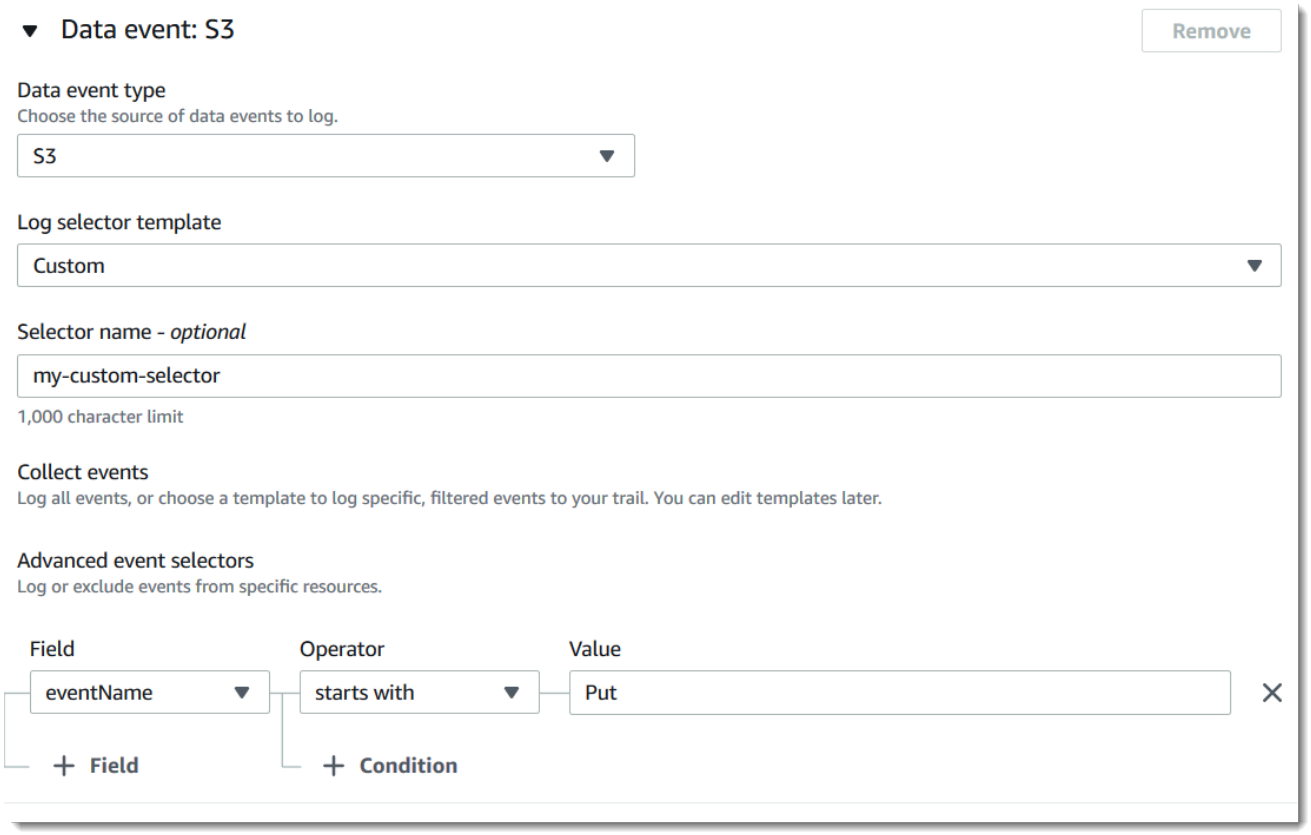
    a. Elija un tipo de evento de datos. Este es el Servicio de AWS recurso en el que se registran los eventos de datos. Para registrar los eventos de datos de AWS Glue las tablas creadas por Lake Formation, elija Lake Formation como tipo de datos.

    b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede elegir registrar todos los eventos de datos, eventos `readOnly`, eventos `writeOnly`, o Custom (Personalizado) para crear un selector de registros personalizado.

    c. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo opcional para un selector de eventos avanzado, como “Registrar eventos de datos para solo dos buckets de S3”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la Vista JSON.

    d. En Advanced event selectors (Selectores de eventos avanzados), cree expresiones mediante la selección de valores para Field (Campo), Operator (Operador) y Value (Valor). Los selectores de eventos avanzados para un almacén de datos de eventos funcionan igual que los selectores de eventos avanzados que se aplican a un registro de seguimiento. Para obtener más información sobre cómo crear selectores de eventos avanzados, consulte Registrar eventos de datos con selectores de eventos avanzados.

El siguiente ejemplo utiliza una plantilla de selector de registro Custom (Personalizada) para elegir únicamente los nombres de los eventos de objetos S3 que comienzan por `Put`, como `PutObject`. Dado que el selector de eventos avanzado no incluye ni excluye ningún otro tipo de evento o ARN de recursos, todos los eventos de datos de S3 que tienen nombres de eventos que empiezan por `Put`, tanto de lectura como de escritura, se almacenan en el almacén de datos de eventos.



> **Important**
>
> Para excluir o incluir eventos de datos con selectores de eventos avanzados mediante el uso de un ARN de bucket de S3, utilice siempre el operador Starts with (Empezar por).

e. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.

18. Para copiar eventos de registro de seguimiento existentes en el almacén de datos, haga lo siguiente.

a. Elija el registro de seguimiento que desea copiar. De forma predeterminada, CloudTrail solo copia CloudTrail los eventos contenidos en el `CloudTrail` prefijo del bucket de S3 y los prefijos incluidos en el `CloudTrail` prefijo, y no comprueba los prefijos de otros servicios. AWS Si desea copiar CloudTrail los eventos contenidos en otro prefijo, elija Introducir el URI de S3 y, a continuación, elija Examinar S3 para buscar el prefijo. Si el depósito de S3 de origen de la ruta utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS CloudTrail permita descifrar los datos. Si el bucket de S3 de origen utiliza varias claves KMS, debe actualizar la política de cada clave CloudTrail para poder descifrar los datos del bucket. Para obtener más información sobre la actualización de la política de claves KMS, consulte Política de claves KMS para descifrar datos en el bucket de S3 de origen.

b. Elija el intervalo de tiempo para copiar los eventos. CloudTrail comprueba el prefijo y el nombre del archivo de registro para comprobar que el nombre contiene una fecha entre la fecha de inicio y la de finalización elegidas antes de intentar copiar los eventos de seguimiento. Puede elegir un intervalo relativo o un intervalo absoluto. Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de tiempo que sea anterior a la creación del almacén de datos de eventos.

> **Note**
>
> CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Por ejemplo, si el período de retención de un almacén de datos de eventos es de 90 días, no CloudTrail copiará ningún evento de ruta que tenga una `eventTime` antigüedad superior a 90 días.

- Si eliges Rango relativo, puedes elegir copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un rango personalizado. CloudTrail copia los eventos registrados en el período de tiempo elegido.
- Si elige Rango absoluto, puede elegir una fecha de inicio y finalización específica. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y finalización elegidas.

c. Para Permissions (Permisos), elija una de las siguientes opciones de rol de IAM. Si elige un rol de IAM existente, verifique que la política de roles de IAM proporcione los permisos

necesarios. Para obtener más información acerca de la actualización de los permisos de rol de IAM, consulte Permisos de IAM para copiar eventos de registro de seguimiento.

- Elija Create a new role (recommended) (Crear un nuevo rol [recomendado]) para crear un nuevo rol de IAM. En Introducir el nombre del rol de IAM, introduzca un nombre para el rol. CloudTrail crea automáticamente los permisos necesarios para este nuevo rol.
- Elija Use a custom IAM role (Utilizar un rol de IAM personalizado) para usar un rol de IAM personalizado que no aparezca en la lista. En Enter IAM role ARN (Ingresar ARN del rol de IAM), escriba el ARN de IAM.
- Seleccione Use an existing role (Utilizar un rol existente) para elegir un rol de IAM existente en la lista desplegable.

19. Elija Next (Siguiente) para revisar las opciones seleccionadas.
20. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).
21. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

    A partir de este momento, el almacén de datos de eventos captura los eventos que coinciden con sus selectores de eventos avanzados (si ha seleccionado la opción Incorporar eventos). Los eventos que ocurrieron antes de que creara el almacén de datos de eventos no estarán en el almacén de datos de eventos, a menos que opte por copiar los eventos de registro de seguimiento existentes.

Ahora puede ejecutar consultas en su nuevo almacén de datos de eventos. La pestaña Sample queries (Consultas de muestra) proporciona ejemplos de consultas para que pueda empezar. Para obtener más información acerca de la creación y la edición de consultas, consulte Creación o edición de una consulta.

También puede ver el panel de control de CloudTrail Lake para visualizar los eventos en su almacén de datos de eventos. Para obtener más información acerca de los paneles de Lake, consulte Ver los paneles de Lake.

Cree un banco de datos de eventos para los eventos de CloudTrail Insights

AWS CloudTrail Insights ayuda a AWS los usuarios a identificar y responder a las actividades inusuales asociadas a las llamadas a la API y a las tasas de error de la API mediante el análisis

continuo CloudTrail de los eventos de gestión. CloudTrail Insights analiza los patrones normales del volumen de llamadas a la API y las tasas de error de la API, también denominadas valores de referencia, y genera eventos de Insights cuando el volumen de llamadas o las tasas de error están fuera de los patrones normales. Los eventos de Insights en el volumen de llamadas de API se generan para las API de administración de `write` y los eventos de Insights en la tasa de errores de API se generan tanto para las API de administración `read` como `write`.

Para registrar los eventos de Insights en CloudTrail Lake, necesita un almacén de datos de eventos de destino que registre los eventos de Insights y un banco de datos de eventos de origen que habilite Insights y registre los eventos de administración.

> **Note**
>
> Para registrar los eventos de Insights sobre el volumen de llamadas a la API, el almacén de datos de eventos de origen debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el almacén de datos de eventos de origen debe registrar los eventos de administración de `read` o `write`.

Si tiene CloudTrail Insights activado en un banco de datos de eventos de origen y CloudTrail detecta actividades inusuales, CloudTrail envía los eventos de Insights al banco de datos de eventos de destino. A diferencia de otros tipos de eventos capturados en un banco CloudTrail de datos de eventos, los eventos de Insights solo se registran cuando CloudTrail detecta cambios en el uso de la API de su cuenta que difieren significativamente de los patrones de uso típicos de la cuenta.

Tras activar CloudTrail Insights por primera vez en un banco de datos de eventos, la entrega del primer evento de Insights puede CloudTrail demorar hasta 7 días si se detecta una actividad inusual.

CloudTrail Insights analiza los eventos de gestión que se producen en una sola región, no a nivel mundial. Un evento de CloudTrail Insights se genera en la misma región en la que se generan los eventos de gestión que lo respaldan.

En el caso de un banco de datos de eventos de la organización, CloudTrail analiza los eventos de gestión de la cuenta de cada miembro en lugar de analizar la agregación de todos los eventos de gestión de la organización.

Se aplican cargos adicionales por la ingesta de eventos de Insights en CloudTrail Lake. Se te cobrará por separado si activas Insights tanto para los almacenes de datos de los senderos como para los

de eventos de CloudTrail Lake. Para obtener información sobre CloudTrail los precios, consulta AWS CloudTrail los precios.

Temas

- Cómo crear un almacén de datos de eventos de destino que registre los eventos de Insights
- Para crear un almacén de datos de eventos de origen que habilite los eventos de Insights

Cómo crear un almacén de datos de eventos de destino que registre los eventos de Insights

Al crear un almacén de datos de eventos de Insights, tiene la opción de elegir un almacén de datos de eventos de origen existente que registre los eventos de administración y, a continuación, especificar los tipos de Insights que desea recibir. O bien, puede habilitar Insights en un almacén de datos de eventos nuevo o existente después de crear su almacén de datos de eventos de Insights y, a continuación, elegir este almacén de datos de eventos como el almacén de datos de eventos de destino.

En este procedimiento, se muestra cómo crear un almacén de datos de eventos de destino que registre los eventos de Insights.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, abra el submenú Lake (Lago) y, a continuación, elija Event data stores (Almacenes de datos de eventos).
3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configure event data store (Configurar el almacén de datos de eventos), en General details (Detalles generales), ingrese un nombre para el almacén de datos de eventos. El nombre es obligatorio.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

- Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
  - Periodo de retención predeterminado: 366 días.
  - Periodo máximo de retención: 3653 días.
- Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
  - Periodo de retención predeterminado: 2557 días.
  - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención en días para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años. El almacén de datos de eventos retiene los datos de eventos durante el número especificado de días.
7. (Opcional) Para habilitar el cifrado AWS Key Management Service, selecciona Usar el mío AWS KMS key. Elija Nuevo para que se AWS KMS key cree una para usted, o bien elija Existente para usar una clave KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

> **Note**
>
> Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.

8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

   Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

   a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

   b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

   c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En la sección Tags (Etiquetas), puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su almacén de datos de eventos y controlar el acceso a él. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo utilizar las etiquetas AWS, consulte Etiquetar AWS los recursos en. Referencia general de AWS

10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.

11. En la página Elegir eventos, elija AWS eventos y, a continuación, elija eventos de CloudTrail Insights.

12. En los eventos de CloudTrail Insights, haga lo siguiente.

    a. Seleccione Permitir el acceso de administrador delegado si desea conceder al administrador delegado de su organización el acceso a este almacén de datos de eventos. Esta opción solo está disponible si ha iniciado sesión con la cuenta de administración de una AWS Organizations organización.

    b. (Opcional) Elija un almacén de datos de eventos de origen existente que registre los eventos de administración y especifique los tipos de Insights que desea recibir.

       Para agregar un almacén de datos de origen, realice lo siguiente.

       i. Elija Agregar almacén de datos de eventos de origen.

       ii. Elija el almacén de datos de eventos de origen.

       iii. Elija el tipo de Insights que desea recibir.

       - `ApiCallRateInsight`: el tipo de Insights `ApiCallRateInsight` analiza las llamadas a la API de administración de solo escritura que se agregan por minuto en comparación con un volumen de llamadas a la API de referencia. Para recibir Insights en `ApiCallRateInsight`, el almacén de datos de eventos de origen debe registrar los eventos de administración Escritura.
       - `ApiErrorRateInsight`: el tipo de Insights `ApiErrorRateInsight` analiza las llamadas a la API de administración que generan códigos de error. El error se muestra si la llamada a la API no se hace correctamente. Para recibir Insights en `ApiErrorRateInsight`, el almacén de datos de eventos de origen debe registrar los eventos de administración Escritura o Lectura.

       iv. Repita los dos pasos anteriores (ii y iii) para agregar cualquier tipo de Insights adicional que desee recibir.

13. Elija Next (Siguiente) para revisar las opciones seleccionadas.

14. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).

15. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

16. Si no eligió un almacén de datos de eventos de origen en el paso 10, siga los pasos que se indican en Para crear un almacén de datos de eventos de origen que habilite los eventos de Insights para crear un almacén de datos de eventos de origen.

Para crear un almacén de datos de eventos de origen que habilite los eventos de Insights

Este procedimiento le muestra cómo crear un almacén de datos de eventos de origen que habilite los eventos de Insights y registre los eventos de administración.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, abra el submenú Lake (Lago) y, a continuación, elija Event data stores (Almacenes de datos de eventos).
3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configure event data store (Configurar el almacén de datos de eventos), en General details (Detalles generales), ingrese un nombre para el almacén de datos de eventos. El nombre es obligatorio.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

   - Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
     - Periodo de retención predeterminado: 366 días.
     - Periodo máximo de retención: 3653 días.
   - Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
     - Periodo de retención predeterminado: 2557 días.
     - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

7. (Opcional) Para habilitar el cifrado mediante AWS Key Management Service, selecciona Usar el mío AWS KMS key. Elija Nuevo para que se AWS KMS key cree una para usted, o bien elija Existente para usar una clave KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

   > **Note**
   >
   > Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.

8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En la sección Tags (Etiquetas), puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su almacén de datos de eventos y controlar el acceso a él. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo utilizar las etiquetas AWS, consulte Etiquetar AWS los recursos en. Referencia general de AWS
10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
11. En la página Elegir eventos, elija AWS eventos y, a continuación, elija CloudTraileventos.
12. En CloudTrail los eventos, deje seleccionada la opción Eventos de administración.
13. Para que su almacén de datos de eventos recopile eventos de todas las cuentas de una organización de AWS Organizations , seleccione Enable for all accounts in my organization (Activar en todas las cuentas de mi organización). Debe iniciar sesión en la cuenta de administración de la organización para crear un almacén de datos de eventos que habilite Insights.
14. Expanda la opción Configuración adicional para elegir si desea que el banco de datos de eventos recopile los eventos de todos los Regiones de AWS eventos o solo los actuales Región de AWS, y elija si el banco de datos de eventos incluye los eventos. De forma predeterminada, el almacén de datos de eventos recopila los eventos de todas las regiones de la cuenta y comienza a ingerirlos cuando se crea.

    a. Seleccione Incluir solo la región actual en el almacén de datos de eventos si desea incluir solo los eventos registrados en la región actual. Si no elige esta opción, su almacén de datos de eventos incluirá eventos de todas las regiones.

b. Deje los eventos de incorporación seleccionados.

15. Elija el tipo de eventos de administración que desea incluir en él. Puede elegir Lectura, Escritura o ambas opciones. Se necesita una como mínimo.

> **Note**
>
> Para registrar los eventos de Insights sobre el volumen de llamadas a la API, el almacén de datos de eventos debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el almacén de datos de eventos debe registrar los eventos de administración de `read` o `write`.

16. Puede optar por excluir AWS Key Management Service o excluir los eventos de la API de datos de Amazon RDS del almacén de datos de eventos. Para obtener más información sobre estas opciones, consulte Registro de eventos de administración.
17. Seleccione Habilitar Insights.
18. En Habilitar Insights, elija el almacén de eventos de destino que registrará los eventos de Insights. El almacén de datos de eventos de destino recopilará los eventos de Insights en función de la actividad de los eventos de administración en este almacén de datos de eventos. Para obtener información acerca de cómo crear un almacén de datos de eventos de destino, consulte Cómo crear un almacén de datos de eventos de destino que registre los eventos de Insights.
19. Elija los tipos de Insights. Puede elegir la tasa de llamadas a la API, la tasa de errores de la API o ambas. Debe registrar los eventos de administración de escritura para registrar los eventos de Insights para calcular la tasa de llamadas a la API. Debe registrar los eventos de administración de lectura o escritura para registrar los eventos de Insights para calcular la tasa de errores de la API.
20. Elija Next (Siguiente) para revisar las opciones seleccionadas.
21. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).
22. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

    A partir de este momento, el almacén de datos de eventos captura los eventos que coinciden con sus selectores de eventos avanzados. Tras activar CloudTrail Insights por primera vez en el

banco de datos de eventos de origen, el primer evento de Insights puede tardar hasta 7 días en enviarse al banco de datos de eventos de destino si se detecta una actividad inusual. CloudTrail

Puede ver el panel de CloudTrail Lake para visualizar los eventos de Insights en el banco de datos de eventos de su destino. Para obtener más información acerca de los paneles de Lake, consulte Ver los paneles de Lake.

Se aplican cargos adicionales por la ingesta de eventos de Insights en CloudTrail Lake. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para obtener información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Creación de un almacén de datos de eventos para los elementos de configuración de AWS Config

Puede crear un almacén de datos de eventos para que incluya elementos de configuración de AWS Config y utilizarlo para investigar los cambios en los entornos de producción que no cumplen con los requisitos. Con un almacén de datos de eventos, puede relacionar las reglas que no cumplen los requisitos con los usuarios y los recursos asociados a los cambios. Un elemento de configuración representa una point-in-time vista de los atributos de un AWS recurso compatible que existe en su cuenta. AWS Config crea un elemento de configuración cada vez que detecta un cambio en un tipo de recurso que está registrando. AWS Config también crea elementos de configuración cuando se captura una instantánea de la configuración.

Puede usar ambos AWS Config y CloudTrail Lake para ejecutar consultas sobre los elementos de configuración. Se puede utilizar AWS Config para consultar el estado de configuración actual de AWS los recursos en función de las propiedades de configuración de una sola Cuenta de AWS cuenta o de varias cuentas y regiones. Región de AWS Por el contrario, puede usar CloudTrail Lake para consultar diversas fuentes de datos, como CloudTrail eventos, elementos de configuración y evaluaciones de reglas. CloudTrail Las consultas de Lake abarcan todos los elementos AWS Config de configuración, incluida la configuración de los recursos y el historial de conformidad.

La creación de un almacén de datos de eventos para los elementos de configuración no afecta a las consultas AWS Config avanzadas existentes ni a AWS Config los agregadores configurados. Puede seguir ejecutando consultas avanzadas utilizando y AWS Config enviando archivos AWS Config de historial a sus depósitos de S3.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios

determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Limitaciones

A los almacenes de datos de eventos para elementos de configuración se aplican las siguientes limitaciones.

- No admiten elementos de configuración personalizados.
- No admiten el filtrado de eventos mediante el uso de selectores de eventos avanzados.

Requisitos previos

Antes de crear el almacén de datos de tus eventos, configura el AWS Config registro de todas tus cuentas y regiones. Puede utilizar la configuración rápida, una función de AWS Systems Manager, para crear rápidamente una grabadora de configuración con tecnología AWS Config.

> **Note**
>
> Se le cobrarán tarifas de uso del servicio cuando AWS Config comience a grabar las configuraciones. Para obtener más información sobre los precios, consulte Precios de AWS Config. Para obtener información acerca de la administración del registrador de configuraciones, consulte Managing the Configuration Recorder (Administración del registrador de configuraciones) en la Guía para desarrolladores de AWS Config .

Además, se recomienda llevar a cabo las siguientes acciones, aunque no son obligatorias para crear un almacén de datos de eventos.

- Configure un bucket de Amazon S3 para recibir una instantánea de configuración a solicitud y el historial de configuración. Para obtener más información acerca de las instantáneas, consulte Managing the Delivery Channel (Administrar el canal de entrega) y Delivering Configuration Snapshot to an Amazon S3 Bucket (Entrega de instantáneas de configuración a un bucket de Amazon S3) en la Guía para desarrolladores de AWS Config .
- Especifique las reglas que desee utilizar AWS Config para evaluar la información de conformidad de los tipos de recursos registrados. Varios de los ejemplos de consultas de CloudTrail Lake AWS

Config requieren Reglas de AWS Config evaluar el estado de cumplimiento de sus AWS recursos. Para obtener más información Reglas de AWS Config, consulte Cómo evaluar los recursos Reglas de AWS Config en la Guía para AWS Config desarrolladores.

Para crear un almacén de datos de eventos para elementos de configuración

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configure event data store (Configurar el almacén de datos de eventos), en General details (Detalles generales), ingrese un nombre para el almacén de datos de eventos. El nombre es obligatorio.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

   - Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.
     - Periodo de retención predeterminado: 366 días.
     - Periodo máximo de retención: 3653 días.
   - Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
     - Periodo de retención predeterminado: 2557 días.
     - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

7. (Opcional) Para habilitar el cifrado mediante AWS Key Management Service, selecciona Usar el mío AWS KMS key. Elija Nuevo para que se AWS KMS key cree una para usted, o bien elija Existente para usar una clave KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

   > **Note**
   >
   > Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.

8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En la sección Tags (Etiquetas), puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su almacén de datos de eventos y controlar el acceso a él. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo utilizar las etiquetas AWS, consulte Etiquetar AWS los recursos en. Referencia general de AWS
10. Elija Siguiente.
11. En la página Elegir eventos, elija Eventos de AWS y, a continuación, Elementos de configuración.
12. CloudTrail almacena el recurso del almacén de datos de eventos en la región en la que lo creó, pero de forma predeterminada, los elementos de configuración recopilados en el banco de datos provienen de todas las regiones de su cuenta que tienen el registro activado. De forma opcional, puede seleccionar Include only the current region in my event data store (Incluir solo la región actual en el almacén de datos de eventos) para incluir solo los elementos de configuración capturados en la región actual. Si no elige esta opción, su almacén de datos de eventos incluirá elementos de configuración de todas las regiones que tengan habilitado el registro.
13. Para que el almacén de datos de eventos recopile los elementos de configuración de todas las cuentas de una AWS Organizations organización, seleccione Activar para todas las cuentas de mi organización. Para crear un almacén de datos de eventos que recopile elementos de configuración para una organización, es necesario haber iniciado sesión con la cuenta de administración o la cuenta de administrador delegado de la organización.
14. Elija Next (Siguiente) para revisar las opciones seleccionadas.

15. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).
16. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

    A partir de este momento, el almacén de datos de eventos capturará los elementos de configuración. Aquellos que se generaron antes de crear el almacén de datos de eventos no estarán en él.

Consultas de ejemplo

Ahora puede ejecutar consultas en su nuevo almacén de datos de eventos. La pestaña Consultas de muestra de la CloudTrail consola proporciona consultas de ejemplo para empezar. A continuación, se muestran algunos ejemplos de consultas que puede ejecutar en el almacén de datos de eventos de elementos de configuración.

Descripción	Consultar
Busque qué usuario realizó una acción que dio lugar a un estado de incumplimiento uniendo el almacén de datos de eventos de un elemento de configuración a un almacén de datos de CloudTrail eventos.	`SELECT element_at(config1.eventDat a.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventDat a.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM config_event_data_store_ID as config1 JOIN config_event_data_store_ID as config2 on element_at(config1 .eventData.configuration, 'targetRe sourceId') = config2.eventData. resourceId JOIN cloudtrail_event_data_store_ID as cloudtrail on config2.eventData.`

Descripción	Consultar

	arn = element_at(cloudtrail.resou
	rces, 1).arn
	WHERE
	    element_at(config1.eventDat
	a.configuration, 'configRuleList')
	 is not null
	AND
	    element_at(config1.eventDat
	a.configuration, 'complianceType') =
	 'NON_COMPLIANT'
	AND
	    cloudtrail.eventTime > '2022-11-
	14 00:00:00'
	AND
	    config2.eventData.resourceType =
	 'AWS::DynamoDB::Table'

Descripción	Consultar
Busque todas AWS Config las reglas y devuelva el estado de conformidad de los elementos de configuración generados el día anterior.	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceName, eventData.resourceCreationTime, element_at(eventData.configuration,'complianceType') AS complianceType, element_at(eventData.configuration, 'configRuleList') AS configRuleList, element_at(eventData.configuration, 'resourceId') AS resourceId, element_at(eventData.configuration, 'resourceType') AS resourceType FROM config_event_data_store_ID WHERE eventData.resourceType = 'AWS::Config::ResourceCompliance' AND eventTime > '2022-11-22 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10`

Descripción	Consultar

Encuentre el recuento total de AWS Config recursos agrupado por tipo de recurso, identific ador de cuenta y región.	`SELECT`
	`    eventData.resourceType, eventData .awsRegion, eventData.accountId,`
	`COUNT (*) AS resourceCount`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventTime > '2022-11-22 00:00:00'`
	`GROUP BY`
	`    eventData.resourceType, eventData .awsRegion, eventData.accountId`

Encuentre la hora de creación de los recursos para todos los elementos de AWS Config configuración generados en una fecha específica.	`SELECT`
	`    eventData.configuration, eventData.accountId,`
	`    eventData.awsRegion, eventData .resourceId,`
	`    eventData.resourceName, eventData .resourceType,`
	`    eventData.availabilityZone, eventData.resourceCreationTime`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventTime > '2022-11-16 00:00:00'`
	`AND`
	`    eventTime < '2022-11-17 00:00:00'`
	
	`ORDER BY`
	`    eventData.resourceCreationTime DESC`
	`    limit 10;`

Para obtener más información acerca de la creación y la edición de consultas, consulte Creación o edición de una consulta.

Esquema de los elementos de configuración

En la siguiente tabla, se describen los elementos del esquema obligatorios y opcionales que coinciden con los de los registros de elementos de configuración. Los elementos de configuración `eventData` proporcionan el contenido de; el resto de los campos los proporcionan CloudTrail después de la ingesta.

CloudTrail el contenido del registro de eventos se describe con más detalle enCloudTrail contenido del registro.

- Los campos que se proporcionan CloudTrail después de la ingestión
- Campos que proporcionan los eventos

Campos proporcionados por CloudTrail After Ingestion

Nombre del campo	Tipo de entrada	Requisito	Descripción
eventVersion	cadena	Obligatoria	La versión del formato del AWS evento.
eventCategory	cadena	Obligatoria	La categoría del evento. Para los elementos de configuración, el valor válido es `ConfigurationItem` .
eventType	cadena	Obligatoria	Tipo de evento. Para los elementos de configuración, el valor válido es `AwsConfigurationItem` .
eventID	cadena	Obligatoria	El ID único de un evento.
eventTime	cadena	Obligatoria	La marca de tiempo del evento, en

Nombre del campo	Tipo de entrada	Requisito	Descripción
			formato `yyyy-MM-DDTHH:mm:ss` , en Hora Universal Coordinada (UTC).
awsRegion	cadena	Obligatoria	La Región de AWS a la que se va a asignar un evento.
recipientAccountId	cadena	Obligatoria	Representa el Cuenta de AWS identific ador que recibió este evento.
addendum	addendum	Opcional	Muestra informaci ón sobre el motivo por el cual se retrasó un evento. Si falta información de un evento existente, el bloque addendum incluye la información que falta y el motivo por el cual aquella falta.

Los elementos de configuración proporcionan los campos de **`eventData`**

Nombre del campo	Tipo de entrada	Requisito	Descripción
eventData	-	Obligatoria	Los elementos de configuración proporcionan los campos de eventData .

Nombre del campo	Tipo de entrada	Requisito	Descripción
• configurationItemVersion	cadena	Opcional	La versión del elemento de configuración desde su origen.
• configurationItemCaptureHora	cadena	Opcional	La hora en que se inició el registro de configuración.
• configurationItemStatus	cadena	Opcional	El estado del elemento de configuración. Los valores válidos son `OK`, `ResourceDiscovered`, `ResourceNotRecorded`, `ResourceDeleted` y `ResourceDeletedNotRecorded`.
• accountId	cadena	Opcional	El Cuenta de AWS identificador de 12 dígitos asociado al recurso.
• resourceType	cadena	Opcional	El tipo de AWS recurso. Para obtener más información sobre los tipos de recursos válidos, consulta ConfigurationItemla referencia de la AWS Config API.

Nombre del campo	Tipo de entrada	Requisito	Descripción
• resourceId	cadena	Opcional	El ID del recurso (por ejemplo, sg-*xxxxxx*).
• resourceName	cadena	Opcional	El nombre personalizado del recurso, si está disponible.
• arn	cadena	Opcional	El Nombre de recurso de Amazon (ARN) asociado al recurso.
• awsRegion	cadena	Opcional	El Región de AWS lugar donde reside el recurso.
• availabilityZone	cadena	Opcional	La zona de disponibilidad asociada al recurso.
• resourceCreationTime	cadena	Opcional	La marca de tiempo en la que se creó el recurso.
• configuración	JSON	Opcional	La descripción de la configuración del recurso.
• supplementaryConfiguration	JSON	Opcional	Atributos de configuración que se AWS Config devuelven para determinados tipos de recursos para complementar la información devuelta para el parámetro de configuración.

Nombre del campo	Tipo de entrada	Requisito	Descripción
• relatedEvents	cadena	Opcional	Una lista de identific adores de CloudTrail eventos.
• relationships	-	Opcional	Una lista de AWS recursos relaciona dos.
• • name	cadena	Opcional	El tipo de relación con el recurso relaciona do.
• • resourceType	cadena	Opcional	El tipo del recurso relacionado.
• • resourceId	cadena	Opcional	El ID del recurso relacionado (por ejemplo, sg-*xxxxxx*).
• • resourceName	cadena	Opcional	El nombre personali zado del recurso relacionado, si está disponible.
• etiquetas	JSON	Opcional	Una asignación de las etiquetas de valores de claves asociadas con el recurso.

En el siguiente ejemplo, se muestra la jerarquía de los elementos de esquema que coinciden con los de los registros de elementos de configuración.

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
```

```
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
       ],
     "tags": {
       JSON
     }
    }
  }
}
```

Cree un almacén de datos de eventos para eventos ajenos a AWS

Puede crear un banco de datos de eventos para incluir eventos ajenos a AWSél y, a continuación, usar CloudTrail Lake para buscar, consultar y analizar los datos que se registran en sus aplicaciones.

Puede usar las integraciones de CloudTrail Lake para registrar y almacenar datos de actividad de AWS los usuarios desde fuera o desde cualquier fuente en sus entornos híbridos, como aplicaciones internas o SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores.

Cuando crea un almacén de datos de eventos para una integración, también crea un canal y asocia una política de recursos al canal.

CloudTrail Los almacenes de datos de eventos de Lake conllevan cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Para crear un almacén de datos de eventos para eventos ajenos a AWS

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija Create event data store (Crear almacén de datos de eventos).
4. En la página Configure event data store (Configurar el almacén de datos de eventos), en General details (Detalles generales), ingrese un nombre para el almacén de datos de eventos. El nombre es obligatorio.
5. Elija la Opción de precios que desee usar para el almacén de datos de eventos. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

   Están disponibles las siguientes opciones:

   - Precio de retención ampliable por un año: en general se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de

hasta 10 años. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin cargo adicional en los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado. Esta es la opción predeterminada.

- Periodo de retención predeterminado: 366 días.
- Periodo máximo de retención: 3653 días.

- Precio de retención ampliable por un año: se recomienda si prevé incorporar más de 25 TB de datos de eventos al mes y desea un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional.
  - Periodo de retención predeterminado: 2557 días.
  - Periodo máximo de retención: 2557 días.

6. Especifique un periodo de retención para el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

   CloudTrail Lake determina si se debe retener un evento comprobando si el `eventTime` evento se encuentra dentro del período de retención especificado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando `eventTime` tengan más de 90 días.

7. (Opcional) Para habilitar el cifrado mediante AWS Key Management Service, selecciona Usar el mío AWS KMS key. Elija Nuevo para que se AWS KMS key cree una para usted, o bien elija Existente para usar una clave KMS existente. En Introducir un alias de KMS, especifique un alias en el formato `alias/` *`MyAliasName`*. El uso de su propia clave de KMS requiere que edite la política de claves de KMS para permitir el cifrado y el descifrado de los CloudTrail registros. Para obtener más información, consulteConfigurar políticas de clave de AWS KMS para CloudTrail. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   El uso de su propia clave KMS conlleva AWS KMS costes de cifrado y descifrado. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

> **Note**
>
> Para habilitar el AWS Key Management Service cifrado en un almacén de datos de eventos de la organización, debe usar una clave KMS existente para la cuenta de administración.

8. (Opcional) Si desea realizar consultas con los datos de su evento mediante Amazon Athena, elija Habilitar en Federación de consultas de Lake. La federación le permite ver los metadatos asociados al almacén de datos de eventos en el catálogo de datos de AWS Glue y ejecutar consultas SQL con los datos de eventos en Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federar un almacén de datos de eventos.

   Para habilitar la federación de consultas de Lake, seleccione Habilitar y, a continuación, haga lo siguiente:

   a. Elija si desea crear un nuevo rol o utilizar un rol de IAM existente. AWS Lake Formation utiliza este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente un rol con los permisos necesarios. Si elige un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

   b. Si va a crear un rol nuevo, introduzca un nombre para identificarlo.

   c. Si está utilizando un rol existente, elija el rol que desea usar. El rol debe existir en su cuenta.

9. (Opcional) En la sección Tags (Etiquetas), puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su almacén de datos de eventos y controlar el acceso a él. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo utilizar las etiquetas AWS, consulte Etiquetar AWS los recursos en. Referencia general de AWS

10. Elija Next (Siguiente) para configurar el almacén de datos de eventos.

11. En la página Choose events (Elegir eventos), elija Events from integrations (Eventos de integraciones).

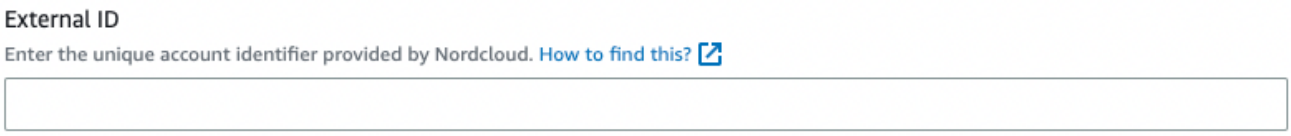
12. En Events from integration (Eventos de integraciones), elija el origen para enviar eventos al almacén de datos de eventos.
13. Proporcione un nombre para identificar el canal de la integración. El nombre puede tener entre 3 y 128 caracteres. Solo se permiten letras, números, puntos, guiones medios y guiones bajos.
14. En Resource policy (Política de recursos), configure la política de recursos para el canal de la integración. Las políticas de recursos son documentos de política JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso y bajo qué condiciones. Las cuentas definidas como entidades principales en la política de recursos pueden llamar a la API `PutAuditEvents` para enviar eventos al canal. El propietario del recurso tiene acceso implícito al recurso si la política de IAM permite la acción `cloudtrail-data:PutAuditEvents`.

    La información necesaria para la política está determinada por el tipo de integración. Para una integración de Direction, agrega CloudTrail automáticamente los ID de AWS cuenta del socio y requiere que introduzcas el ID externo único proporcionado por el socio. Para la integración de una solución, debe especificar al menos un identificador de AWS cuenta como principal y, si lo desea, puede introducir un identificador externo para evitar confusiones con el agente.

    > **Note**
    >
    > Si no se crea una política de recursos para el canal, solo el propietario del canal puede llamar a la API `PutAuditEvents` del canal.

    a. Para una integración directa, ingrese el ID externo proporcionado por el socio. El socio de integración proporciona un ID externo único, como un ID de cuenta o una cadena generada de forma aleatoria, que se utiliza en la integración para evitar un suplente confuso. Es responsabilidad del socio crear y proporcionar un ID externo único.

    Puede elegir How to find this? (¿Cómo encontrar esto?) para ver la documentación del socio que describe cómo encontrar el ID externo.



> **Note**
>
> Si la política de recursos incluye un ID externo, todas las llamadas a la API `PutAuditEvents` deben incluir el ID externo. Sin embargo, si la política no define un ID externo, el socio aún puede llamar a la API `PutAuditEvents` y especificar un parámetro `externalId`.

b. Para integrar una solución, seleccione Añadir AWS cuenta para especificar cada identificador de AWS cuenta que desee añadir como principal en la política.

15. Elija Next (Siguiente) para revisar las opciones seleccionadas.
16. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) para realizar cambios en una sección. Cuando esté listo para crear el almacén de datos de eventos, elija Create event data store (Crear almacén de datos de eventos).
17. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.
18. Proporcione el nombre de recurso de Amazon (ARN) del canal a la aplicación asociada. Las instrucciones para proporcionar el ARN del canal a la aplicación asociada se encuentran en el sitio web de documentación de socios. Para obtener más información, elija el enlace Learn more (Más información) del socio en la pestaña Available sources (Orígenes disponibles) de la página Integrations (Integraciones) para abrir la página del socio en AWS Marketplace.

El almacén de datos de eventos comienza a incorporar los eventos de los socios CloudTrail a través del canal de integración cuando usted, el socio o las aplicaciones del socio llaman a la `PutAuditEvents` API del canal.

Copiar eventos de registro de seguimiento en un almacén de datos de eventos

Puede copiar los eventos del sendero a un banco de datos de eventos de CloudTrail Lake para crear una point-in-time instantánea de los eventos registrados en el sendero. Copiar los eventos de un registro de seguimiento no interfiere con la capacidad del registro de seguimiento para registrar eventos y no modifica el registro de seguimiento de ninguna manera.

Puede copiar los eventos de los senderos a un banco de datos de eventos existente configurado para CloudTrail eventos, o puede crear un nuevo banco de datos de CloudTrail eventos y elegir la

opción Copiar los eventos de los senderos como parte de la creación del banco de datos de eventos. Para obtener más información acerca de cómo copiar eventos de registros de seguimiento en un almacén de datos de eventos existente, consulte Copiar eventos de registro de seguimiento a un almacén de datos de eventos existente. Para obtener más información acerca de la creación de un nuevo almacén de datos de eventos, consulte Cree un banco de datos de CloudTrail eventos para eventos.

Si va a copiar los eventos de registro de seguimiento en el almacén de datos de eventos de una organización, debe utilizar la cuenta de administración de la organización. No puede copiar los eventos de registro de seguimiento con la cuenta del administrador delegado de una organización.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Cuando copias los eventos de los senderos a un banco de datos de eventos de CloudTrail Lake, incurres en cargos en función de la cantidad de datos sin comprimir que ingiera el almacén de datos de eventos.

Al copiar los eventos de los senderos en CloudTrail Lake, se CloudTrail descomprimen los registros almacenados en formato gzip (comprimido) y, a continuación, se copian los eventos contenidos en los registros en el almacén de datos de eventos. El tamaño de los datos sin comprimir podría ser mayor que el tamaño real del almacenamiento de S3. Para obtener una estimación general del tamaño de los datos sin comprimir, puede multiplicar por 10 el tamaño de los registros del bucket de S3.

Puede reducir los costos especificando un intervalo de tiempo más reducido para los eventos copiados. Si planea usar solo el almacén de datos de eventos para consultar los eventos copiados, puede desactivar la ingesta de eventos para evitar generar cargos por eventos futuros. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

Escenarios

En la siguiente tabla, se describen algunos escenarios habituales para copiar eventos de registros de seguimiento y cómo seguir cada uno de ellos mediante la consola.

Escenario	¿Cómo puedo lograr esto en la consola?
Analiza y consulta los eventos históricos de los senderos de CloudTrail Lake sin ingerir nuevos eventos	Cree un nuevo almacén de datos de eventos y seleccione la opción Copiar eventos de registros de seguimiento como parte de la creación del almacén de datos de eventos. Al crear el almacén de datos de eventos, desmarque Incorporar eventos (paso 15 del procedimiento) para garantizar que el almacén de datos de eventos contenga solo los eventos históricos del registro de seguimiento y no los eventos futuros.
Sustituya su sendero actual por un almacén de datos de eventos de CloudTrail Lake	Cree un almacén de datos de eventos con los mismos selectore s de eventos que el registro de seguimiento para asegurarse de que el almacén de datos de eventos tenga la misma cobertura que el registro de seguimiento. Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de fecha para los eventos copiados que sea anterior a la creación del almacén de datos de eventos. Después de crear el almacén de datos de eventos, puede desactivar el registro del registro de seguimiento para evitar cargos adicionales.

Temas

- Consideraciones para copiar eventos de registros de seguimiento
- Permisos necesarios para copiar eventos de registro de seguimiento
- Copiar eventos de registro de seguimiento a un almacén de datos de eventos existente
- Detalles de la copia del evento

Consideraciones para copiar eventos de registros de seguimiento

Tenga en cuenta los siguientes factores al copiar eventos de registro de seguimiento.

- Al copiar los eventos de las rutas, CloudTrail utiliza la operación de la `GetObject`API de S3 para recuperar los eventos de las rutas del depósito de S3 de origen. Hay algunas clases de

almacenamiento archivado de S3, como S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts y S3 Intelligent-Tiering Deep Archive, a las que no puede acceder con `GetObject`. Para copiar los eventos de registros de seguimiento almacenados en estas clases de almacenamiento archivado, primero debe restaurar una copia mediante la operación `RestoreObject` de S3. Para obtener información sobre la restauración de objetos archivados, consulte Restauración de objetos archivados en la Guía del usuario de Amazon S3.

- Al copiar los eventos de seguimiento a un banco de datos de eventos, CloudTrail copia todos los eventos de seguimiento, independientemente de la configuración de los tipos de eventos del banco de datos de eventos de destino, de los selectores de eventos avanzados o Región de AWS.
- Antes de copiar los eventos del registro de seguimiento a un almacén de datos de eventos existente, asegúrese de que la opción de precios y el periodo de retención del almacén de datos de eventos estén configurados adecuadamente para su caso de uso.
  - Opción de precios: la opción de precios determina el costo de la incorporación y el almacenamiento de los eventos. Para obtener más información sobre las opciones de precios, consulte Precios de AWS CloudTrail y Opciones de precios del almacén de datos de eventos.
  - Período de retención: el período de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos del evento. CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Para determinar el período de retención adecuado, tome la suma del evento más antiguo que desea copiar en días y el número de días que desea conservar los eventos en el almacén de datos del evento (período de retención = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.
- Si está copiando eventos de registros de seguimiento en un almacén de datos de eventos para investigarlos y no desea incorporar ningún evento futuro, puede detener la incorporación en el almacén de datos de eventos. Al crear el almacén de datos de eventos, desmarque la opción Incorporar eventos (paso 15 del procedimiento) para garantizar que el almacén de datos de eventos contenga solo los eventos históricos del registro de seguimiento y no los eventos futuros.
- Antes de copiar los eventos de registro de seguimiento, desactive cualquier lista de control de acceso (ACL) adjunta al bucket de S3 de origen y actualice la política de buckets de S3 para el almacén de datos de eventos de destino. Para obtener más información sobre la actualización de la política de buckets de S3, consulte Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento. Para obtener más información sobre cómo desactivar las ACL, consulte

Control de la propiedad de los objetos y desactivación de las ACL del bucket en la Guía del usuario de Amazon S3.

- CloudTrail solo copia los eventos de seguimiento de los archivos de registro comprimidos con Gzip que se encuentran en el depósito S3 de origen. CloudTrail no copia los eventos de seguimiento de archivos de registro sin comprimir ni de archivos de registro que se comprimieron con un formato distinto de Gzip.
- Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de tiempo para los eventos copiados que sea anterior a la creación del almacén de datos de eventos.
- De forma predeterminada, CloudTrail solo copia CloudTrail los eventos contenidos en el prefijo del bucket de S3 y los `CloudTrail` prefijos incluidos en el prefijo, y no comprueba los `CloudTrail` prefijos de otros servicios. AWS Si desea copiar los CloudTrail eventos incluidos en otro prefijo, debe elegir el prefijo al copiar los eventos de seguimiento.
- Para copiar los eventos de los registros de seguimiento en el almacén de datos de eventos de una organización, debe utilizar su cuenta de administración. La cuenta del administrador delegado no puede copiar los eventos de registro de seguimiento en el almacén de datos de eventos de una organización.

Permisos necesarios para copiar eventos de registro de seguimiento

Antes de copiar los eventos de seguimiento, asegúrese de tener todos los permisos necesarios para su función de IAM. Solo necesita actualizar los permisos del rol de IAM si elige un rol de IAM existente para copiar los eventos de registro de seguimiento. Si decide crear un nuevo rol de IAM, CloudTrail proporciona todos los permisos necesarios para el rol.

Si el depósito de S3 de origen utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS CloudTrail permita descifrar los datos del depósito. Si el bucket de S3 de origen usa varias claves KMS, debe actualizar la política de cada clave CloudTrail para poder descifrar los datos del bucket.

Temas

- Permisos de IAM para copiar eventos de registro de seguimiento
- Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento
- Política de claves KMS para descifrar datos en el bucket de S3 de origen

Permisos de IAM para copiar eventos de registro de seguimiento

Al copiar eventos de registro de seguimiento, tiene la opción de crear un nuevo rol de IAM o utilizar uno existente. Al elegir una nueva función de IAM, CloudTrail crea una función de IAM con los permisos necesarios y no es necesario que realice ninguna otra acción por su parte.

Si elige un rol existente, asegúrese de que las políticas del rol de IAM permitan CloudTrail copiar los eventos de seguimiento del bucket de S3 de origen. Esta sección proporciona ejemplos de las políticas de confianza y de permisos necesarias para el rol de IAM.

En el siguiente ejemplo, se proporciona la política de permisos, que permite CloudTrail copiar los eventos de seguimiento del depósito de S3 de origen. Sustituya *myBucketNamemyAccountID*, *region*, *prefijo* e *eventDataStoreId* por los valores adecuados para su configuración. El *myAccountID* es el identificador de AWS cuenta utilizado para CloudTrail Lake, que puede no coincidir con el identificador de cuenta del bucket de S3. AWS

Sustituya *key-region*, *keyAccountID* y *keyID* por los valores de la clave de KMS utilizada para cifrar el bucket de S3 de origen. Puede omitir la instrucción `AWSCloudTrailImportKeyAccess` si el bucket de S3 de origen no utiliza una clave de KMS para el cifrado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
```

```
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

El siguiente ejemplo proporciona la política de confianza de IAM, que permite asumir una función de IAM CloudTrail para copiar los eventos de seguimiento del bucket de S3 de origen. Sustituya *myAccountID*, *region* y *eventDataStoreArn* por los valores adecuados para su configuración. El *Cuenta de AWS myAccountID* es el identificador utilizado para CloudTrail Lake, que puede no coincidir con el identificador de cuenta del bucket de S3. AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
```

```
        }
      }
    }
  ]
}
```

Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento

De forma predeterminada, los buckets y los objetos de Amazon S3 son privados. Solo el propietario del recurso (la cuenta de AWS que creó el bucket) puede tener acceso al bucket y a los objetos que contiene. El propietario del recurso puede conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Antes de copiar los eventos de seguimiento, debe actualizar la política de buckets de S3 CloudTrail para permitir copiar los eventos de trail del bucket de S3 de origen.

Puede añadir la siguiente declaración a la política de buckets de S3 para conceder estos permisos. Sustituya *RoLearn* y por *myBucketName*los valores adecuados para su configuración.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

Política de claves KMS para descifrar datos en el bucket de S3 de origen

Si el depósito de S3 de origen utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS proporcione CloudTrail `kms:GenerateDataKey` los permisos necesarios

para copiar los eventos de seguimiento de un depósito de S3 con el cifrado SSE-KMS activado. `kms:Decrypt` Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave. La actualización de la política de claves de KMS CloudTrail permite descifrar los datos del bucket S3 de origen, realizar comprobaciones de validación para garantizar que los eventos cumplen con los CloudTrail estándares y copiar los eventos en el almacén de datos de eventos de CloudTrail Lake.

El siguiente ejemplo proporciona la política de claves de KMS, que CloudTrail permite descifrar los datos del bucket de S3 de origen. Sustituya *RoLearn myBucketName*, *eventDataStoremyAccountID, region e Id* por los valores adecuados para su configuración. El *myAccountID* es el identificador de AWS cuenta utilizado para CloudTrail Lake, que puede no coincidir con el identificador de cuenta del bucket de S3. AWS

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Copiar eventos de registro de seguimiento a un almacén de datos de eventos existente

Utilice el siguiente procedimiento para copiar los eventos de registros de seguimiento en un almacén de datos de eventos existente. Para obtener información sobre cómo crear un nuevo almacén de datos de eventos, consulte Cree un banco de datos de CloudTrail eventos para eventos.

> **Note**
>
> Antes de copiar los eventos del registro de seguimiento a un almacén de datos de eventos existente, asegúrese de que la opción de precios y el periodo de retención del almacén de datos de eventos estén configurados adecuadamente para su caso de uso.
>
> - Opción de precios: la opción de precios determina el costo de la incorporación y el almacenamiento de los eventos. Para obtener más información sobre las opciones de precios, consulte Precios de AWS CloudTrail y Opciones de precios del almacén de datos de eventos.
> - Período de retención: el período de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos del evento. CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Para determinar el período de retención adecuado, tome la suma del evento más antiguo que desea copiar en días y el número de días que desea conservar los eventos en el almacén de datos del evento (período de retención = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.

Para copiar eventos de registros de seguimiento en un almacén de datos de eventos

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija Copy trail events (Copiar eventos de registros de seguimiento).
4. En la página Copy trail events (Copiar eventos de registro de seguimiento), elija el registro de seguimiento que desea copiar para Event source (Origen del evento). De forma predeterminada, CloudTrail solo copia CloudTrail los eventos contenidos en el `CloudTrail` prefijo del bucket

de S3 y los prefijos incluidos en el `CloudTrail` prefijo, y no comprueba los prefijos de otros servicios. AWS Si desea copiar CloudTrail los eventos contenidos en otro prefijo, elija Introducir el URI de S3 y, a continuación, elija Examinar S3 para buscar el prefijo. Si el depósito de S3 de origen de la ruta utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS CloudTrail permita descifrar los datos. Si el bucket de S3 de origen utiliza varias claves KMS, debe actualizar la política de cada clave CloudTrail para poder descifrar los datos del bucket. Para obtener más información sobre la actualización de la política de claves KMS, consulte Política de claves KMS para descifrar datos en el bucket de S3 de origen.

La política del bucket de S3 debe permitir el CloudTrail acceso a la copia de los eventos de seguimiento de su bucket de S3. Para obtener más información sobre la actualización de la política de buckets de S3, consulte Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento.

5. En Especificar un rango de tiempo de eventos, elija el rango de tiempo para copiar los eventos. CloudTrail comprueba el prefijo y el nombre del archivo de registro para comprobar que el nombre contiene una fecha entre la fecha de inicio y la de finalización elegidas antes de intentar copiar los eventos de la ruta. Puede elegir un intervalo relativo o un intervalo absoluto. Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de tiempo que sea anterior a la creación del almacén de datos de eventos.

   > **Note**
   >
   > CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Por ejemplo, si el período de retención de un almacén de datos de eventos es de 90 días, no CloudTrail copiará ningún evento de ruta que tenga una `eventTime` antigüedad superior a 90 días.

   - Si eliges Rango relativo, puedes elegir copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un rango personalizado. CloudTrail copia los eventos registrados en el período de tiempo elegido.
   - Si elige Rango absoluto, puede elegir una fecha de inicio y finalización específica. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y finalización elegidas.

6. Para Delivery location (Lugar de entrega), elija el almacén de datos de eventos de destino en la lista desplegable.

7. Para Permissions (Permisos), elija una de las siguientes opciones de rol de IAM. Si elige un rol de IAM existente, verifique que la política de roles de IAM proporcione los permisos necesarios. Para obtener más información acerca de la actualización de los permisos de rol de IAM, consulte Permisos de IAM para copiar eventos de registro de seguimiento.

   - Elija Create a new role (recommended) (Crear un nuevo rol [recomendado]) para crear un nuevo rol de IAM. En Enter IAM role name (Ingresar nombre del rol de IAM), escriba un nombre único para el rol. CloudTrail crea automáticamente los permisos necesarios para este nuevo rol.
   - Elija Usar un ARN de rol de IAM personalizado para usar un rol de IAM personalizado que no aparezca en la lista. En Enter IAM role ARN (Ingresar ARN del rol de IAM), escriba el ARN de IAM.
   - Elija un rol de IAM existente de la lista desplegable.
8. Elija Copy events (Copiar eventos).
9. Se le solicitará que confirme. Cuando esté listo para confirmar, elija Copy trail events to Lake (Copiar eventos de registro de seguimiento en Lake) y, a continuación, Copy events (Copiar eventos).
10. En la página Copy details (Detalles de la copia), puede observar el estado de la copia y revisar cualquier error. Cuando se completa la copia de un evento de registro de seguimiento, el campo Copy status (Estado de la copia) se establece en Completed (Completa), si no hubo errores, o Failed (Error), si hubo errores.

    > **Note**
    >
    > Los detalles que aparecen en la página de detalles de la copia del evento no aparecen en tiempo real. Los valores reales de detalles, como los prefijos copiados, pueden ser superiores a los que se muestran en la página. CloudTrail actualiza los detalles de forma incremental a lo largo del texto del evento.

11. Si Copy status (Estado de la copia) está establecido en Failed (Error), corrija los errores que aparecen en Copy failures (Errores de la copia) y, a continuación, elija Retry copy (Volver a copiar). Al volver a intentar una copia, la CloudTrail reanuda en la ubicación en la que se produjo el error.

Para obtener más información sobre cómo ver los detalles de la copia de un evento de registro de seguimiento, consulte Detalles de la copia del evento.

Detalles de la copia del evento

Después de que se inicie la copia de un evento de registro de seguimiento, puede ver los detalles de la copia del evento, incluido el estado de la copia, e información sobre cualquier error de la copia.

> **Note**
>
> Los detalles que aparecen en la página de detalles de la copia del evento no aparecen en tiempo real. Los valores reales de detalles, como los prefijos copiados, pueden ser superiores a los que se muestran en la página. CloudTrail actualiza los detalles de forma incremental a lo largo de la copia del evento.

Para acceder a la página de detalles de copia del evento

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación de la izquierda, en Lake, seleccione Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. Elija la copia del evento en la sección Event copy status (Estado de la copia del evento).

Detalles de la copia

En Copy details (Detalles de la copia), puede ver los siguientes detalles sobre la copia del evento de registro de seguimiento.

- Event log S3 location (Ubicación de S3 del registro de eventos): la ubicación del bucket de S3 de origen que contiene los archivos de registros de eventos del registro de seguimiento.
- Copy ID (ID de la copia): el ID de la copia.
- Prefixes copied (Prefijos copiados): representa el número de prefijos de S3 copiados. Durante la copia de un evento de registro de seguimiento, CloudTrail copia los eventos en los archivos de registros del registro de seguimiento que se almacenan en los prefijos.
- Copy status (Estado de la copia): el estado de la copia.
  - Initializing (Inicio): el estado inicial que se muestra cuando comienza la copia del evento de registro de seguimiento.
  - In progress (En curso): indica que la copia del evento de registro de seguimiento está en progreso.

> **Note**
>
> No puede copiar eventos de registro de seguimiento si otra copia del evento de registro de seguimiento tiene el estado In progress (En curso). Para detener una copia de un evento de registro de seguimiento, seleccione Stop copy (Detener copia).

  - Stopped (Detenida): indica que ocurrió la acción Stop copy (Detener copia). Para volver a realizar la copia de un evento de registro de seguimiento, seleccione Retry copy (Volver a copiar).
  - Failed (Error): se ha completado la copia, pero algunos eventos de registro de seguimiento no se han podido copiar. Revise los mensajes de error en Copy failures (Errores de la copia). Para volver a realizar la copia de un evento de registro de seguimiento, seleccione Retry copy (Volver a copiar). Cuando vuelva a realizar la copia, CloudTrail reanuda la copia en la ubicación en la que se produjo el error.
  - Completed (Completa): la copia se completó sin errores. Puede consultar los eventos de registro de seguimiento copiados en el almacén de datos de eventos.
- Created time (Hora de creación): indica cuándo comenzó la copia del evento de registro de seguimiento.
- Finish time (Hora de finalización): indica cuándo se completó o se detuvo la copia del evento de registro de seguimiento.

Errores de la copia

En Copy failures (Errores de la copia), puede revisar la ubicación del error, el mensaje de error y el tipo de error de cada error de la copia. Dentro de las razones más comunes de los errores se incluye si un prefijo de S3 contenía un archivo sin comprimir o un archivo entregado por un servicio que no fuera CloudTrail. Otra posible causa de error se relaciona con los problemas de acceso. Por ejemplo, si el bucket de S3 del almacén de datos de eventos no concedió acceso a CloudTrail para importar los eventos, obtiene un error de `AccessDenied`.

Para cada error de la copia, revise la siguiente información de error.

- Error location (Ubicación del error): indica la ubicación en el bucket de S3 donde ocurrió el error. Si se produjo un error porque el bucket de S3 de origen contenía un archivo sin comprimir, Error location (Ubicación del error) incluye el prefijo en el que se encuentra ese archivo.

- Error message (Mensaje de error): brinda una explicación de la razón por la que se produjo el error.
- Error type (Tipo de error): proporciona el tipo de error. Por ejemplo, un tipo de error de `AccessDenied` indica que el error se ha producido debido a un problema de permisos. Para obtener más información sobre los permisos necesarios para copiar eventos de registro de seguimiento, consulte Permisos necesarios para copiar eventos de registro de seguimiento.

Después de resolver los errores, seleccione Retry copy (Volver a copiar). Cuando vuelva a realizar la copia, CloudTrail reanuda la copia en la ubicación en la que se produjo el error.

Administración de los ciclos de vida de los almacenes de datos de eventos

A continuación, se detallan las etapas del ciclo de vida de un almacén de datos de eventos:

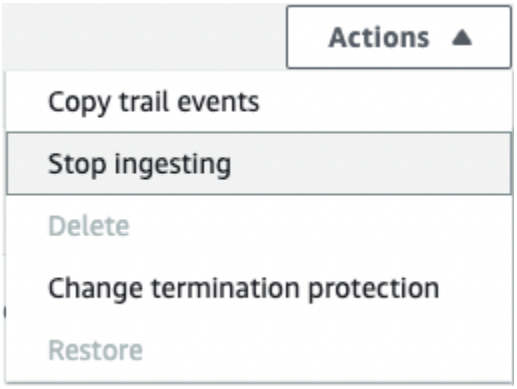
- `CREATED`: un estado a corto plazo que indica que se ha creado el almacén de datos de eventos.
- `ENABLED`: el almacén de datos de eventos está activo e ingiere eventos. Puede ejecutar consultas y copiar eventos de registro de seguimiento en el almacén de datos de eventos.
- `STARTING_INGESTION`: un estado a corto plazo que indica que el almacén de datos de eventos comenzará a ingerir eventos en vivo.
- `STOPPING_INGESTION`: un estado a corto plazo que indica que el almacén de datos de eventos dejará de ingerir eventos en vivo.
- `STOPPED_INGESTION`: el almacén de datos de eventos no está ingiriendo eventos en vivo. Todavía puede ejecutar consultas en cualquier evento que ya esté en el almacén de datos de eventos y copiar los eventos de registros de seguimiento en el almacén de datos de eventos.
- `PENDING_DELETION`: el estado del almacén de datos de eventos era `ENABLED` o `STOPPED_INGESTION` y se ha eliminado, pero está dentro del periodo de espera de 7 días antes de la eliminación permanente. No puede ejecutar consultas en el almacén de datos de eventos ni puede llevar a cabo ninguna operación en el almacén de datos de eventos, excepto la restauración.

Solo puede eliminar un almacén de datos de eventos si la protección contra terminación y federación está desactivada. Protección contra terminación evita que el almacén de datos de eventos se elimine accidentalmente. De forma predeterminada, la protección contra la terminación está activada en los almacenes de datos de eventos. Federación le permite consultar los datos del almacén de datos de eventos en Athena y está desactivada de forma predeterminada.

Después de eliminar un almacén de datos de eventos, este permanece en el estado `PENDING_DELETION` durante 7 días antes de su eliminación definitiva. Puede restaurar un almacén de datos de eventos durante el periodo de espera de 7 días. Mientras está en estado `PENDING_DELETION`, un almacén de datos de eventos no está disponible para consultas y no se pueden realizar otras operaciones en el almacén de datos de eventos, excepto operaciones de restauración. Un almacén de datos de eventos que está pendiente de eliminación no ingiere eventos ni genera costos.

Acciones disponibles en los almacenes de datos de eventos

Para eliminar o restaurar un almacén de datos de eventos, copiar eventos de registros de seguimiento, iniciar o detener la incorporación de eventos o activar o desactivar la protección contra la terminación de un almacén de datos de eventos, utilice los comandos del menú Acciones de la página de detalles del almacén de datos de eventos.



La opción de copiar eventos de seguimiento solo está disponible en los almacenes de datos de eventos que contienen eventos CloudTrail de administración y datos. Las opciones Iniciar y detener la ingesta solo están disponibles en los bancos de datos de eventos que contienen CloudTrail eventos (eventos de administración y datos) o elementos de AWS Config configuración.

Actualización de un almacén de datos de eventos

En esta sección, se describe cómo actualizar la configuración de un almacén de datos de eventos mediante la AWS Management Console. Para obtener información sobre cómo actualizar un banco de datos de eventos mediante el AWS CLI, consulte. Actualizar un almacén de datos de eventos con la AWS CLI

Para actualizar un almacén de datos de eventos

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.

2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos que desea actualizar. Esta acción abre la página de detalles del almacén de datos de eventos.
4. En Detalles generales, elija Editar para cambiar la siguiente configuración:

   - Nombre del almacén de datos de eventos: cambie el nombre que identifica el almacén de datos de eventos.
   - Opción de precios: en el caso de los almacenes de datos de eventos que utilizan la opción Precios de retención de siete años, puede optar por utilizar en su lugar Precio de retención ampliable por un año. Recomendamos un precio de retención ampliable por un año para los almacenes de datos de eventos que incorporen menos de 25 TB de datos de eventos al mes. También recomendamos precios de retención ampliables por un año si busca un periodo de retención flexible de hasta 10 años. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

     > **Note**
     >
     > No puede cambiar la opción de precios de los almacenes de datos de eventos que utilizan Precios de retención ampliables por un año. Si quiere usar Precio de retención de siete años, detenga la incorporación en el almacén de datos de eventos actual. A continuación, cree un nuevo almacén de datos de eventos con la opción Precios de retención de siete años.

   - Periodo de retención: cambie el periodo de retención del almacén de datos de eventos. El periodo de retención determina cuánto tiempo se conservan los datos del evento en el almacén de datos de eventos. Los periodos de retención pueden oscilar entre 7 y 3653 días (unos 10 años) para la opción Precios de retención ampliables por un año, o entre 7 días y 2557 días (unos siete años) para la opción Precios de retención por siete años.

     > **Note**
     >
     > Si reduce el período de retención de un almacén de datos de eventos, CloudTrail se eliminarán los eventos que tengan un período de retención `eventTime` anterior al nuevo. Por ejemplo, si el período de retención anterior era de 365 días y lo reduces a 100 días, CloudTrail se eliminarán los eventos con una `eventTime` antigüedad superior a 100 días.

- Cifrado: para cifrar su almacén de datos de eventos con su propia clave de KMS, seleccione Usar mi propia AWS KMS key. De forma predeterminada, todos los eventos de un almacén de datos de eventos se cifran con CloudTrail. Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS .

  > **Note**
  >
  > Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar.

- Seleccione Incluir la región actual en el almacén de datos de eventos para incluir solo los eventos registrados en la Región de AWS actual. Si no elige esta opción, su almacén de datos de eventos incluirá eventos de todas las regiones.
- Para que su almacén de datos de eventos recopile eventos de todas las cuentas de una AWS Organizations organización, seleccione Activar para todas las cuentas de mi organización. Esta opción solo está disponible si ha iniciado sesión con la cuenta de administración de su organización y el tipo de evento del banco de datos de CloudTraileventos es eventos o elementos de configuración.

Cuando haya finalizado, elija Guardar cambios.

5. En Federación de consultas de Lake, seleccione Editar para activar o desactivar la federación de consultas de Lake. Al habilitar la federación de consultas de Lake, puede ver los metadatos del almacén de datos de su evento en el catálogo de AWS Glue datos y ejecutar consultas SQL en los datos del evento mediante Amazon Athena. Al deshabilitar la federación de consultas de Lake, se deshabilita la integración con AWS Glue AWS Lake Formation, y Amazon Athena. Tras deshabilitar la federación de consultas de Lake, ya no podrá consultar sus datos en Athena. Al deshabilitar la federación, no se elimina ningún dato de CloudTrail Lake y puede seguir realizando consultas en Lake. CloudTrail

   Para habilitar la federación, haga lo siguiente:

   a. Seleccione Habilitar.

   b. Elija si desea crear un nuevo rol de IAM, o utilizar un rol existente. Al crear un rol nuevo, crea CloudTrail automáticamente un rol con los permisos necesarios. Si utiliza un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.

   c. Si está creando un rol de IAM nuevo, ingrese un nombre para el rol.

d. Si elige un rol de IAM existente, elija el rol que quiere usar. El rol debe existir en su cuenta.

Cuando haya terminado, seleccione Guardar cambios.

6. Edite cualquier configuración adicional para su tipo de evento.

Tipo de evento	Ajustes editables
CloudTrail eventos	Puede editar los siguientes ajustes para CloudTrail los eventos: • Para cambiar los eventos que registra tu almacén de datos de eventos, selecciona Editar en CloudTrail eventos. • En Eventos de administración, elija Editar para cambiar la configuración de registro de eventos de administración. Para obtener más información, consulte Registro de eventos de administración con la AWS Management Console (Paso 3). • En Eventos de datos, elija Editar para cambiar la configuración de los eventos de datos. Puede elegir qué tipos de eventos de datos quiere registrar y elegir la plantilla de selección de registros que quiere usar. Para obtener más información, consulte Actualización de un almacén de datos de eventos existente para registrar los eventos de datos en el AWS Management Console. Cuando haya finalizado, elija Guardar cambios.
Eventos de integración	En Integraciones, elija su integración. Luego elija Editar, para cambiar la siguiente configuración:

Tipo de evento	Ajustes editables
	• En Detalles de la integración, cambie el nombre que identifica el canal de su integración. • En Ubicación de entrega del evento, elija el destino para sus eventos. • En Resource policy (Política de recursos) , configure la política de recursos para el canal de la integración. Cuando haya finalizado, elija Guardar cambios. Para obtener más información sobre estas opciones, consulte Creación de una integración con un origen de eventos externo a AWS.

7. Para agregar, cambiar o eliminar etiquetas, seleccione Editar en Etiquetas. Puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar, ordenar su almacén de datos de eventos y controlar el acceso a él. Cuando haya finalizado, elija Guardar cambios.

Detener e iniciar la incorporación de eventos

De forma predeterminada, los almacenes de datos de eventos están configurados para ingerir eventos. Puedes impedir que un banco de datos de eventos ingiera eventos mediante la consola o AWS CLI las API.

Las opciones para iniciar la ingesta y detener la ingesta solo están disponibles en los almacenes de datos de eventos que contienen CloudTrail eventos (eventos de administración y datos) o AWS Config elementos de configuración.

Al detener la ingesta en un almacén de datos de eventos, el estado del almacén de datos de eventos cambia a `STOPPED_INGESTION`. Todavía puede ejecutar consultas en cualquier evento que ya esté en el almacén de datos de eventos. También puede copiar los eventos de seguimiento al banco de datos de eventos (si solo contiene eventos de CloudTrail administración o de datos).

Para evitar que un almacén de datos de eventos ingiera eventos

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. En Acciones, elija Detener ingesta.
5. Cuando se le pida confirmación, elija Detener ingesta. El almacén de datos de eventos dejará de ingerir eventos en vivo.
6. Para reanudar la ingestión, elija Iniciar ingesta.

Para reiniciar la incorporación de eventos

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. En Acciones, elija Detener incorporación.

Federar un almacén de datos de eventos

La federación de un banco de datos de eventos le permite ver los metadatos asociados al banco de datos de eventos en el catálogo de AWS Glue datos, registrar el catálogo de datos con AWS Lake Formationél y ejecutar consultas SQL sobre los datos de sus eventos mediante Amazon Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar.

Puede habilitar la federación mediante la CloudTrail consola o la operación AWS CLI de la EnableFederationAPI. Al habilitar la federación de consultas de Lake, CloudTrail crea una base de datos administrada con un nombre `aws:cloudtrail` (si la base de datos aún no existe) y una tabla federada administrada en el catálogo de AWS Glue datos. El ID del banco de datos de eventos se usa para el nombre de la tabla. CloudTrail registra el ARN de la función de federación y el almacén de datos de eventos AWS Lake Formation, el servicio responsable de permitir un control de acceso detallado de los recursos federados del catálogo de datos. AWS Glue

Para habilitar la federación de consultas de Lake, debe crear un nuevo rol de IAM o elegir uno existente. Lake Formation usa este rol para administrar los permisos del almacén de datos de eventos federados. Al crear un nuevo rol mediante la CloudTrail consola, crea CloudTrail automáticamente los permisos necesarios para el rol. Si elige un rol existente, asegúrese de que el rol proporcione los permisos mínimos.

Puede deshabilitar la federación mediante la CloudTrail consola o la AWS CLI operación de la DisableFederationAPI. Al deshabilitar la federación, CloudTrail deshabilita la integración con AWS Glue AWS Lake Formation, y Amazon Athena. Tras deshabilitar la federación de consultas de Lake, ya no podrá consultar los datos de sus eventos en Athena. Al deshabilitar la federación, no se elimina ningún dato de CloudTrail Lake y puede seguir realizando consultas en CloudTrail Lake.

La federación de un almacén de datos de eventos de CloudTrail Lake no conlleva ningún CloudTrail cargo. Realizar consultas en Amazon Athena tiene costos. Para obtener más información acerca de los precios de Athena, consulte la Precios de Amazon Athena.

Temas

- Consideraciones
- Permisos necesarios para habilitar la federación
- Habilitación de la federación de consultas de Lake
- Deshabilitar la federación de consultas de Lake
- Administra los recursos de la federación de CloudTrail Lake con AWS Lake Formation

Consideraciones

Debe tener en cuenta los factores siguientes al federar un almacén de datos de eventos:

- La federación de un almacén de datos de eventos de CloudTrail Lake no conlleva ningún CloudTrail cargo. Realizar consultas en Amazon Athena tiene costos. Para obtener más información acerca de los precios de Athena, consulte la Precios de Amazon Athena.
- Lake Formation se usa para administrar los permisos de los recursos federados. Si eliminas el rol de federación o revocas los permisos a los recursos de Lake Formation AWS Glue, no puedes ejecutar consultas desde Athena. Para obtener más información sobre el uso de Lake Formation, consulte Administra los recursos de la federación de CloudTrail Lake con AWS Lake Formation.
- Cualquier persona que utilice Amazon Athena para consultar datos registrados en Lake Formation debe tener una política de permisos de IAM que permita

la acción `lakeformation:GetDataAccess`. La política AWS gestionada: AmazonAthenaFullAccesspermite esta acción. Si utiliza políticas insertadas, asegúrese de actualizar las políticas de permisos para permitir esta acción. Para obtener más información, consulte Administración de permisos de usuario de Lake Formation y Athena.

- Para crear vistas en tablas federadas en Athena, necesita una base de datos de destino distinta de `aws:cloudtrail`. Esto se debe a que la `aws:cloudtrail` base de datos está gestionada por CloudTrail.
- Para crear un conjunto de datos en Amazon QuickSight, debe elegir la opción Usar SQL personalizado. Para obtener más información, consulte Creación de un conjunto de datos con los datos de Amazon Athena.
- Si la federación está habilitada, no podrá eliminar un almacén de datos de eventos. Para eliminar un almacén de datos de eventos federado, primero debe deshabilitar la federación y la protección de terminación si está habilitada.
- Las siguientes consideraciones se aplican a los almacenes de datos de eventos de la organización:
  - Solo una cuenta de administrador delegado o la cuenta de administración pueden habilitar la federación en el almacén de datos de eventos de una organización. Otras cuentas de administrador delegado aún pueden consultar y compartir información mediante la característica de intercambio de datos de Lake Formation.
  - Cualquier cuenta de administrador delegado o la cuenta de administración de la organización puede deshabilitar la federación.

Permisos necesarios para habilitar la federación

Antes de federar un almacén de datos de eventos, asegúrese de tener todos los permisos necesarios para el rol de federación y para habilitar e deshabilitar la federación. Solo necesita actualizar los permisos del rol de federación si elige un rol de IAM existente para habilitar la federación. Si decide crear un nuevo rol de IAM mediante la CloudTrail consola, CloudTrail proporciona todos los permisos necesarios para el rol.

Temas

- Permisos de IAM para federar un almacén de datos de eventos
- Permisos necesarios para habilitar la federación
- Permisos necesarios para deshabilitar la federación

Permisos de IAM para federar un almacén de datos de eventos

Cuando habilita la federación, tiene la opción de crear un nuevo rol de IAM o utilizar un rol de IAM existente. Al elegir una nueva función de IAM, CloudTrail crea una función de IAM con los permisos necesarios y no es necesario que realice ninguna otra acción por su parte.

Si elige un rol existente, asegúrese de que las políticas de roles de IAM proporcionen los permisos necesarios para habilitar la federación. Esta sección proporciona ejemplos de las políticas de confianza y de permisos necesarias para el rol de IAM.

En el siguiente ejemplo, se proporciona la política de permisos para el rol de federación. Para la primera instrucción, proporcione el ARN completo del almacén de datos de su evento para el `Resource`.

La segunda instrucción de esta política permite a Lake Formation descifrar los datos de un almacén de datos de eventos cifrados con una clave de KMS. Sustituya *`key-region`*, *`account-id`* y *`key-id`* por los valores de su clave de KMS. Puede omitir esta afirmación si el almacén de datos de eventos no utiliza una clave de KMS para el cifrado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

En el siguiente ejemplo, se muestra la política de confianza de IAM, que permite a AWS Lake Formation asumir un rol de IAM para administrar los permisos del almacén de datos de eventos federados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Permisos necesarios para habilitar la federación

En el siguiente ejemplo de política, se proporcionan los permisos mínimos necesarios para habilitar la federación en un almacén de datos de eventos. Esta política permite CloudTrail habilitar la federación en el almacén de datos del evento, AWS Glue crear los recursos federados en el catálogo de AWS Glue datos y gestionar el registro de AWS Lake Formation los recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
```

```
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Permisos necesarios para deshabilitar la federación

En el siguiente ejemplo de política, se proporcionan los recursos mínimos necesarios para deshabilitar la federación en un almacén de datos de eventos. Esta política CloudTrail permite deshabilitar la federación en el almacén de datos del evento, AWS Glue eliminar la tabla federada administrada del catálogo de AWS Glue datos y Lake Formation anular el registro del recurso federado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
```

```
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "Allow Lake Formation to deregister the resource",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Habilitación de la federación de consultas de Lake

Puede habilitar la federación de consultas de Lake mediante la CloudTrail consola o la operación de la API AWS CLI. EnableFederation Al habilitar la federación de consultas de Lake, CloudTrail crea una base de datos administrada denominada `aws:cloudtrail` (si la base de datos aún no existe) y una tabla federada administrada en el catálogo de AWS Glue datos. El ID del banco de datos de eventos se usa para el nombre de la tabla. CloudTrail registra el ARN de la función de federación y el almacén de datos de eventos AWS Lake Formation, el servicio responsable de permitir un control de acceso detallado de los recursos federados del catálogo de datos. AWS Glue

En esta sección se describe cómo habilitar la federación mediante la consola y. CloudTrail AWS CLI

CloudTrail console

En el siguiente procedimiento, se muestra cómo habilitar la federación de consultas de Lake en un almacén de datos de eventos existente.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.

3. Elija el almacén de datos de eventos que desea actualizar. Se abrirá la página de detalles del almacén de datos de eventos.
4. En Federación de consultas de Lake, elija Editar y, a continuación, elija Habilitar.
5. Elija si desea crear un nuevo rol de IAM, o utilizar un rol existente. Al crear un rol nuevo, crea CloudTrail automáticamente un rol con los permisos necesarios. Si utiliza un rol existente, asegúrese de que la política del rol proporcione los permisos mínimos requeridos.
6. Si está creando un rol de IAM nuevo, ingrese un nombre para el rol.
7. Si elige un rol de IAM existente, elija el rol que quiere usar. El rol debe existir en su cuenta.
8. Elija Guardar cambios. El Estado de la federación cambia a `Enabled`.

AWS CLI

Para habilitar la federación, ejecute el comando aws cloudtrail enable-federation proporcionando los parámetros --event-data-store y --role necesarios. En --event-data-store, proporcione el ARN del almacén de datos de eventos (o el sufijo de ID del ARN). En --role, proporcione el ARN de su rol de federación. El rol debe existir en su cuenta y proporcionar los permisos mínimos necesarios.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

En este ejemplo, se muestra cómo un administrador delegado puede habilitar la federación en un almacén de datos de eventos de la organización especificando el ARN del almacén de datos de eventos en la cuenta de administración y el ARN del rol de federación en la cuenta de administrador delegado.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Deshabilitar la federación de consultas de Lake

Puede deshabilitar la federación mediante la CloudTrail consola o la AWS CLI operación de la DisableFederationAPI. Al deshabilitar la federación, CloudTrail deshabilita la integración con AWS

Glue AWS Lake Formation, y Amazon Athena. Tras deshabilitar la federación de consultas de Lake, ya no podrá consultar los datos de sus eventos en Athena. Al deshabilitar la federación, no se elimina ningún dato de CloudTrail Lake y puede seguir realizando consultas en CloudTrail Lake.

En esta sección se describe cómo deshabilitar la federación mediante la CloudTrail consola y AWS CLI.

CloudTrail console

En el siguiente procedimiento, se muestra cómo deshabilitar la federación de consultas de Lake en un almacén de datos de eventos existente.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos que desea actualizar. Se abrirá la página de detalles del almacén de datos de eventos.
4. En Federación de consultas de Lake, elija Editar y, a continuación, elija Deshabilitar.
5. Elija Guardar cambios. El Estado de la federación cambia a `Disabled`.

AWS CLI

Para deshabilitar la federación en el almacén de datos de eventos, ejecute el comando aws cloudtrail disable-federation. El almacén de datos de eventos especificado por `--event-data-store`, que acepta un ARN de almacén de datos de eventos, o el sufijo de ID del ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Si se trata de un almacén de datos de eventos de la organización, utilice el ID de la cuenta que corresponde a la cuenta de administración.

Administra los recursos de la federación de CloudTrail Lake con AWS Lake Formation

Al federar un banco de datos de eventos, CloudTrail registra el ARN de la función de federación y el almacén de datos de eventos AWS Lake Formation en el servicio responsable de permitir un control de acceso detallado de los recursos federados en el catálogo de datos. AWS Glue En esta sección se describe cómo puede utilizar Lake Formation para gestionar los recursos de la federación de CloudTrail lagos.

Al habilitar la federación, CloudTrail crea los siguientes recursos en el catálogo AWS Glue de datos.

- Base de datos gestionada: CloudTrail crea 1 base de datos con el nombre de `aws:cloudtrail` cada cuenta. CloudTrail administra la base de datos. No puede eliminar ni modificar la base de datos en AWS Glue.
- Tabla federada gestionada: CloudTrail crea 1 tabla para cada banco de datos de eventos federado y utiliza el ID del banco de datos de eventos como nombre de la tabla. CloudTrail administra las tablas. No puede eliminar ni modificar las tablas que contiene AWS Glue. Para eliminar una tabla, debe deshabilitar la federación en el almacén de datos de eventos.

Cómo controlar el acceso a los recursos federados

Puede usar uno de los dos métodos de permisos para controlar el acceso a la base de datos y las tablas administradas.

- Control de acceso solo de IAM: con el control de acceso solo de IAM, todos los usuarios de la cuenta con los permisos de IAM requeridos tienen acceso a todos los recursos del catálogo de datos. Para obtener información sobre cómo AWS Glue funciona con IAM, consulte Cómo AWS Glue funciona con IAM.

  En la consola de Lake Formation, este método aparece como Utilizar solo control de acceso IAM.

  > **Note**
  >
  > Si desea crear filtros de datos y usar otras características de Lake Formation, debe usar el control de acceso de Lake Formation.

- Control de acceso a Lake Formation: este método ofrece las siguientes ventajas.
  - Puede implementar seguridad a nivel de columna, de fila y de celda mediante el uso de filtros de datos.

- La base de datos y las tablas solo son visibles para los administradores de Lake Formation y los creadores de la base de datos y los recursos. Si otro usuario necesita acceder a estos recursos, debe conceder el acceso de forma explícita mediante los permisos de Lake Formation.

Para obtener más información sobre el control de acceso, consulte Métodos para el control de acceso detallado.

Cómo determinar el método de permisos para un recurso federado

Cuando habilita la federación por primera vez, CloudTrail crea una base de datos gestionada y una tabla federada gestionada con la configuración del lago de datos de Lake Formation.

Una vez CloudTrail habilitada la federación, puede comprobar qué método de permisos está utilizando para la base de datos gestionada y la tabla federada gestionada comprobando los permisos de esos recursos. Si el recurso tiene la configuración `ALL` (Super) en `IAM_ALLOWED_PRINCIPALS` , el recurso se administra exclusivamente mediante permisos de IAM. Si falta la configuración, el recurso se administra mediante los permisos de Lake Formation. Para obtener más información sobre los permisos de Lake Formation, consulte Referencia de permisos de Lake Formation.

El método de permisos para la base de datos administrada y la tabla federada administrada puede diferir. Por ejemplo, si comprueban los valores de la base de datos y la tabla, puede ver lo siguiente:

- En el caso de la base de datos, está presente el valor que asigna `ALL` (Super) a `IAM_ALLOWED_PRINCIPALS` en los permisos, lo que indica que utiliza el control de acceso exclusivo de IAM para la base de datos.
- En la tabla, no está presente el valor que asigna `ALL` (Super) a `IAM_ALLOWED_PRINCIPALS` en los permisos, lo que indica el control de acceso mediante los permisos de Lake Formation.

Puede cambiar entre los métodos de acceso en cualquier momento al agregar o quitar el permiso `ALL` (Super) al permiso `IAM_ALLOWED_PRINCIPALS` en cualquier recurso federado de Lake Formation.

Uso compartido de datos entre cuentas mediante Lake Formation

En esta sección, se describe cómo compartir una base de datos administrada y una tabla federada administrada entre cuentas mediante Lake Formation.

Puede compartir una base de datos administrada entre cuentas siguiendo estos pasos:

1. Actualice la versión para compartir datos entre cuentas a la versión 4.
2. Elimine `Super` de los permisos `IAM_ALLOWED_PRINCIPALS` de la base de datos, si están presentes, para cambiar al control de acceso de Lake Formation.
3. Conceda permisos `Describe` a la cuenta externa en la base de datos.
4. Si comparte un recurso del catálogo de datos con usted Cuenta de AWS y su cuenta no pertenece a la misma AWS organización que la cuenta compartida, acepte la invitación para compartir recursos de AWS Resource Access Manager (AWS RAM). Para obtener más información, consulte Aceptar una invitación de AWS RAM para compartir recursos.

Tras completar estos pasos, la base de datos debería estar visible para la cuenta externa. De forma predeterminada, compartir la base de datos no da acceso a ninguna tabla de la base de datos.

Puede compartir todas las tablas federadas administradas o de forma individual con una cuenta externa siguiendo estos pasos:

1. Actualice la versión para compartir datos entre cuentas a la versión 4.
2. Elimine `Super` de los permisos `IAM_ALLOWED_PRINCIPALS` de la tabla si están presentes para cambiar al control de acceso de Lake Formation.
3. (Opcional) Especifique cualquier filtro de datos para restringir las columnas o filas.
4. Conceda permisos `Select` a la cuenta externa de la tabla.
5. Si comparte un recurso del catálogo de datos con usted Cuenta de AWS y su cuenta no pertenece a la misma AWS organización que la cuenta compartida, acepte la invitación para compartir recursos de AWS Resource Access Manager (AWS RAM). Para una organización, puede aceptar automáticamente el uso de la configuración de RAM. Para obtener más información, consulte Aceptar una invitación de AWS RAM para compartir recursos.
6. La tabla ahora debería estar visible. Para habilitar las consultas de Amazon Athena en esta tabla, cree un enlace de recursos en esta cuenta con la tabla compartida.

La cuenta propietaria puede revocar el uso compartido en cualquier momento quitando los permisos de la cuenta externa de Lake Formation o deshabilitando la federación en. CloudTrail

Cambiar la protección contra la terminación

De forma predeterminada, los almacenes de datos de eventos de AWS CloudTrail Lake están configurados con la protección de terminación habilitada. La protección contra terminación evita que el almacén de datos de eventos se elimine accidentalmente. Si desea eliminar el almacén de datos

de eventos, debe deshabilitar la protección contra la terminación. Puede deshabilitar la protección de terminación mediante las operaciones de la API AWS Management Console AWS CLI, o.

Para desactivar la protección contra la terminación

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. En Acciones, elija Cambiar protección contra la terminación.
5. Elija Deshabilitar.
6. Seleccione Guardar. Ahora puede eliminar el almacén de datos de eventos.

Para activar la protección contra la terminación

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. En Acciones, elija Cambiar protección contra la terminación.
5. Para habilitar la protección de terminación, elija Habilitada.
6. Seleccione Guardar.

Eliminación de un almacén de datos de eventos

En esta sección, se describe cómo eliminar un almacén de datos de eventos mediante la consola de AWS CloudTrail . Para obtener información sobre cómo eliminar un almacén de datos de eventos mediante el AWS CLI, consulteEliminar un almacén de datos de eventos con la AWS CLI.

> **Note**
>
> No puede eliminar un almacén de datos de eventos si la protección contra la terminación o la federación de consultas de Lake están habilitadas. De forma predeterminada, CloudTrail habilita la protección de terminación para evitar que un almacén de datos de eventos se elimine accidentalmente.

Para eliminar un almacén de datos de eventos con un tipo de evento de integración, primero debe eliminar el canal de la integración. Puede eliminar el canal desde la página de detalles de la integración o mediante el comando aws cloudtrail delete-channel. Para más información, consulte Eliminar un canal para eliminar una integración con la AWS CLI

Para eliminar un almacén de datos de eventos

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. En Actions (Acciones), seleccione Delete (Eliminar).
5. Escriba el nombre del almacén de datos de eventos para confirmar que desea eliminarlo.
6. Elija Eliminar.

Después de eliminar un almacén de datos de eventos, el estado del almacén de datos de eventos cambia a `PENDING_DELETION` y permanece en él durante 7 días. Puede restaurar un almacén de datos de eventos durante el periodo de espera de 7 días. Mientras está en estado `PENDING_DELETION`, un almacén de datos de eventos no está disponible para consultas y no se pueden realizar otras operaciones en el almacén de datos de eventos, excepto operaciones de restauración. Un almacén de datos de eventos que está pendiente de eliminación no ingiere eventos ni genera costos.

Restauración de un almacén de datos de eventos

Tras eliminar un almacén de datos de eventos en AWS CloudTrail Lake, su estado cambia a ese estado `PENDING_DELETION` y permanece en ese estado durante 7 días. Durante este tiempo, puede restaurar el almacén de datos de eventos mediante la operación AWS Management Console AWS CLI, o la RestoreEventDataStoreAPI.

En esta sección, se describe cómo restaurar un almacén de datos de eventos mediante la consola. Para obtener información sobre cómo restaurar un banco de datos de eventos mediante el AWS CLI, consulteRestaurar un almacén de datos de eventos con la AWS CLI.

Para restaurar un almacén de datos de eventos

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos.
4. En Acciones, elija Restaurar.

Almacenes de datos de eventos de la organización

Si ha creado una organización en AWS Organizations, puede crear un almacén de datos de eventos de la organización que registre todos los eventos de todos los Cuentas de AWS miembros de esa organización. Los almacenes de datos de eventos de la organización se pueden aplicar a todas las Regiones de AWS regiones o a la región actual. No se puede utilizar el almacén de datos de eventos de la organización para recopilar eventos fuera de AWS.

Puede crear un banco de datos de eventos de la organización mediante la cuenta de administración o la cuenta de administrador delegado. Cuando un administrador delegado crea un almacén de datos de eventos de la organización, el almacén de datos de eventos de la organización existe en la cuenta de administración de la organización. Este enfoque se debe a que la cuenta de administración mantiene la propiedad de todos los recursos de la organización.

La cuenta de administración de una organización puede actualizar un banco de datos de eventos a nivel de cuenta para aplicarlo a una organización.

Cuando se especifica que el almacén de datos de eventos de la organización se aplica a una organización, se aplica automáticamente a todas las cuentas de miembros de la organización. Las cuentas de miembro no pueden ver el almacén de datos de eventos de la organización, ni pueden modificarlo o eliminarlo. De forma predeterminada, las cuentas de miembro no tienen acceso al almacén de datos de eventos de la organización, ni pueden realizar consultas en los almacenes de datos de eventos de la organización.

En la siguiente tabla se muestran las capacidades de la cuenta de administración y las cuentas de administrador delegado de la organización. AWS Organizations

Capacidades	Cuenta de administración	Cuenta de administrador delegado
Registrar o eliminar las cuentas de administrador delegado.	Sí	No
Cree un almacén de datos de eventos de la organización para AWS CloudTrail los eventos o los elementos AWS Config de configuración.	Sí	Sí
Habilite Insights en un almacén de datos de eventos de la organización.	Sí	No
Actualizar un almacén de datos de eventos de la organización.	Sí	Sí[1]
Habilitar la federación de consultas de Lake en un almacén de datos de eventos de la organización. [2]	Sí	Sí
Deshabilitar la federación de consultas de Lake en un almacén de datos de eventos de la organización.	Sí	Sí
Eliminar un almacén de datos de eventos de la organización.	Sí	Sí
Copie eventos de registro de seguimiento en un almacén de datos de eventos.	Sí	No
Ejecutar consultas en almacenes de datos de eventos de la organización.	Sí	Sí
Consulta el panel de control de CloudTrail Lake para ver un almacén de datos de eventos de la organización.	Sí	Sí

[1] Solo la cuenta de administración puede convertir un banco de datos de eventos de la organización en un banco de datos de eventos a nivel de cuenta, o convertir un banco de datos de eventos a nivel de cuenta en un banco de datos de eventos de la organización. Estas acciones no están permitidas para el administrador delegado porque los almacenes de datos de eventos de la organización solo existen en la cuenta de administración. Cuando un banco de datos de eventos de la organización se convierte en un banco de datos de eventos a nivel de cuenta, solo la cuenta de administración tiene acceso al banco de datos de eventos. Del mismo modo, solo un almacén de datos de eventos a nivel de cuenta de la cuenta de administración se puede convertir en un almacén de datos de eventos de la organización.

[2] Solo una cuenta de administrador delegado o la cuenta de administración pueden habilitar la federación en el almacén de datos de eventos de una organización. Otras cuentas de administrador delegado pueden consultar y compartir información mediante la característica de uso compartido de datos de Lake Formation. Cualquier cuenta de administrador delegado, así como la cuenta de administración de la organización, pueden deshabilitar la federación.

Cree un almacén de datos de eventos de la organización

La cuenta de administración o la cuenta de administrador delegado de una organización pueden crear un banco de datos de eventos de la organización para recopilar CloudTrail eventos (eventos de administración, eventos de datos) o elementos de AWS Config configuración.

> **Note**
>
> Solo la cuenta de administración de la organización puede copiar los eventos de seguimiento a un banco de datos de eventos.

CloudTrail console

Para crear un almacén de datos de eventos de la organización mediante la consola

1. Siga los pasos del procedimiento de creación de un banco de datos de CloudTrail eventos para crear un banco de datos de eventos de la organización para eventos CloudTrail de administración o de datos.

   OR

Siga los pasos del procedimiento de creación de un banco de datos de eventos para los elementos de AWS Config configuración para crear un banco de datos de eventos de la organización para los elementos de AWS Config configuración.

2. En la página Elegir eventos, elija Activar para todas las cuentas de mi organización.

AWS CLI

Para crear un almacén de datos de eventos de la organización, ejecute el create-event-data-storecomando e incluya la `--organization-enabled` opción.

El siguiente AWS CLI `create-event-data-store` comando de ejemplo crea un banco de datos de eventos de la organización que recopila todos los eventos de administración. Dado que CloudTrail registra los eventos de administración de forma predeterminada, no es necesario especificar selectores de eventos avanzados si el banco de datos de eventos registra todos los eventos de administración y no recopila ningún evento de datos.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
```

```
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

El siguiente AWS CLI `create-event-data-store` comando de ejemplo crea un banco de datos de eventos de la organización denominado `config-items-org-eds` que recopila los elementos AWS Config de configuración. Para recopilar los elementos de configuración, especifique que el `eventCategory` campo es igual al `ConfigurationItem` de los selectores de eventos avanzados.

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Aplique un banco de datos de eventos a nivel de cuenta a una organización

La cuenta de administración de la organización puede convertir un banco de datos de eventos a nivel de cuenta para aplicarlo a una organización.

CloudTrail console

Para actualizar un almacén de datos de eventos a nivel de cuenta mediante la consola

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. Elija el almacén de datos de eventos que desea actualizar. Esta acción abre la página de detalles del almacén de datos de eventos.

4. En General details (Detalles generales), elijaEdit (Editar).
5. Selecciona Activar para todas las cuentas de mi organización.
6. Elija Guardar cambios.

Para obtener información adicional sobre la actualización de un banco de datos de eventos, consulteActualización de un almacén de datos de eventos.

AWS CLI

Para actualizar un banco de datos de eventos a nivel de cuenta para aplicarlo a una organización, ejecute el update-event-data-storecomando e incluya la `--organization-enabled` opción.

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Véase también

- Administrador delegado de la organización
- Agrega un administrador delegado CloudTrail
- Eliminar un administrador CloudTrail delegado

Creación de una integración con un origen de eventos externo a AWS

Puede utilizar CloudTrail para registrar y almacenar datos de actividad de los usuarios desde cualquier origen en los entornos híbridos, como aplicaciones internas o de SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores. Puede almacenar, acceder y analizar los datos, solucionar problemas y tomar medidas al respecto sin tener que mantener varios agregadores de registros y herramientas de informes.

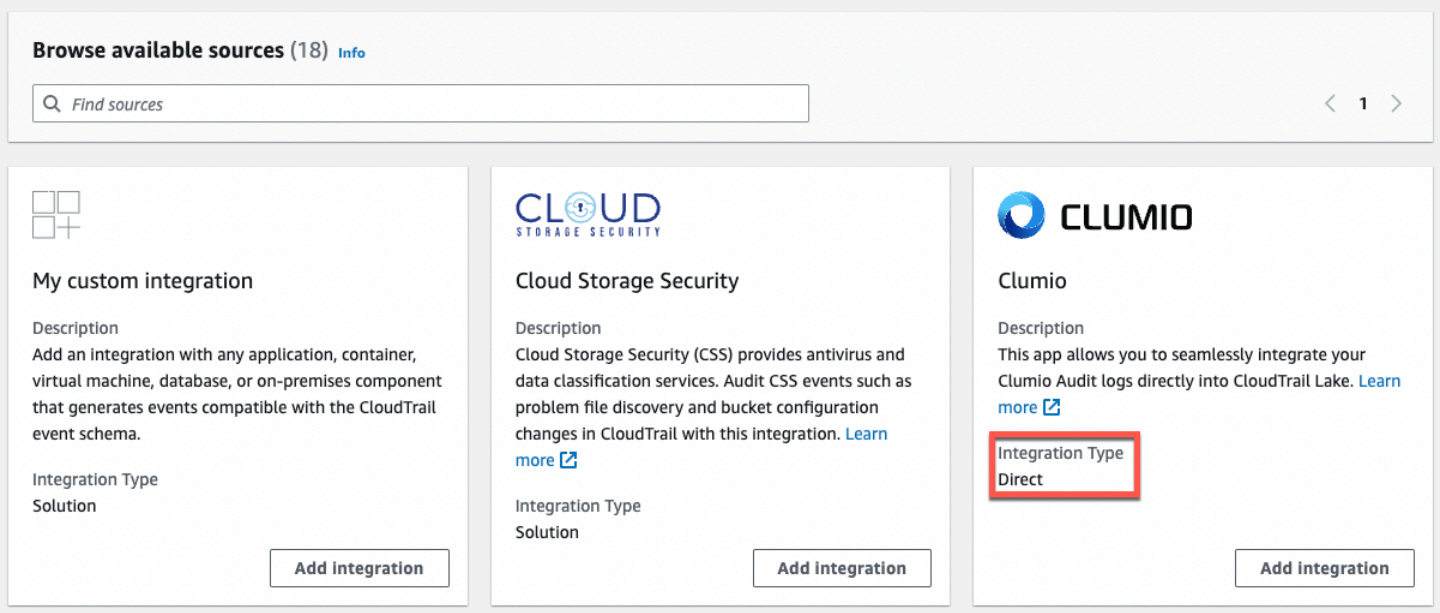
Los eventos de actividad de orígenes que no son de AWS funcionan con canales para incluir eventos a CloudTrail Lake de socios externos que trabajan con CloudTrail o de sus orígenes. Cuando crea un canal, elige uno o más almacenes de datos de eventos para almacenar los eventos que llegan del origen del canal. Puede cambiar los almacenes de datos de eventos de destino de un canal según

sea necesario, siempre que los almacenes de datos de eventos de destino estén configurados para registrar eventos `eventCategory="ActivityAuditLog"`. Cuando crea un canal para eventos de un socio externo, proporciona un ARN de canal a la aplicación asociada o de origen. La política de recursos asociada al canal permite que el origen transmita eventos a través del canal. Si un canal no tiene una política de recursos, solo el propietario del canal puede llamar a la API `PutAuditEvents` en el canal.

CloudTrail se asoció con muchos proveedores de orígenes de eventos, como Okta y LaunchDarkly. Cuando crea una integración con un origen de eventos externo a AWS, puede elegir uno de estos socios como origen de eventos o elegir My custom integration (Mi integración personalizada) para integrar eventos de sus orígenes en CloudTrail. Se permite un máximo de un canal por origen.

Existen dos tipos de integraciones: directas y de solución. Con las integraciones directas, el socio llama a la API `PutAuditEvents` para enviar eventos al almacén de datos de eventos de su cuenta de AWS. Con las integraciones de solución, la aplicación se ejecuta en su cuenta de AWS y la aplicación llama a la API `PutAuditEvents` para enviar eventos al almacén de datos de eventos de su cuenta de AWS.

En la página Integrations (Integraciones), puede elegir la pestaña Available sources (Orígenes disponibles) para ver el Integration type (Tipo de integración) para los socios.



Para comenzar, cree una integración para registrar eventos de orígenes de socios o de otras aplicaciones mediante la consola de CloudTrail.

Temas

- Creación de una integración con un socio de CloudTrail
- Creación de una integración personalizada
- Información adicional acerca de los socios de integración
- Esquema de eventos de integraciones de CloudTrail Lake

Creación de una integración con un socio de CloudTrail

Cuando crea una integración con un origen de eventos externo a AWS, puede elegir uno de estos socios como origen de eventos. Cuando crea una integración en CloudTrail con una aplicación asociada, el socio necesita el nombre de recurso de Amazon (ARN) del canal que usted crea en este flujo de trabajo para enviar eventos a CloudTrail. Después de que crea la integración, termina de configurarla según las instrucciones del socio para proporcionarle el ARN del canal requerido. La integración comienza a ingerir eventos de socios en CloudTrail después de que el socio llama a `PutAuditEvents` en el canal de la integración.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Integraciones.
3. En la página Add integration (Agregar integración), ingrese un nombre para el canal. El nombre puede tener entre 3 y 128 caracteres. Solo se permiten letras, números, puntos, guiones medios y guiones bajos.
4. Elija el origen de la aplicación asociada del que desea obtener los eventos. Si realiza la integración con eventos de sus aplicaciones alojadas en las instalaciones o en la nube, elija My custom integration (Mi integración personalizada).
5. En Event delivery location (Ubicación de entrega de eventos), elija registrar los mismos eventos de actividad en los almacenes de datos de eventos existentes o cree un almacén de datos de eventos nuevo.

   Si elige crear un almacén de datos de eventos nuevo, ingrese un nombre para el almacén de datos de eventos, elija una opción de precios y especifique el periodo de retención en días. El almacén de datos de eventos retiene los datos de eventos durante el número especificado de días.

   Si decide registrar los eventos de actividad en uno o más almacenes de datos de eventos existentes, elija los almacenes de datos de eventos de la lista. Los almacenes de datos de eventos solo pueden incluir eventos de actividad. El tipo de evento en la consola debe ser

Events from integrations (Eventos de integraciones). En la API, el valor `eventCategory` debe ser `ActivityAuditLog`.

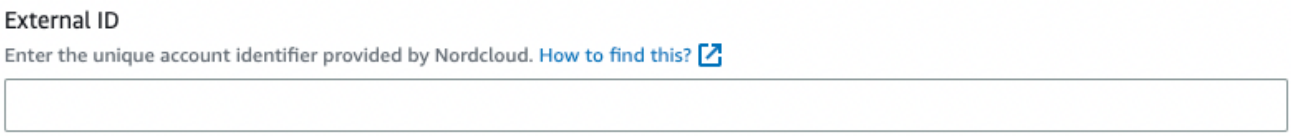
6. En Resource policy (Política de recursos), configure la política de recursos para el canal de la integración. Las políticas de recursos son documentos de política JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso y bajo qué condiciones. Las cuentas definidas como entidades principales en la política de recursos pueden llamar a la API `PutAuditEvents` para enviar eventos al canal. El propietario del recurso tiene acceso implícito al recurso si la política de IAM permite la acción `cloudtrail-data:PutAuditEvents`.

   La información necesaria para la política está determinada por el tipo de integración. Para una integración directa, CloudTrail agrega de forma automática los ID de la cuenta de AWS del socio y requiere que usted ingrese el ID externo único proporcionado por el socio. Para la integración de una solución, debe especificar al menos un ID de cuenta de AWS como entidad principal y, si lo desea, puede ingresar un ID externo para evitar un suplente confuso.

   > **Note**
   >
   > Si no se crea una política de recursos para el canal, solo el propietario del canal puede llamar a la API `PutAuditEvents` del canal.

   a. Para una integración directa, ingrese el ID externo proporcionado por el socio. El socio de integración proporciona un ID externo único, como un ID de cuenta o una cadena generada de forma aleatoria, que se utiliza en la integración para evitar un suplente confuso. Es responsabilidad del socio crear y proporcionar un ID externo único.

      Puede elegir How to find this? (¿Cómo encontrar esto?) para ver la documentación del socio que describe cómo encontrar el ID externo.

      > **Note**
      >
      > Si la política de recursos incluye un ID externo, todas las llamadas a la API `PutAuditEvents` deben incluir el ID externo. Sin embargo, si la política no define

un ID externo, el socio aún puede llamar a la API `PutAuditEvents` y especificar un parámetro `externalId`.

b. Para una integración de solución, elija Agregar cuenta de AWS para especificar el ID de una cuenta de AWS que se agregará como entidad principal en la política.

7. (Opcional) En el área Tags (Etiquetas), puede agregar hasta 50 pares de claves y valores de etiquetas para que lo ayuden a identificar, ordenar y controlar el acceso al almacén de datos de eventos y al canal. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo puede utilizar las etiquetas en AWS, consulte Etiquetado de los recursos de AWS en la Referencia general de AWS.
8. Cuando esté listo para crear la integración nueva, elija Add integration (Agregar integración). No hay página de revisión. CloudTrail crea la integración, pero usted debe proporcionar el nombre de recurso de Amazon (ARN) del canal a la aplicación asociada. Las instrucciones para proporcionar el ARN del canal a la aplicación asociada se encuentran en el sitio web de documentación de socios. Para obtener más información, elija el enlace Learn more (Más información) del socio en la pestaña Available sources (Orígenes disponibles) de la página Integrations (Integraciones) para abrir la página del socio en AWS Marketplace.

Para finalizar la configuración de la integración, proporcione el ARN del canal a la aplicación asociada o de origen. En función del tipo de integración, usted, el socio o la aplicación ejecutarán la API `PutAuditEvents` para enviar eventos de actividad al almacén de datos de eventos de su cuenta de AWS. Una vez que se envían los eventos de actividad, puede utilizar CloudTrail Lake para buscar, consultar y analizar los datos que se registran de las aplicaciones. Los datos de eventos incluyen campos que coinciden con la carga útil de eventos de CloudTrail, como `eventVersion`, `eventSource` y `userIdentity`.

Creación de una integración personalizada

Puede utilizar CloudTrail para registrar y almacenar datos de actividad de los usuarios desde cualquier origen en los entornos híbridos, como aplicaciones internas o de SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores. Realice la primera mitad de este procedimiento en la consola de CloudTrail Lake, luego llame a la API `PutAuditEvents` para ingerir eventos y proporcione el ARN del canal y la carga útil del evento. Después de utilizar

la API `PutAuditEvents` para ingerir la actividad de la aplicación en CloudTrail, puede utilizar CloudTrail Lake para buscar, consultar y analizar los datos que se registran de las aplicaciones.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Integraciones.
3. En la página Add integration (Agregar integración), ingrese un nombre para el canal. El nombre puede tener entre 3 y 128 caracteres. Solo se permiten letras, números, puntos, guiones medios y guiones bajos.
4. Elija My custom integration (Mi integración personalizada).
5. En Event delivery location (Ubicación de entrega de eventos), elija registrar los mismos eventos de actividad en los almacenes de datos de eventos existentes o cree un almacén de datos de eventos nuevo.

   Si elige crear un almacén de datos de eventos nuevo, ingrese un nombre para el almacén de datos de eventos y especifique el periodo de retención en días. Puede conservar los datos de eventos en un almacén de datos de eventos durante un máximo de 3653 días (unos 10 años) si elige la opción de precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción de precio de retención de siete años.

   Si decide registrar los eventos de actividad en uno o más almacenes de datos de eventos existentes, elija los almacenes de datos de eventos de la lista. Los almacenes de datos de eventos solo pueden incluir eventos de actividad. El tipo de evento en la consola debe ser Events from integrations (Eventos de integraciones). En la API, el valor `eventCategory` debe ser `ActivityAuditLog`.
6. En Resource policy (Política de recursos), configure la política de recursos para el canal de la integración. Las políticas de recursos son documentos de política JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso y bajo qué condiciones. Las cuentas definidas como entidades principales en la política de recursos pueden llamar a la API `PutAuditEvents` para enviar eventos al canal.

   > **Note**
   >
   > Si no se crea una política de recursos para el canal, solo el propietario del canal puede llamar a la API `PutAuditEvents` del canal.

a. (Opcional) Ingrese un ID externo único para proporcionar una capa de protección adicional. El ID externo es una cadena única, como un ID de cuenta o una cadena generada de forma aleatoria, para evitar un suplente confuso.

> **Note**
>
> Si la política de recursos incluye un ID externo, todas las llamadas a la API `PutAuditEvents` deben incluir el ID externo. Sin embargo, si la política no define un ID externo, usted puede llamar a la API `PutAuditEvents` y especificar un parámetro `externalId`.

b. Elija Agregar cuenta de AWS para especificar el ID de cada cuenta de AWS que desea agregar como entidad principal en la política de recursos del canal.

7. (Opcional) En el área Tags (Etiquetas), puede agregar hasta 50 pares de claves y valores de etiquetas para que lo ayuden a identificar, ordenar y controlar el acceso al almacén de datos de eventos y al canal. Para obtener más información sobre cómo utilizar las políticas de IAM para autorizar el acceso a un almacén de datos de eventos en función de etiquetas, consulte Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas. Para obtener más información sobre cómo puede utilizar las etiquetas en AWS, consulte Etiquetado de los recursos de AWS en la Referencia general de AWS.
8. Cuando esté listo para crear la integración nueva, elija Add integration (Agregar integración). No hay página de revisión. CloudTrail crea la integración, pero para integrar los eventos personalizados, debe especificar el ARN del canal en una solicitud `PutAuditEvents`.
9. Llame a la API `PutAuditEvents` para ingerir los eventos de actividad en CloudTrail. Puede agregar hasta 100 eventos de actividad (o hasta 1 MB) por solicitud `PutAuditEvents`. Necesitará el ARN del canal que creó en los pasos anteriores, la carga útil de los eventos que desea que CloudTrail agregue y el ID externo (si lo especificó en la política de recursos). Asegúrese de que no haya información confidencial o de identificación personal en la carga útil del evento antes de incorporarla en CloudTrail. Los eventos que ingiera en CloudTrail deben seguir el Esquema de eventos de integraciones de CloudTrail Lake.

> **Tip**
>
> Utilice AWS CloudShell para asegurarse de que se están ejecutando las API AWS más recientes.

Los siguientes ejemplos muestran cómo utilizar el comando put-audit-events de la CLI. Los parámetros --audit-events y --channel-arn son obligatorios. Necesita el ARN del canal que creó en los pasos previos, el cual se puede copiar de la página de detalles de la integración. El valor de --audit-events es una matriz JSON de objetos de eventos. `--audit-events` incluye un ID obligatorio del evento, la carga útil requerida del evento como el valor de `EventData` y una suma de comprobación opcional para ayudar a validar la integridad del evento una vez ingerido en CloudTrail.

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

A continuación, se muestra un comando de ejemplo con dos ejemplos de eventos.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

El siguiente comando de ejemplo agrega el parámetro `--cli-input-json` para especificar un archivo JSON (`custom-events.json`) de la carga útil del evento.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

A continuación, se presenta el contenido de muestra del archivo JSON de ejemplo, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

(Opcional) Cálculo de un valor de la suma de comprobación

La suma de comprobación que se especifica como valor de `EventDataChecksum` en una solicitud `PutAuditEvents` ayuda a verificar que CloudTrail recibe el evento que coincide con la suma de comprobación y ayuda a verificar la integridad de los eventos. El valor de la suma de comprobación es un algoritmo base64-SHA256 que se calcula mediante la ejecución del siguiente comando.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
       \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
       \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
       \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
       \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
       \"additionalEventData\":{\"key\":\"value\"},
       \"sourceIPAddress\":\"source_IP_address\",
       \"recipientAccountId\":\"recipient_account_ID\"}",
```

```
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

El comando devuelve la suma de comprobación. A continuación, se muestra un ejemplo.

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

El valor de la suma de comprobación se convierte en el valor de `EventDataChecksum` en la solicitud `PutAuditEvents`. Si la suma de comprobación no coincide con la del evento proporcionado, CloudTrail rechaza el evento y se produce un error `InvalidChecksum`.

Información adicional acerca de los socios de integración

La tabla en la siguiente sección brinda el nombre de origen de cada socio de integración e identifica el tipo de integración (directa o de solución).

La información en la columna Source name (Nombre del origen) es obligatoria para llamar a la API `CreateChannel`. Especifica el nombre del origen como el valor para el parámetro `Source`.

Nombre del socio (consola)	Nombre del origen (API)	Tipo de integración
My custom integration	`Custom`	solución
Cloud Storage Security	`CloudStorageSecurityConsole`	solución
Clumio	`Clumio`	directa
CrowdStrike	`CrowdStrike`	solución
CyberArk	`CyberArk`	solución
GitHub	`GitHub`	solución
Kong Inc	`KongGatewayEnterprise`	solución
LaunchDarkly	`LaunchDarkly`	directa

Nombre del socio (consola)	Nombre del origen (API)	Tipo de integración
Netskope	`NetskopeCloudExchange`	solución
Nordcloud, an IBM Company	`IBMMulticloud`	directa
MontyCloud	`MontyCloud`	directa
Okta	`OktaSystemLogEvents`	solución
One Identity	`OneLogin`	solución
Shoreline.io	`Shoreline`	solución
Snyk.io	`Snyk`	directa
Wiz	`WizAuditLogs`	solución

Consulta de la documentación de socios

Para obtener más información sobre la integración de un socio con CloudTrail Lake, consulte la documentación del socio.

Para consultar la documentación de socios

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Integraciones.
3. En la página Integrations (Integraciones), elija Available sources (Orígenes disponibles) y, luego, elija Learn more (Más información) acerca del socio cuya documentación desea consultar.

Esquema de eventos de integraciones de CloudTrail Lake

En la siguiente tabla, se describen los elementos del esquema obligatorios y opcionales que coinciden con los de los registros de eventos de CloudTrail. Los eventos proporcionan el contenido de `eventData`, mientras que CloudTrail proporciona otros campos después de la ingesta de datos.

El contenido del registro de eventos de CloudTrail se describe con más detalle en CloudTrail contenido del registro.

- Campos que proporciona CloudTrail después de la ingesta de datos
- Campos que proporcionan los eventos

Campos que proporciona CloudTrail después de la ingesta de datos

Nombre del campo	Tipo de entrada	Requisito	Descripción
eventVersion	cadena	Obligatoria	La versión del evento.
eventCategory	cadena	Obligatoria	La categoría del evento. Para los eventos que no son de AWS, el valor es `ActivityAuditLog` .
eventType	cadena	Obligatoria	Tipo de evento. Para los eventos que no son de AWS, el valor válido es `ActivityLog` .
eventID	cadena	Obligatoria	El ID único de un evento.
eventTime	cadena	Obligatoria	Marca de tiempo del evento, en formato `yyyy-MM-DDTHH:mm:ss` , en tiempo universal coordinado (UTC).
awsRegion	cadena	Obligatoria	La Región de AWS donde la llamada

Nombre del campo	Tipo de entrada	Requisito	Descripción
			`PutAuditEvents` se realizó.
recipientAccountId	cadena	Obligatoria	Representa el ID de cuenta que recibió este evento. CloudTrail completa este campo mediante el cálculo a partir de la carga útil del evento.
addendum	-	Opcional	Muestra informaci ón sobre el motivo por el cual se retrasó el procesamiento de eventos. Si falta información de un evento existente, el bloque addendum incluye la información que falta y el motivo por el cual aquella falta.
• reason	cadena	Opcional	El motivo por el que faltaba el evento o parte de su contenido.
• updatedFields	cadena	Opcional	Los campos de registro de eventos que se actualizan mediante el anexo. Esto solo se proporcio na si el motivo es `UPDATED_DATA` .

Nombre del campo	Tipo de entrada	Requisito	Descripción
• originalUID	cadena	Opcional	El UID del evento original del origen. Esto solo se proporciona si el motivo es `UPDATED_DATA` .
• originalEventID	cadena	Opcional	El ID del evento original. Esto solo se proporciona si el motivo es `UPDATED_DATA` .
metadata	-	Obligatoria	Información acerca del canal que utilizó el evento.
• ingestionTime	cadena	Obligatoria	La marca de tiempo en que se procesó el evento, en formato `yyyy-MM-DDTHH:mm:ss` , en tiempo universal coordinado (UTC).
• channelARN	cadena	Obligatoria	El ARN del canal que utilizó el evento.

Campos proporcionados por eventos de clientes

Nombre del campo	Tipo de entrada	Requisito	Descripción
eventData	-	Obligatoria	Los datos de auditoría enviados a CloudTrail en una llamada `PutAuditEvents` .

Nombre del campo	Tipo de entrada	Requisito	Descripción
• versión	cadena	Obligatoria	La versión del evento desde el origen. Limitaciones de longitud: longitud máxima de 256 caracteres.
• userIdentity	-	Obligatoria	Información acerca del usuario que realizó una solicitud.
• • type	cadena	Obligatoria	El tipo de identidad de usuario. Limitaciones de longitud: longitud máxima de 128 caracteres.
• • principalId	cadena	Obligatoria	Un identificador único para el actor del evento. Limitaciones de longitud: longitud máxima de 1024 caracteres.
• • details	Objeto JSON	Opcional	Información adicional acerca de la identidad .

Nombre del campo	Tipo de entrada	Requisito	Descripción
• userAgent	cadena	Opcional	El agente que realizó la solicitud. Limitaciones de longitud: longitud máxima de 1024 caracteres.
• eventSource	cadena	Obligatoria	Este es el origen de eventos asociado o la aplicación personalizada en que se registran los eventos. Limitaciones de longitud: longitud máxima de 1024 caracteres.
• eventName	cadena	Obligatoria	La acción solicitada, una de las acciones de la API para la aplicación o el servicio de origen. Limitaciones de longitud: longitud máxima de 1024 caracteres.
• eventTime	cadena	Obligatoria	Marca de tiempo del evento, en formato `yyyy-MM-DDTHH:mm:ss` , en tiempo universal coordinado (UTC).

Nombre del campo	Tipo de entrada	Requisito	Descripción
• UID	cadena	Obligatoria	El valor de UID que identifica la solicitud . El servicio o la aplicación que se llama genera este valor. Limitaciones de longitud: longitud máxima de 1024 caracteres.
• requestParameters	Objeto JSON	Opcional	Los parámetros, si hay alguno, que se enviaron con la solicitud. Este campo tiene un tamaño máximo de 100 kB y el contenido que supere el límite se rechaza.
• responseElements	Objeto JSON	Opcional	El elemento de respuesta de las acciones que realizaron cambios (acciones de creación, actualiza ción o eliminación). Este campo tiene un tamaño máximo de 100 kB y el contenido que supere el límite se rechaza.

Nombre del campo	Tipo de entrada	Requisito	Descripción
• errorCode	cadena	Opcional	Una cadena que representa un error para el evento. Limitaciones de longitud: longitud máxima de 256 caracteres.
• errorMessage	cadena	Opcional	La descripción del error. Limitaciones de longitud: longitud máxima de 256 caracteres.
• sourceIPAddress	cadena	Opcional	La dirección IP desde la que se realizó la solicitud Se aceptan direcciones IPv4 y IPv6.
• recipientAccountId	cadena	Obligatoria	Representa el ID de cuenta que recibió este evento. El ID de la cuenta debe ser el mismo que el ID de la cuenta de AWS propietaria del canal.

Nombre del campo	Tipo de entrada	Requisito	Descripción
• additionalEventData	Objeto JSON	Opcional	Datos adicionales sobre el evento que no forman parte de la solicitud o la respuesta. Este campo tiene un tamaño máximo de 28 kB y el contenido que supere ese límite se rechaza.

En el siguiente ejemplo, se muestra la jerarquía de los elementos del esquema que coinciden con los de los registros de eventos de CloudTrail.

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
       "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
```

```
            JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

Ver los paneles de Lake

Puede utilizar los paneles de CloudTrail Lake para ver los eventos de un almacén de datos de eventos. Puede seleccionar entre varios tipos de paneles. Los tipos de paneles disponibles para un almacén de datos de eventos dependen de la configuración de los selectores de eventos avanzados del almacén de datos de eventos. Por ejemplo, si un tipo de panel muestra información sobre los eventos de administración de CloudTrail, solo puede seleccionar el panel si el almacén de datos de eventos seleccionado actualmente recopila los eventos de administración de CloudTrail.

Cada tipo de panel consta de varios widgets y cada widget representa una consulta SQL. Para ver la consulta de un widget, elija Ver y analizar en el editor de consultas para abrir el editor de consultas. No puede modificar la consulta generada por el sistema que se utiliza para rellenar el widget, pero puede modificarla y ejecutarla en el editor de consultas para analizarla más a fondo.

Para rellenar y actualizar un panel, elija Ejecutar consultas. Al elegir Ejecutar consultas, CloudTrail ejecuta consultas generadas por el sistema en su nombre. Dado que la ejecución de consultas genera costos, CloudTrail le pide que confirme los costos asociados a la ejecución de consultas. Solo

tendrá que confirmarlos una vez. Para obtener más información acerca de los precios de CloudTrail, consulte Precios de CloudTrail.

Temas

- Limitaciones
- Requisitos previos
- Elección de un panel
- Filtrado de un panel por intervalo de fecha u hora
- Visualización de la consulta de un widget de panel

Limitaciones

La versión actual presenta las siguientes limitaciones.

- La versión actual no admite paneles, widgets ni consultas personalizados.
- La versión actual solo proporciona paneles para los almacenes de datos de eventos que recopilan eventos de CloudTrail (eventos de datos y de administración) y eventos de Insights.
- La versión actual no admite la edición de las consultas generadas por el sistema que se utilizan para rellenar el panel. Puede ver y editar la consulta subyacente de cualquier widget en la pestaña Editor de consultas; sin embargo, los cambios realizados en la consulta solo servirán para efectuar un análisis complementario fuera del panel.

Requisitos previos

Para usar los paneles de Lake hay que cumplir los siguientes requisitos previos.

- Para ver y usar los paneles de Lake, debe crear al menos un almacén de datos de eventos de CloudTrail Lake. Puede crear almacenes de datos de eventos mediante la consola, la AWS CLI o los SDK. Para obtener información acerca de cómo crear un almacén de datos de eventos mediante la consola, consulte Cree un banco de datos de CloudTrail eventos para eventos. Para obtener información acerca de cómo crear un almacén de datos de eventos mediante la AWS CLI, consulte Administrar CloudTrail Lake mediante la AWS CLI.
- Para rellenar el panel, CloudTrail ejecuta consultas en su nombre. La primera vez que consulte la página Paneles, CloudTrail le pedirá que confirme los costos asociados a la ejecución de consultas. Elija Acepto para reconocer el costo de ejecutar las consultas.

Elección de un panel

Utilice el siguiente procedimiento para seleccionar el almacén de datos de eventos y el tipo de panel que desea ver.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación izquierdo, elija Lago y, a continuación, Panel.
3. Elija el almacén de datos de eventos cuyos datos desea visualizar.
4. Elija el tipo de panel que desea ver. La lista de paneles se rellena en función de la configuración de los selectores de eventos avanzados del almacén de datos de eventos seleccionado.

   Los tipos de paneles posibles son los siguientes:

   - Panel Información general: muestra los usuarios, las Regiones de AWS y los Servicios de AWS más activos por recuento de eventos. También puede ver información sobre la actividad de los eventos de administración de `read` y `write`, los eventos con más limitación y los principales errores. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración.
   - Panel Eventos de administración: muestra los eventos de inicio de sesión en la consola, los eventos de acceso denegado, las acciones destructivas y los principales errores por usuario. También puede ver información sobre las versiones de TLS y las llamadas de TLS obsoletas por usuario. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración.
   - Panel Eventos de datos de S3: muestra la actividad de la cuenta de S3, los objetos de S3 a los que más se ha accedido, los principales usuarios de S3 y las principales acciones de S3. Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos de Amazon S3.
   - Panel de eventos de Insights: muestra la proporción total de eventos de Insights por tipo de Insights, la proporción de eventos de Insights por tipo de Insights para los principales usuarios y servicios, y el número de eventos de Insights por día. El panel también incluye un widget que muestra hasta 30 días de eventos de Insights. Este panel solo está disponible para los almacenes de datos de eventos que recopilan eventos de Insights.

> **Note**
>
> - Después de que habilite CloudTrail Insights por primera vez en el almacén de datos de eventos de origen, CloudTrail puede tardar hasta 7 días en entregar el primer evento de Insights, si se detecta una actividad inusual. Para obtener más información, consulte Descripción de la entrega de eventos de Insights.
> - El panel Eventos de Insights solo muestra información sobre los eventos de Insights recopilados por el almacén de datos de eventos seleccionado, que viene determinada por la configuración del almacén de datos de eventos de origen. Por ejemplo, si configura el almacén de datos de eventos de origen para habilitar los eventos de Insights en `ApiCallRateInsight`, pero no en `ApiErrorRateInsight`, no verá la información sobre los eventos de Insights en `ApiErrorRateInsight`.

5. Elija si desea filtrar los datos del panel por Intervalo absoluto o Intervalo relativo. Elija Intervalo absoluto para seleccionar un intervalo de fechas y horas específico. Elija Intervalo relativo para seleccionar un intervalo de tiempo predefinido o personalizado. De forma predeterminada, el panel muestra los datos de eventos de las últimas 24 horas.

> **Note**
>
> Las consultas de CloudTrail Lake generan cargos según la cantidad de datos que se analizan. Para ayudar a controlar los costos, puede filtrar por un periodo más reducido. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

6. Elija Ejecutar consultas para ejecutar las consultas de los widgets del panel.

Filtrado de un panel por intervalo de fecha u hora

De forma predeterminada, el panel muestra los datos de las últimas 24 horas. Puede filtrar un panel por Intervalo absoluto o Intervalo relativo.

Elija Intervalo absoluto para seleccionar un intervalo de fechas y horas específico.

Elija Intervalo relativo para seleccionar un intervalo de tiempo predefinido o personalizado.

Una vez elegido el intervalo de tiempo, elija Ejecutar consultas para actualizar el panel.

> **Note**
>
> Las consultas de CloudTrail Lake generan cargos según la cantidad de datos que se analizan. Para ayudar a controlar los costos, puede filtrar por un periodo más reducido. Para obtener más información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Visualización de la consulta de un widget de panel

Cada widget representa una consulta SQL. Para ver la consulta de un widget, elija Ver y analizar en el editor de consultas para abrir el editor de consultas. Con el editor de consultas, puede ajustar aún más la consulta fuera del panel y ejecutarla para ver los resultados de la consulta actualizada. Para obtener más información acerca de cómo trabajar con consultas, consulte Creación o edición de una consulta.

> **Note**
>
> No puede modificar la consulta generada por el sistema para un widget de panel. Los cambios realizados en la consulta en la pestaña Editor de consultas solo servirán para efectuar un análisis más exhaustivo fuera del panel.

Consultas sobre Lake

Las consultas de CloudTrail Lake se crean en SQL. Puede crear una consulta en la pestaña Editor de CloudTrail Lake escribiendo la consulta en SQL desde cero o abriendo una consulta guardada o de muestra y editándola. No puede sobrescribir una consulta de muestra ya incluida con sus cambios, pero puede guardarla como una nueva consulta. Para obtener más información acerca del lenguaje de consulta SQL permitido, consulte CloudTrail Restricciones de Lake SQL.

Una consulta ilimitada (como `SELECT * FROM edsID`) analiza todos los datos de su almacén de datos de eventos. Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales `eventTime` de inicio y finalización a las consultas. A continuación, se muestra un ejemplo que realiza una búsqueda de todos los eventos en un almacén de datos de eventos especificado en el que la hora del evento es posterior (>) al 5 de enero de 2023 a la 13.51 h

y anterior (<) al 19 de enero de 2023 a las 13.51 h. Dado que un almacén de datos de eventos tiene un periodo de retención mínimo de siete días, el lapso de tiempo mínimo entre los valores `eventTime` iniciales y finales también es de siete días.

```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

Temas

- Creación o edición de una consulta
- Consultas de ejemplo
- Ejecutar una consulta y guardar los resultados de la consulta
- Visualización de los resultados de la consulta
- Obtener y descargar resultados de consultas guardados
- Validación de los resultados de consultas guardados

Creación o edición de una consulta

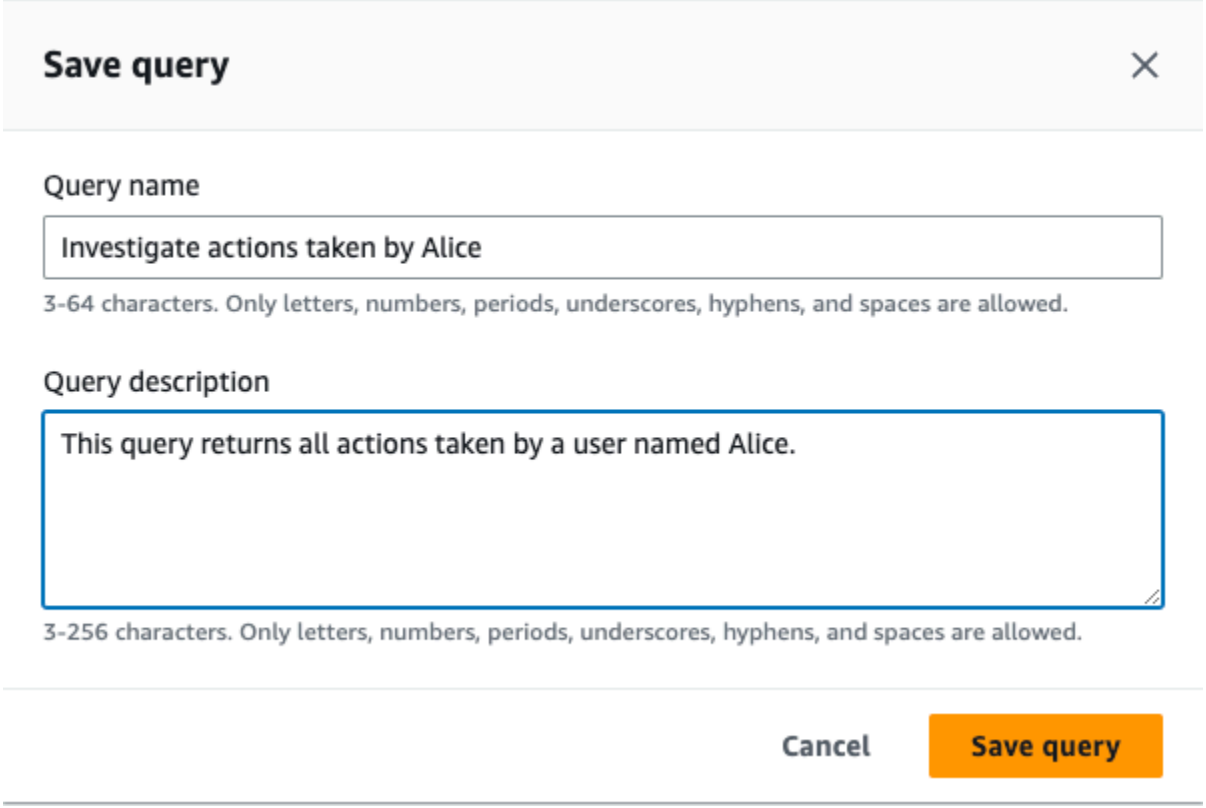
En este tutorial, abrimos una de las consultas de muestra, la editamos para buscar las acciones hechas por un usuario específico llamado `Alice` y la guardamos como una nueva consulta. También puede editar una consulta guardada en la pestaña Saved queries (Consultas guardadas), en caso de que tenga consultas guardadas Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales `eventTime` de inicio y finalización a las consultas.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Consulta.
3. En la página Query (Consultas), elija la pestaña Sample queries (Consultas de ejemplo).
4. Para abrir una consulta de ejemplo, elija el Nombre de la consulta. Esto abre la consulta en la pestaña Editor. En este ejemplo, seleccionaremos la consulta denominada Investigar acciones de usuarios y editaremos la consulta para buscar las acciones de un usuario específico denominado `Alice`.
5. En la pestaña Editor, edite la línea `WHERE` para especificar el usuario que desea investigar y actualice los valores de `eventTime` según sea necesario. El valor de `FROM` es la parte del ID

del ARN del almacén de datos de eventos y CloudTrail lo rellena automáticamente al elegir el almacén de datos de eventos.

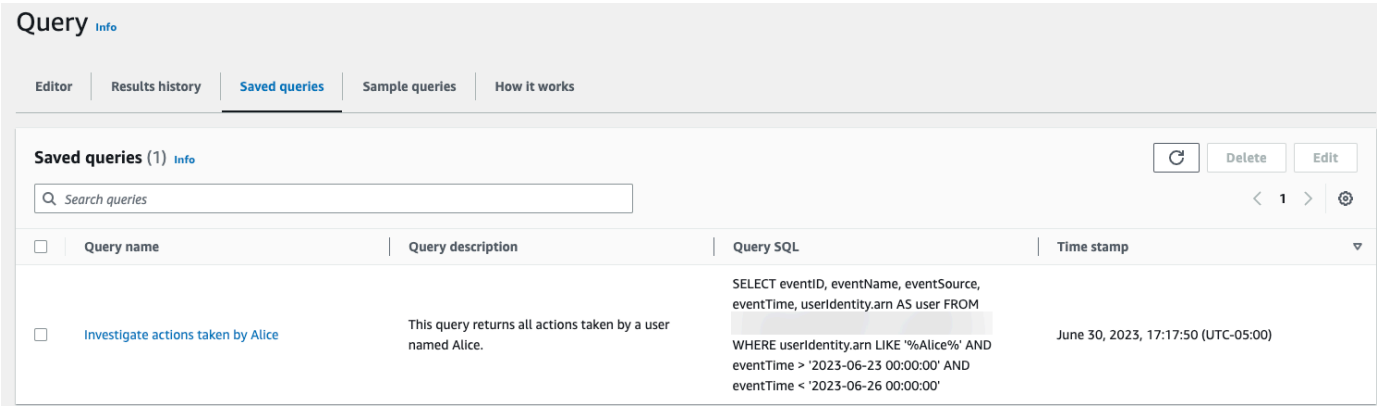
```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. Puede ejecutar una consulta antes de guardarla, para verificar que ésta funciona. Para ejecutar una consulta, elija un almacén de datos de eventos de la lista desplegable Event data store (Almacén de datos de eventos) y, a continuación, elija Run (Ejecutar). Compruebe la columna Status (Estado) de la pestaña Command output (Resultado del comando) de la consulta activa para verificar que la consulta se ha ejecutado correctamente.
7. Cuando haya actualizado la consulta de ejemplo, elija Guardar.
8. En Save query (Guardar consulta), ingrese un nombre y una descripción para la consulta. Elija Save query (Guardar consulta) para guardar los cambios como una nueva consulta. Para descartar los cambios en una consulta, elija Cancel (Cancelar) o cierre la ventana Save query (Guardar consulta).



> **Note**
>
> Las consultas guardadas están vinculadas al navegador. Si utiliza un navegador diferente o un dispositivo diferente para acceder a la consola de CloudTrail, las consultas guardadas no estarán disponibles.

9. Abra la pestaña Saved queries (Consultas guardadas) para ver la nueva consulta en la tabla.



Herramientas del editor de consultas

Una barra de herramientas situada en la parte superior derecha del editor de consultas ofrece comandos que ayudan a crear y dar formato a la consulta SQL.

La siguiente lista describe los comandos de la barra de herramientas.

- Undo (Deshacer): revierte el último cambio de contenido realizado en el editor de consultas.
- Redo (Rehacer): repite el último cambio de contenido realizado en el editor de consultas.
- Format selected (Formato seleccionado): organiza el contenido del editor de consultas de acuerdo con las convenciones de formato y espaciado de SQL.
- Comentar/descomentar seleccionado: comenta la parte de la consulta seleccionada si todavía no está comentada. Si la parte seleccionada ya está comentada, se elimina el comentario al seleccionar esta opción.

Consultas de ejemplo

La siguiente sección describe cómo puede acceder a consultas de ejemplo en la consola de CloudTrail Lake e incluye algunas consultas de CloudTrail Lake de ejemplo para ayudarlo a comenzar.

> **Note**
>
> Además, puede ver consultas creadas por la comunidad de GitHub. Para obtener más información y ver las consultas de ejemplo, consulte Consultas de ejemplo de CloudTrail Lake en el sitio web de GitHub. AWS CloudTrail no evaluó las consultas en GitHub.

Temas

- Visualización de consultas de ejemplo en la consola de CloudTrail
- Ejemplo: buscar todas las identidades de usuarios de entidades principales que llamaron a CreateBucket el 22 de enero de 2023
- Ejemplo: buscar todas las API a las que llamó un usuario el 22 de enero de 2023

- Ejemplo: buscar la cantidad de llamadas a la API desde el 1 de enero de 2023, agrupadas por eventName y eventSource
- Ejemplo: buscar todos los usuarios que iniciaron sesión en la consola en un conjunto de regiones
- Ejemplo: buscar todas las consultas de CloudTrail Lake que se ejecutaron en enero de 2023

Visualización de consultas de ejemplo en la consola de CloudTrail

La consola de CloudTrail brinda una serie de consultas de ejemplo que pueden ayudarlo a empezar a escribir sus propias consultas.

Para acceder a las consultas de ejemplo en la consola de CloudTrail

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Consulta.
3. Elija la pestaña Sample queries (Consultas de muestra).
4. Para editar una consulta de ejemplo, elija el Nombre de la consulta. Para obtener información sobre la ejecución de consultas, consulte Ejecutar una consulta y guardar los resultados de la consulta.

Ejemplo: buscar todas las identidades de usuarios de entidades principales que llamaron a **`CreateBucket`** el 22 de enero de 2023

```
SELECT
    userIdentity.principalid,
    eventName
FROM
    event_data_store_ID
WHERE
    userIdentity.principalid IS NOT NULL
AND
    eventTime > '2023-01-22 00:00:00'
AND
    eventTime < '2023-01-23 00:00:00'
AND
    eventName='CreateBucket'
```

Resultados

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 1,
        "TotalResultsCount": 1,
        "BytesScanned": 25077
    },
    "QueryResultRows": [
        [
            {
                "principalid": "principal_ID"
            },
            {
                "eventName": "CreateBucket"
            }
        ]
    ]
}
```

Ejemplo: buscar todas las API a las que llamó un usuario el 22 de enero de 2023

```
SELECT
    eventID,
    eventName,
    eventSource,
    eventTime
FROM
    event_data_store_ID
WHERE
    userIdentity.username = 'bob'
AND
    eventTime > '2023-01-22 00:00:00'
AND
    eventTime < '2023-01-23 00:00:00'
```

Resultados

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 2,
        "TotalResultsCount": 2,
```

```
        "BytesScanned": 13287
    },
    "QueryResultRows": [
        [
            {
                "eventID": "EXAMPLE-c3b6-43e4-aa35-b2490EXAMPLE"
            },
            {
                "eventName": "DescribeQuery"
            },
            {
                "eventSource": "cloudtrail.amazonaws.com"
            },
            {
                "eventTime": "2023-01-22 16:53:53.000"
            }
        ],
        [
            {
                "eventID": "EXAMPLE6-ac95-4b37-b587-76a80EXAMPLE"
            },
            {
                "eventName": "ListBuckets"
            },
            {
                "eventSource": "s3.amazonaws.com"
            },
            {
                "eventTime": "2023-01-22 20:25:01.000"
            }
        ]
    ]
}
```

Ejemplo: buscar la cantidad de llamadas a la API desde el 1 de enero de 2023, agrupadas por **`eventName`** y **`eventSource`**

```
SELECT
    eventSource,
    eventName,
    COUNT(*) AS apiCount
FROM
    event_data_store_ID
```

```
WHERE
    eventTime > '2023-01-01 00:00:00'
GROUP BY
    eventSource, eventName
ORDER BY
    apiCount DESC
```

Resultados

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 3,
        "TotalResultsCount": 3,
        "BytesScanned": 10442
    },
    "QueryResultRows": [
        [
            {
                "eventSource": "s3.amazonaws.com"
            },
            {
                "eventName": "PutObject"
            },
            {
                "apiCount": "96059"
            }
        ],
        [
            {
                "eventSource": "dynamodb.amazonaws.com"
            },
            {
                "eventName": "DescribeTable"
            },
            {
                "apiCount": "49426"
            }
        ],
        [
            {
                "eventSource": "sts.amazonaws.com"
            },
```

```
            {
                "eventName": "AssumeRole"
            },
            {
                "apiCount": "45617"
            }
        ]
    ]
}
```

Ejemplo: buscar todos los usuarios que iniciaron sesión en la consola en un conjunto de regiones

```
SELECT
    eventTime,
    useridentity.arn,
    awsRegion
FROM
    event_data_store_ID
WHERE
    awsRegion in ('us-east-1', 'us-west-2')
AND
    eventName = 'ConsoleLogin'
```

Resultados

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 2,
        "TotalResultsCount": 2,
        "BytesScanned": 15580
    },
    "QueryResultRows": [
        [
            {
                "eventTime": "2022-02-08 19:54:44.000"
            },
            {
                "arn": "arn:aws:sts::123456789012:assumed-role/example-identity"
            },
            {
```

```
                "awsRegion": "us-east-1"
            }
        ],
        [
            {
                "eventTime": "2022-01-21 16:38:27.000"
            },
            {
                "arn": "arn:aws:sts::123456789012:assumed-role/example-identity"
            },
            {
                "awsRegion": "us-west-2"
            }
        ]
    ]
}
```

Ejemplo: buscar todas las consultas de CloudTrail Lake que se ejecutaron en enero de 2023

```
SELECT
    element_at(responseElements, 'queryId'),
    element_at(requestParameters, 'queryStatement')
FROM
    event_data_store_ID
WHERE
    eventName='StartQuery'
AND
    eventSource = 'cloudtrail.amazonaws.com'
AND
    responseElements IS NOT NULL
AND
    eventTime > '2023-01-01 00:00:00'
AND
    eventTime < '2023-02-01 00:00:00'
```

Resultados

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 1,
```

```
        "TotalResultsCount": 1,
        "BytesScanned": 13002
    },
    "QueryResultRows": [
        [
            {
                "_col0": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE"
            },
            {
                "_col1": "select * from event_data_store_ID limit 1;"
            }
        ]
    ]
}
```

Ejecutar una consulta y guardar los resultados de la consulta

Después de elegir o guardar una consulta, puede ejecutarla en un almacén de datos de eventos.

Al ejecutar una consulta, tiene la opción de guardar los resultados de la consulta en un bucket de Amazon S3. Cuando ejecuta consultas en CloudTrail Lake, incurre en cargos según la cantidad de datos escaneados por la consulta. No hay cargos adicionales de CloudTrail Lake por guardar los resultados de las consultas en un bucket de S3; sin embargo, sí hay cargos por almacenamiento de S3. Para obtener más información acerca de los precios de S3, consulte Precios de Amazon S3.

Si se guardan los resultados de la consulta, estos pueden mostrarse en la consola de CloudTrail antes de que se puedan ver en el bucket de S3, ya que CloudTrail entrega los resultados de la consulta luego de finalizar el análisis de esta. Si bien la mayoría de las consultas se completan en unos minutos, según el tamaño del almacén de datos de eventos, CloudTrail puede tardar mucho más en entregar los resultados de las consultas a su bucket de S3. CloudTrail entrega los resultados de la consulta al bucket de S3 en formato gzip comprimido. De media, una vez que se complete el escaneo de la consulta, puede esperar una latencia de 60 a 90 segundos por cada GB de datos que se entregue al bucket de S3.

Para ejecutar una consulta con CloudTrail Lake

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Consulta.

3. En las pestañas Consultas guardadas o Consultas de ejemplo, elija el Nombre de la consulta para elegir una consulta para que se ejecute.
4. En la pestaña Editor (Editor), para Event data store (Almacén de datos de eventos), seleccione un almacén de datos de eventos de la lista desplegable.
5. (Opcional) En la pestaña Editor, elija Save results to S3 (Guardar resultados en S3) para guardar los resultados de la consulta en un bucket de S3. Cuando elige el bucket de S3 predeterminado, CloudTrail crea y aplica las políticas de bucket necesarias. Para obtener más información sobre cómo guardar los resultados de consultas, consulte Información adicional sobre los resultados de consultas guardados.

   > **Note**
   >
   > Para usar un bucket diferente, especifique un nombre de bucket o elija Browse S3 (Examinar S3) para elegir un bucket. La política del bucket debe conceder permiso a CloudTrail para que pueda enviar los resultados de las consultas al bucket. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake.

6. En la pestaña Editor (Editor), seleccione Run (Ejecutar).

   Dependiendo del tamaño de su almacén de datos de eventos y del número de días de datos que incluya, una consulta puede tardar varios minutos en ejecutarse. La pestaña Command output (Resultado del comando) muestra el estado de una consulta y si la consulta ha terminado de ejecutarse. Cuando una consulta haya terminado de ejecutarse, abra Query results (Resultados de la consulta) para ver una tabla de resultados de la consulta activa (la consulta que se muestra actualmente en el editor).

> **Note**
>
> Es posible que las consultas que se ejecuten durante más de una hora agoten el tiempo de espera. Aun así, puede que obtenga resultados parciales que se hayan procesado antes de que se agotara el tiempo de espera de la consulta. CloudTrail no entrega resultados de consultas parciales a un bucket de S3. Para evitar que se agote el tiempo de espera, puede refinar la consulta para limitar la cantidad de datos escaneados si especifica un intervalo de tiempo más estrecho.

Información adicional sobre los resultados de consultas guardados

Después de guardar los resultados de la consulta, puede descargar los resultados de la consulta guardados desde el bucket de S3. Para obtener más información sobre la búsqueda y descarga de los resultados de consultas guardados, consulte Obtener y descargar resultados de consultas guardados.

También puede validar los resultados de consultas guardados para determinar si los resultados de consultas se han modificado, eliminado o continúan igual después de que CloudTrail los envió. Para obtener más información sobre la validación de resultados de consultas guardados, consulte Validación de los resultados de consultas guardados.

Visualización de los resultados de la consulta

Una vez finalizada la consulta, puede ver los resultados. Los resultados de una consulta están disponibles durante siete días después de la finalización de la misma. Puede ver los resultados de la consulta activa en la pestaña Query results (Resultados de la consulta) o puede acceder a los resultados de todas las consultas recientes en la pestaña Results history (Historial de resultados) de la página principal de Lake.

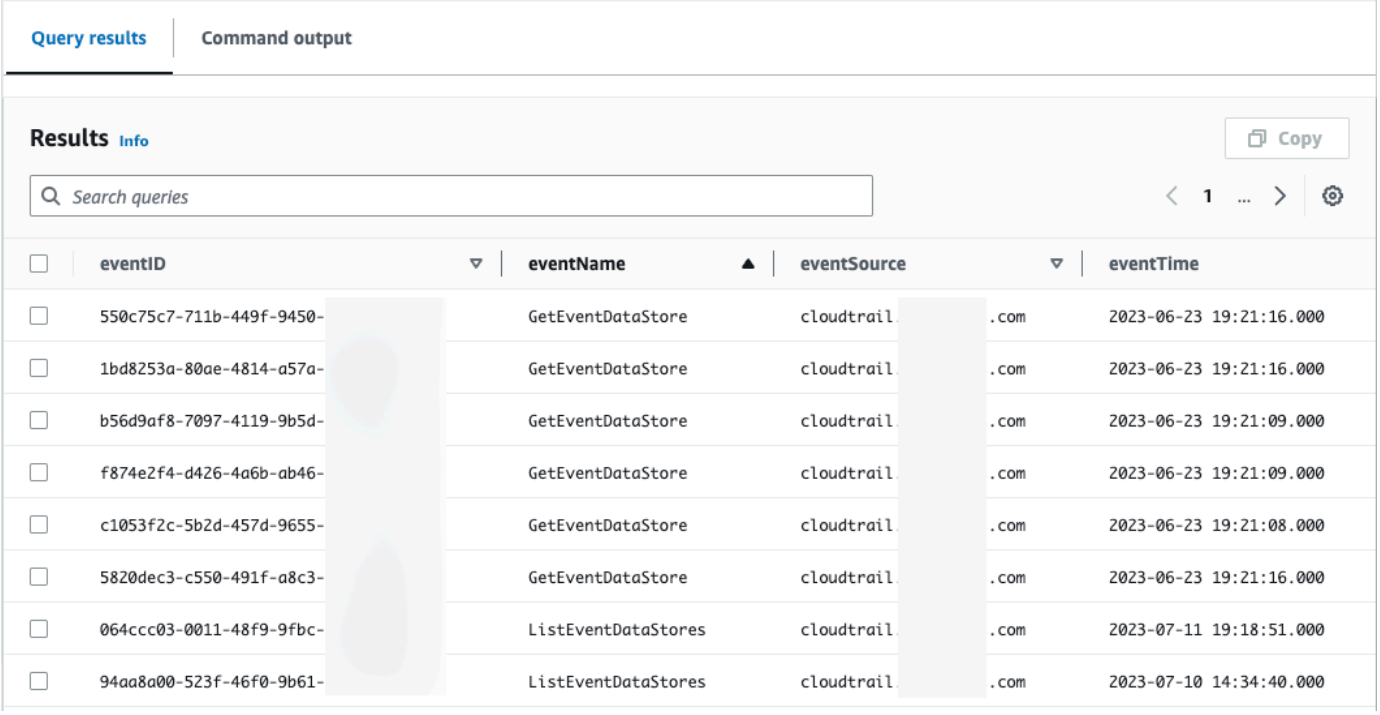
Los resultados de la consulta pueden cambiar de las ejecuciones más antiguas de una consulta a las más recientes, ya que se pueden registrar eventos posteriores en el periodo de la consulta entre consultas.

Si se guardan los resultados de la consulta, estos pueden mostrarse en la consola de CloudTrail antes de que se puedan ver en el bucket de S3, ya que CloudTrail entrega los resultados de la consulta luego de finalizar el análisis de esta. Si bien la mayoría de las consultas se completan en unos minutos, según el tamaño del almacén de datos de eventos, CloudTrail puede tardar mucho más en entregar los resultados de las consultas a su bucket de S3. CloudTrail entrega los resultados de la consulta al bucket de S3 en formato gzip comprimido.
De media, una vez que se complete el análisis de la consulta, puede esperar una latencia de 60 a 90 segundos por cada GB de datos que se entrega al bucket de S3. Para obtener más información sobre la búsqueda y descarga de los resultados de consultas guardados, consulte Obtener y descargar resultados de consultas guardados.

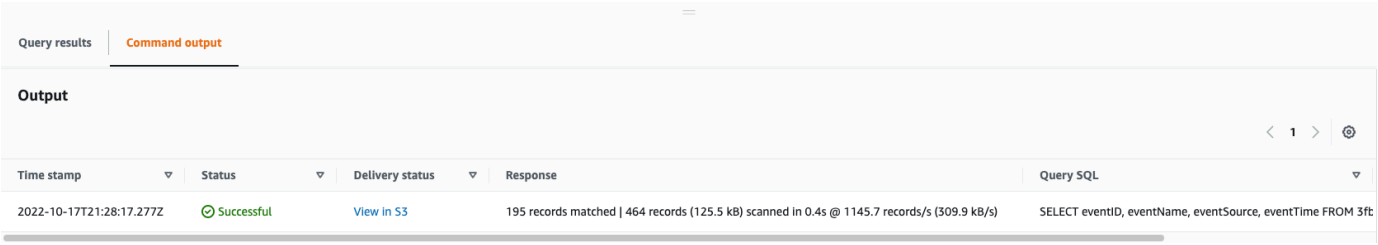
> **Note**
>
> Es posible que las consultas que se ejecuten durante más de una hora agoten el tiempo de espera. Aun así, puede que obtenga resultados parciales que se hayan procesado antes

de que se agotara el tiempo de espera de la consulta. CloudTrail no entrega resultados de consultas parciales a un bucket de S3. Para evitar que se agote el tiempo de espera, puede refinar la consulta para limitar la cantidad de datos escaneados si especifica un intervalo de tiempo más estrecho.

1. En la pestaña Query results (Resultados de la consulta) para una consulta activa, cada fila representa un resultado de evento que coincide con la consulta. Filtre los resultados introduciendo en la barra de búsqueda la totalidad o parte del valor de un campo de evento. Para copiar un evento, elija el evento que desee copiar y, a continuación, elija Copiar.



2. En la pestaña Command output (Resultado del comando), puede visualizar los metadatos de la consulta que se ha ejecutado, como el ID del almacén de datos de eventos, la hora de ejecución, el número de resultados escaneados y si la consulta se ha ejecutado correctamente o no. Si guardó los resultados de la consulta en un bucket de Amazon S3, los metadatos también incluyen un enlace al bucket de S3 que contiene los resultados de la consulta guardados.



Obtener y descargar resultados de consultas guardados

Después de guardar los resultados de la consulta, debe poder localizar el archivo que contiene los resultados de la consulta. CloudTrail entrega los resultados de la consulta al bucket de Amazon S3 que especifique al guardar los resultados de la consulta.

> **Note**
>
> Al guardar los resultados de la consulta, los resultados de la consulta pueden mostrarse en la consola antes de que se puedan ver en el bucket de S3, ya que CloudTrail entrega los resultados de la consulta una vez finalizado el análisis de la consulta. Si bien la mayoría de las consultas se completan en unos minutos, según el tamaño del almacén de datos de eventos, CloudTrail puede tardar mucho más en entregar los resultados de las consultas a su bucket de S3. CloudTrail entrega los resultados de la consulta al bucket de S3 en formato gzip comprimido. De media, una vez que se complete el escaneo de la consulta, puede esperar una latencia de 60 a 90 segundos por cada GB de datos que se entregue al bucket de S3.

Temas

- Buscar resultados de consultas guardados de CloudTrail
- Descargar los resultados de consultas guardados de CloudTrail Lake

Buscar resultados de consultas guardados de CloudTrail

CloudTrail publica archivos de resultados de consultas y de firma en su bucket de S3. El archivo de resultados de consultas contiene el resultado de la consulta guardada y el archivo de firma proporciona la firma y el valor de hash de los resultados de la consulta. Puede usar el archivo de firma para validar los resultados de la consulta. Para obtener más información sobre la validación de resultados de consultas, consulte Validación de los resultados de consultas guardados.

Para recuperar un archivo de firma o de resultados de consultas, puede usar la consola de Amazon S3, la interfaz de línea de comandos (CLI) de Amazon S3 o la API.

Para buscar archivos de firma y de resultados de consultas con la consola de Amazon S3

1. Abra la consola de Amazon S3.

2. Elija el bucket especificado.
3. Recorra la jerarquía de objetos hasta que encuentre los archivos de firma y de resultados de consultas. El archivo de resultados de consultas tiene una extensión .csv.gz y el archivo de firma tiene una extensión .json.

Verá una jerarquía de objetos similar a la del siguiente ejemplo, pero con diferente nombre de bucket, ID de cuenta, fecha e ID de consulta.

```
All Buckets
    Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

Descargar los resultados de consultas guardados de CloudTrail Lake

Al guardar resultados de consultas, CloudTrail entrega dos tipos de archivos a su bucket de Amazon S3.

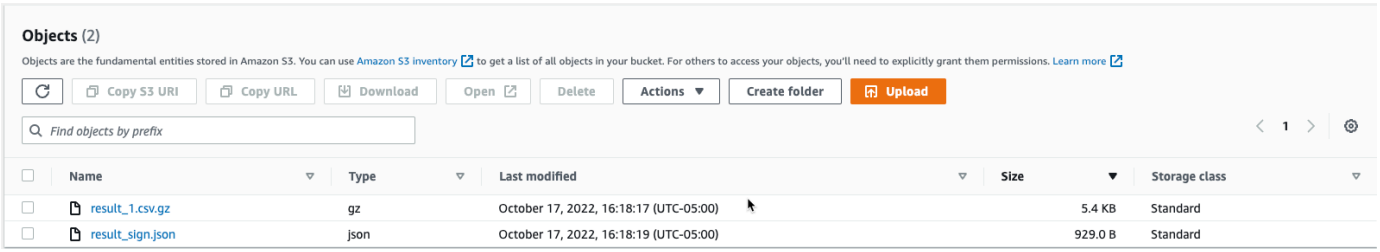
- Un archivo de firma en formato JSON que puede usar para validar los archivos de resultados de consultas. El archivo de firma se denomina result_sign.json. Para obtener más información acerca del archivo de firma, consulte Estructura de los archivos de firma de CloudTrail.
- Uno o más archivos de resultados de consultas en formato CSV, los cuales contienen los resultados de la consulta. El número de archivos de resultados de consultas entregados depende del tamaño total de los resultados de la consulta. El tamaño de archivo máximo de un archivo de resultados de consultas es de 1 TB. Cada archivo de resultados de consultas se denomina result_*number*.csv.gz. Por ejemplo, si el tamaño total de los resultados de la consulta era de 2 TB, tendría dos archivos de resultados de la consulta, result_1.csv.gz y result_2.csv.gz.

Los archivos de firma y de resultados de consultas de CloudTrail son objetos de Amazon S3. Para recuperar los archivos de firma y de resultados de consultas, puede usar la consola de S3, la AWS Command Line Interface (CLI) o la API de S3.

En el procedimiento siguiente se describe cómo descargar el resultado de la consulta y los archivos de firma con la consola de Amazon S3.

Para descargar el resultado de la consulta o el archivo de firma con la consola de Amazon S3

1. Abra la consola de Amazon S3.
2. Elija el bucket y el archivo que desea descargar.



3. Elija Download (Descargar) y siga las instrucciones para guardar el archivo.

> **Note**
>
> Algunos navegadores, como Chrome, extraen automáticamente el archivo de resultados de consultas por usted. Si lo hace así su navegador, vaya al paso 5.

4. Use un producto como 7-Zip para extraer el archivo de resultados de consultas.
5. Abra el archivo de firma o de resultados de consultas.

Validación de los resultados de consultas guardados

Para determinar si los resultados de la consulta se han modificado, eliminado o continúan igual después de que CloudTrail los envió, puede usar la validación de integridad de los resultados de las consultas de CloudTrail. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto de vista informático modificar, eliminar o falsificar archivos de resultados de consultas de CloudTrail sin que se detecte. Puede usar la línea de comandos para validar los archivos de resultados de consultas.

¿Por qué utilizarla?

Los archivos de resultados de consultas validados son muy valiosos para las investigaciones de seguridad y forenses. Por ejemplo, un archivo de resultados de consultas validado le permite afirmar de forma positiva que el archivo de resultados de la consulta en sí no ha cambiado. El proceso de

validación de integridad de los archivos de resultados de consultas de CloudTrail también le permiten saber si un archivo de resultados de consultas se ha eliminado o modificado.

Temas

- Validar los resultados de consultas guardados con la AWS CLI
- Estructura de los archivos de firma de CloudTrail
- Implementaciones personalizadas para validar la integridad de los archivos de resultados de consultas de CloudTrail

Validar los resultados de consultas guardados con la AWS CLI

Puede validar la integridad de los archivos de resultados de la consulta y el archivo de firma mediante el comando aws cloudtrail verify-query-results.

Requisitos previos

Para validar la integridad de los resultados de la consulta con la línea de comandos, deben cumplirse las siguientes condiciones:

- Debe disponer de conectividad en línea a AWS.
- Debe utilizar la versión 2 de la AWS CLI.
- Para validar los archivos de resultados de la consulta y el archivo de firma de forma local, se aplican las siguientes condiciones:
  - Debe colocar los archivos de resultados de la consulta y el archivo de firma en la ruta de archivo especificada. Especifique la ruta del archivo como valor del parámetro --local-export-path.
  - No debe cambiar el nombre de los archivos de resultados de la consulta ni del archivo de firma.
- Para validar los archivos de resultados de la consulta y el archivo de firma en el bucket de S3, se aplican las siguientes condiciones:
  - No debe cambiar el nombre de los archivos de resultados de la consulta ni del archivo de firma.
  - Debe disponer de acceso de lectura al bucket de Amazon S3 que contiene los archivos de resultados de la consulta y el archivo de firma.
  - El prefijo de S3 especificado debe contener los archivos de resultados de la consulta y el archivo de firma. Especifique el prefijo de S3 como valor del parámetro --s3-prefix.

verify-query-results

El comando verify-query-results verifica el valor de hash de cada archivo de resultados de la consulta comparando el valor con el valor de `fileHashValue` del archivo de firma y, a continuación, validando el valor de `hashSignature` del archivo de firma.

Al comprobar los resultados de la consulta, puede utilizar las opciones --s3-bucket y --s3-prefix de la línea de comandos para validar los archivos de resultados de la consulta y el archivo de firma almacenados en un bucket de S3, o bien puede utilizar la opción --local-export-path de la línea de comandos para llevar a cabo una validación local de los archivos de resultados de la consulta y del archivo de firma descargados.

> **Note**
>
> El comando verify-query-results es específico de la región. Debe especificar la opción global --region para validar los resultados de la consulta de una Región de AWS específica.

A continuación se enumeran las opciones del comando verify-query-results.

--s3-bucket *<cadena>*

Especifica el nombre del bucket de S3 que almacena los archivos de resultados de la consulta y el archivo de firma. No puede utilizar este parámetro con --local-export-path.

--s3-prefix *<cadena>*

Especifica la ruta de S3 de la carpeta de S3 que contiene los archivos de resultados de la consulta y el archivo de firma (por ejemplo, `s3/path/`). No puede utilizar este parámetro con --local-export-path. No es necesario proporcionar este parámetro si los archivos están ubicados en el directorio raíz del bucket de S3.

--local-export-path *<cadena>*

Especifica el directorio local que contiene los archivos de resultados de la consulta y el archivo de firma (por ejemplo, `/local/path/to/export/file/`). No puede utilizar este parámetro con --s3-bucket o --s3-prefix.

Ejemplos

En el siguiente ejemplo, se validan los resultados de la consulta mediante las opciones --s3-bucket y --s3-prefix de la línea de comandos para especificar el nombre y el prefijo del bucket de S3 que contienen los archivos de resultados de la consulta y el archivo de firma.

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

En el siguiente ejemplo, se validan los resultados de la consulta descargados mediante la opción --local-export-path de la línea de comandos para especificar la ruta de acceso local de los archivos de resultados de la consulta y el archivo de firma. Para obtener información sobre la descarga de los archivos de resultados de la consulta, consulte Descargar los resultados de consultas guardados de CloudTrail Lake.

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

Resultados de la validación

En la siguiente tabla se describen los posibles mensajes de validación para los archivos de resultados de la consulta y el archivo de firma.

Tipo de archivo	Mensaje de validación	Descripción
`Sign file`	`Successfully validated sign and query result files`	La firma del archivo de firma es válida. Se pueden comprobar los archivos de resultados de la consulta a los que hace referencia.
`Query result file`	`ValidationError: "File` *`file_name`* `has inconsistent hash value with hash value recorded in sign file, hash value in sign file is` *`expected_hash`* `, but get` *`computed_hash`*	Se ha producido un error en la validación porque el valor hash del archivo de resultados de la consulta no coincide con el valor de `fileHashValue` del archivo de firma.

Tipo de archivo	Mensaje de validación	Descripción
`Sign file`	`ValidationError: Invalid signature in sign file`	Se ha producido un error en la validación del archivo de firma porque la firma no es válida.

Estructura de los archivos de firma de CloudTrail

El archivo de firma contiene el nombre de cada archivo de resultados de la consulta que se envió al bucket de Amazon S3 al guardar los resultados de la consulta, el valor hash de cada archivo de resultados de la consulta y la firma digital del archivo. La firma digital y los valores hash se usan para validar la integridad de los archivos de resultados de consultas y del archivo de firma en sí.

Ubicación del archivo de firma

El archivo de firma se envía a una ubicación de bucket de Amazon S3 con la siguiente sintaxis.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

Contenido del archivo de firma de ejemplo

El siguiente ejemplo de archivo de firma contiene información de resultados de consultas de CloudTrail.

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
```

```
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

Descripciones de los campos de los archivos de firma

Las siguientes son descripciones de cada campo del archivo de firma:

`version`

La versión del archivo de firma.

`region`

La región de la cuenta de AWS usada para guardar los resultados de la consulta.

`files.fileHashValue`

El valor hash codificado hexadecimal del contenido del archivo de resultados de consultas comprimido.

`files.fileName`

El nombre del archivo de resultados de consultas.

`hashAlgorithm`

El algoritmo hash que se usa para el archivo de resultados de consultas.

`signatureAlgorithm`

El algoritmo que se usa para firmar el archivo.

`queryCompleteTime`

Indica cuándo CloudTrail entregó los resultados de la consulta al bucket S3. Puede usar este valor para buscar la clave pública.

`hashSignature`

La firma hash del archivo.

`publicKeyFingerprint`

La huella digital codificada hexadecimal de la clave pública usada para firmar el archivo.

Implementaciones personalizadas para validar la integridad de los archivos de resultados de consultas de CloudTrail

Dado que CloudTrail emplea funciones hash y algoritmos criptográficos estándar del sector disponibles abiertamente, puede crear sus propias herramientas para validar la integridad de los archivos de resultados de consultas de CloudTrail. Al guardar los resultados de las consultas en un bucket de Amazon S3, CloudTrail entrega un archivo de firma a su bucket de S3. Puede implementar su propia solución de validación para validar la firma y los archivos de resultados de consultas. Para obtener más información acerca del archivo de firma, consulte Estructura de los archivos de firma de CloudTrail.

En este tema se describe cómo se firman los archivos de firma, y a continuación, se detallan los pasos que debe seguir para implementar una solución que valide el archivo de firma y los archivos de resultados de consultas a los que hace referencia.

Cómo se firman los archivos de firma de CloudTrail

Los archivos de firma de CloudTrail se firman con firmas digitales RSA. Para cada archivo de firma, CloudTrail hace lo siguiente:

1. Crea una lista de hash que contiene el valor de hash de cada archivo de resultados de la consulta.
2. Obtiene una clave privada única para la región.
3. Pasa el hash SHA-256 de la cadena y la clave privada al algoritmo de firma RSA, que produce una firma digital.
4. Codifica el código de bytes de la firma en formato hexadecimal.
5. Coloca la firma digital en el archivo de firma.

Contenido de la cadena de firma de datos

La cadena de firma de datos consiste en el valor de hash de cada archivo de resultados de la consulta separado por un espacio. El archivo de firma muestra el `fileHashValue` por cada archivo de resultados de la consulta.

Pasos de implementación de la validación personalizada

Cuando implemente una solución de validación personalizada, deberá validar en primer lugar el archivo de firma y, a continuación, los archivos de resultado de la consulta a los que hace referencia.

Validar el archivo de firma

Para validar un archivo de firma, necesita su firma, la clave pública cuya clave privada se ha usado para firmarlo y una cadena de firma de datos que debe calcular.

1. Obtenga el archivo de firma.
2. Compruebe que el archivo de firma se haya recuperado de su ubicación original.
3. Obtenga la firma en codificación hexadecimal del archivo de firma.
4. Obtenga la huella en codificación hexadecimal de la clave pública cuya clave privada se ha usado para firmar el archivo de firma.
5. Recupere la clave pública para el intervalo de tiempo correspondiente a `queryCompleteTime` en el archivo de firma. Para el intervalo de tiempo, elija un `StartTime` anterior a `queryCompleteTime` y otro `EndTime` posterior a `queryCompleteTime`.
6. De entre las claves públicas recuperadas, elija la clave pública cuya huella coincida con el valor `publicKeyFingerprint` en el archivo de firma.
7. Mediante una lista de hash que contenga el valor de hash de cada archivo de resultados de la consulta separado por un espacio, vuelva a crear la cadena de firma de datos usada para verificar la firma del archivo de firma. El archivo de firma muestra el `fileHashValue` por cada archivo de resultados de la consulta.

   Por ejemplo, si la matriz `files` del archivo de firma contiene los siguientes tres archivos de resultados de la consulta, la lista de hash será “aaa bbb ccc”.

```
“files": [

   {
```

```
        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"

    },
    {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

    },
    {

        "fileHashValue" : “ccc”,

        "fileName" : "result_3.csv.gz"

    }
],
```

8. Valide la firma pasando el hash SHA-256 de la cadena, la clave pública y la firma como parámetros al algoritmo de verificación de firmas RSA. Si el resultado es verdadero, el archivo de firma es válido.

Validar los archivos de resultados de consultas

Si el archivo de firma es válido, valide los archivos de resultados de la consulta a los que hace referencia el archivo de firma. Para validar la integridad de un archivo de resultados de consulta, calcule su valor de hash SHA-256 en su contenido comprimido y compare los resultados con el `fileHashValue` del archivo de resultados de la consulta registrado en el archivo de firma. Si los hash coinciden, el archivo de resultados de la consulta es válido.

En las siguientes secciones se describe el proceso de validación de manera detallada.

A. Obtener el archivo de firma

Los primeros pasos son obtener el archivo de firma y obtener la huella digital de la clave pública.

1. Obtenga el archivo de firma de su bucket de Amazon S3 para los resultados de la consulta que desea validar.
2. A continuación, obtenga el valor `hashSignature` del archivo de firma.

3. En el archivo de firma, obtenga la huella de la clave pública cuya clave privada se ha usado para firmar el archivo de firma en el campo `publicKeyFingerprint`.

B. Recuperar la clave pública para validar el archivo de firma

Para obtener la clave pública para validar el archivo de firma, puede usar la AWS CLI o la API de CloudTrail. En ambos casos, debe especificar un intervalo de tiempo (es decir, una hora de inicio y una de finalización) para el archivo de firma que desea validar. Use un intervalo de tiempo correspondiente al `queryCompleteTime` del archivo de firma. Se podrían devolver una o varias claves públicas para el intervalo de tiempo que se especifique. Las claves devueltas pueden tener intervalos de tiempo de validez que se solapan.

> **Note**
>
> Dado que CloudTrail usa diferentes pares de claves públicas/privadas por región, cada archivo de firma se firma con una clave privada única para su región. Por lo tanto, al validar un archivo de firma desde una región determinada, debe recuperar su clave pública desde la misma región.

Utilizar la AWS CLI para recuperar claves públicas

A fin de recuperar una clave pública para un archivo de firma mediante la AWS CLI, use el comando `cloudtrail list-public-keys`. El comando tiene el siguiente formato:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Los parámetros de la hora de inicio y de finalización son marcas de tiempo UTC (opcionales). Si no se especifica, se utiliza la hora actual y se devuelven las claves públicas que actualmente están activas.

Respuesta de ejemplo

La respuesta será una lista de objetos JSON que representan las claves devueltas:

Utilice la API de CloudTrail para recuperar claves públicas

Para recuperar una clave pública para un archivo de firma mediante la API de CloudTrail, pase los valores de la hora de inicio y finalización a la API `ListPublicKeys`. La API `ListPublicKeys`

devuelve las claves públicas cuyas claves privadas se han usado para firmar el archivo en el intervalo de tiempo especificado. Para cada clave pública, la API también devuelve la huella correspondiente.

`ListPublicKeys`

En esta sección se describen los parámetros de solicitud y los elementos de respuesta de la API `ListPublicKeys`.

> **Note**
>
> La codificación de los campos binarios de `ListPublicKeys` está sujeta a cambios.

Parámetros de solicitud

Nombre	Descripción
`StartTime`	Opcionalmente, especifica el inicio del intervalo de tiempo (en UTC) para buscar la clave pública para el archivo de firma de CloudTrail. Si StartTime no está especificado, se utiliza la hora actual y se devuelve la clave pública actual. Tipo: DateTime
`EndTime`	Opcionalmente, especifica el fin del intervalo de tiempo (en UTC) para buscar las claves públicas para los archivos de firma de CloudTrail. Si EndTime no está especificado, se utiliza la hora actual. Tipo: DateTime

Elementos de respuesta

`PublicKeyList`, una matriz de objetos `PublicKey` que contiene:

Nombre	Descripción
`Value`	El valor de clave pública codificado de DER en formato PKCS # 1.

	Tipo: Blob
`ValidityStartTime`	La hora de inicio de la validez de la clave pública. Tipo: DateTime
`ValidityEndTime`	La hora de finalización de la validez de la clave pública. Tipo: DateTime
`Fingerprint`	La huella de la clave pública. La huella puede usarse para identificar la clave pública que debe usar para validar el archivo de firma. Tipo: String

C. Elegir la clave pública que va a utilizar para la validación

De entre las claves públicas recuperadas por `list-public-keys` o `ListPublicKeys`, elija la clave pública cuya huella coincida con la huella registrada en el campo `publicKeyFingerprint` del archivo de firma. Esta es la clave pública que usará para validar el archivo de firma.

D. Volver a crear la cadena de la firma de datos

Ahora que ya tiene la firma del archivo de firma y la clave pública asociada, debe calcular la cadena de firma de datos. Después de haber calculado la cadena de la firma de datos, tendrá las entradas necesarias para verificar la firma.

La cadena de firma de datos consiste en el valor de hash de cada archivo de resultados de la consulta separado por un espacio. Después de volver a crear esta cadena, puede validar el archivo de firma.

E. Validar el archivo de firma

Pase la cadena de firma de datos recreada, la firma digital y la clave pública al algoritmo de verificación de la firma RSA. Si el resultado es verdadero, la firma del archivo de firma se verifica y el archivo de firma es válido.

F. Validar los archivos de resultados de consultas

Una vez que haya validado el archivo de firma, puede validar los archivos de resultados de la consulta a los que hace referencia. El archivo de firma contiene hashes SHA-256 de los archivos de

resultados de consultas. Si uno de los archivos de resultado de la consulta se ha modificado después de que CloudTrail lo haya entregado, los hashes SHA-256 cambiarán y la firma del archivo de firma no coincidirá.

Use el siguiente procedimiento para validar los archivos de resultados de la consulta que figuran en la matriz `files` del archivo de firma.

1. Recupere el hash original del archivo desde el campo `files.fileHashValue` en el archivo de firma.
2. Convierta en hash el contenido comprimido del archivo de resultados de la consulta con el algoritmo de hash especificado en `hashAlgorithm`.
3. Compare el valor de hash que ha generado para cada archivo de resultados de la consulta con el `files.fileHashValue` del archivo de firma. Si los hashes coinciden, los archivos de resultados de la consulta son válidos.

Validación de archivos de resultados de consultas y firmas sin conexión

Cuando valida archivos de resultados de consultas y firmas sin conexión, generalmente puede seguir los procedimientos descritos en las secciones anteriores. Sin embargo, debe tener en cuenta la siguiente información sobre las claves públicas.

Claves públicas

Para realizar la validación sin conexión, primero se debe obtener en línea la clave pública que necesita para validar los archivos de resultados de consultas en un intervalo de tiempo determinado (al llamar a `ListPublicKeys`, por ejemplo) y, a continuación, guardarla sin conexión. Este paso debe repetirse siempre que desee validar más archivos fuera del intervalo de tiempo inicial especificado.

Fragmento de código de validación de ejemplo

El siguiente fragmento de código de ejemplo muestra el código básico para validar archivos de firma y archivos de resultados de consultas de CloudTrail. El código básico no depende del estado en línea o sin conexión; es decir, el usuario es quien debe decidir si lo implementará en línea o sin conexión a AWS. La implementación sugerida utiliza Java Cryptography Extension (JCE) y Bouncy Castle como proveedor de seguridad.

En el fragmento de código de ejemplo, se muestra lo siguiente:

- Cómo crear la cadena de firma de datos que se usa para validar la firma de archivos de firma.

- Cómo verificar la firma del archivo de firma.
- Cómo calcular el valor de hash del archivo de resultados de consultas y compararlo con el `fileHashValue` que aparece en el archivo de firma para comprobar la autenticidad del archivo de resultados de consultas.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();
```

```
        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3ObjectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                        s3Bucket, fileS3ObjectKey,
                        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                        s3Bucket, fileS3ObjectKey));
            }

            hashList.add(file.getString("fileHashValue"));
        }
        String hashListString = hashList.stream().collect(Collectors.joining(" "));

        /*
            NOTE:
            To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
            of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
            returned from ListPublicKey API are DER encoded in PKCS#1 format:

            PublicKeyInfo ::= SEQUENCE {
                algorithm       AlgorithmIdentifier,
                PublicKey       BIT STRING
            }
```

```
            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
rsaPublicKey);

        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

Recursos de aprendizaje

Los siguientes recursos pueden ayudarlo a comprender mejor qué es CloudTrail Lake y cómo puede utilizarlo.

- Modernice la gestión de sus registros de auditoría con CloudTrail Lake (video de YouTube)

- Log Activity Events from Non-AWS Sources in AWS CloudTrail Lake (video de YouTube)
- Obtenga visibilidad de los registros de actividad de las identidades de sus empleados y clientes (Blog de AWS)
- Uso de AWS CloudTrail Lake para identificar conexiones TLS antiguas a puntos de conexión de servicio de AWS (Blog de AWS)
- Cómo Arctic Wolf utiliza AWS CloudTrail Lake para simplificar la seguridad y las operaciones (Blog de AWS)
- Preguntas frecuentes sobre CloudTrail Lake
- Referencia de la API de AWS CloudTrail
- Referencia de la API de datos de AWS CloudTrail
- Guía de incorporación de socios de AWS CloudTrail

Administrar CloudTrail Lake mediante la AWS CLI

Los siguientes son comandos de muestra de la AWS CLI para crear y administrar almacenes de datos de eventos y consultas en CloudTrail Lake.

Temas

- Crear un almacén de datos de eventos con la AWS CLI
- Importar eventos de registros de seguimiento a un almacén de datos de eventos con la AWS CLI
- Crear una integración para registrar eventos externos a AWS con la AWS CLI
- Obtener un almacén de datos de eventos con la AWS CLI
- Enumerar todos los almacenes de datos de eventos de una cuenta con la AWS CLI
- Actualizar un almacén de datos de eventos con la AWS CLI
- Detener la incorporación en un almacén de datos de eventos con la AWS CLI
- Iniciar la incorporación en un almacén de datos de eventos con la AWS CLI
- Habilitar la federación en un almacén de datos de eventos
- Deshabilitar la federación en un almacén de datos de eventos
- Eliminar un almacén de datos de eventos con la AWS CLI
- Restaurar un almacén de datos de eventos con la AWS CLI
- Enumerar todos los canales con la AWS CLI
- Actualizar un canal con la AWS CLI

- Eliminar un canal para eliminar una integración con la AWS CLI
- Iniciar una consulta con la AWS CLI
- Obtener metadatos sobre una consulta con la AWS CLI
- Obtener los resultados de consultas con la AWS CLI
- Enumerar todas las consultas en un almacén de datos de eventos con la AWS CLI
- Cancelar una consulta en curso con la AWS CLI

Crear un almacén de datos de eventos con la AWS CLI

Utilice el comando `create-event-data-store` para crear un almacén de datos de eventos.

Cuando crea un almacén de datos de eventos, el único parámetro requerido es `--name` que se utiliza para identificar el almacén de datos de eventos. Puede configurar parámetros opcionales adicionales, que incluyen:

- `--advanced-event-selectors`: especifica el tipo de eventos que desea incluir en el almacén de datos de eventos. De forma predeterminada, los almacenes de datos de eventos registran eventos de administración. Para obtener más información acerca de los selectores de eventos avanzados, consulte AdvancedEventSelector en la Referencia de la API de CloudTrail.
- `--kms-key-id`: especifica el ID de la clave de AWS KMS que se va a utilizar para cifrar los eventos entregados por CloudTrail. El valor puede ser un nombre de alias con un prefijo de `alias/`, un ARN totalmente especificado a un alias, un ARN totalmente especificado a una clave o un identificador único global.
- `--multi-region-enabled`: crea un almacén de datos de eventos de varias regiones que registra los eventos de todas las Regiones de AWS de su cuenta. De forma predeterminada, `--multi-region-enabled` está configurada, aunque no se agregue el parámetro.
- `--organization-enabled`: habilita a un almacén de datos de eventos para que recopile los eventos de todas las cuentas de una organización. De forma predeterminada, el almacén de datos de eventos no está habilitado para todas las cuentas de una organización.
- `--billing-mode`: determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención máximo y predeterminado del almacén de datos de eventos.

  A continuación se muestran los posibles valores:

  - `EXTENDABLE_RETENTION_PRICING`: por lo general, se recomienda este modo de facturación si consume menos de 25 TB de datos de eventos al mes y desea un periodo de retención

flexible de hasta 3653 días (unos 10 años). El periodo de retención predeterminado para este modo de facturación es de 366 días.

- `FIXED_RETENTION_PRICING`: se recomienda este modo de facturación si piensa incorporar más de 25 TB de datos de eventos al mes y necesita un periodo de retención de hasta 2557 días (unos 7 años). El periodo de retención predeterminado para este modo de facturación es de 2557 días.

El valor predeterminado es `EXTENDABLE_RETENTION_PRICING`.

- `--retention-period`: la cantidad de días que se van a conservar los eventos en el almacén de datos de eventos. Los valores válidos son enteros entre 7 y 3653 si el `--billing-mode` es `EXTENDABLE_RETENTION_PRICING`, o entre 7 y 2557 si el `--billing-mode` está establecido en `FIXED_RETENTION_PRICING`. Si no especifica el `--retention-period`, CloudTrail utiliza el periodo de retención predeterminado para el `--billing-mode`.
- `--start-ingestion`: el parámetro `--start-ingestion` inicia la incorporación de eventos en el almacén de datos de eventos cuando se crea. Este parámetro se establece aunque no se agregue.

  Especifique `--no-start-ingestion` si no quiere que el almacén de datos de eventos incorpore eventos en vivo. Por ejemplo, es posible que desee establecer este parámetro si está copiando eventos al almacén de datos de eventos y solo piensa usar los datos de eventos para analizar los eventos pasados. El parámetro `--no-start-ingestion` solo es válido cuando la `eventCategory` es `Management`, `Data` o `ConfigurationItem`.

En los siguientes ejemplos, se muestra cómo crear diferentes tipos de almacenes de datos de eventos.

Temas

- Crear un almacén de datos de eventos para eventos de datos de S3 con la AWS CLI
- Crear un almacén de datos de eventos para los elementos de configuración deAWS Config con la AWS CLI
- Crear un almacén de datos de eventos para eventos de administración con la AWS CLI
- Crear almacenes de datos de eventos para los eventos de Insights con la AWS CLI

Crear un almacén de datos de eventos para eventos de datos de S3 con la AWS CLI

El siguiente comando de ejemplo create-event-data-store de la AWS Command Line Interface (AWS CLI) crea un almacén de datos de eventos denominado `my-event-data-store` que selecciona todos los eventos de datos de Amazon S3 y se cifra mediante una clave de KMS.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
    ]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
```

```
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

Crear un almacén de datos de eventos para los elementos de configuración deAWS Config con la AWS CLI

El siguiente comando de ejemplo de la AWS CLI create-event-data-store crea un almacén de datos de eventos denominado `config-items-eds` que selecciona elementos de configuración de AWS Config. Para recopilar los elementos de configuración, especifique que el campo `eventCategory` iguala a `ConfigurationItem` en los selectores de eventos avanzados.

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

Crear un almacén de datos de eventos para eventos de administración con la AWS CLI

El siguiente comando de ejemplo create-event-data-store de la AWS CLI crea un almacén de datos de eventos de la organización que recopila todos los eventos de administración y establece el parámetro `--billing-mode` en `FIXED_RETENTION_PRICING`.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
```

```
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

Crear almacenes de datos de eventos para los eventos de Insights con la AWS CLI

Para registrar los eventos de Insights en CloudTrail Lake, necesita un almacén de datos de eventos de destino que recopile los eventos de Insights y un almacén de datos de eventos de origen que habilite Insights y registre los eventos de administración.

Este procedimiento le muestra cómo crear los almacenes de datos de eventos de origen y destino y, a continuación, habilitar los eventos de Insights.

1. Ejecute el comando aws cloudtrail create-event-data-store para crear un almacén de datos de eventos de destino que recopile los eventos de Insights. El valor para `eventCategory` debe ser `Insight`. Sustituya los *`retention-period-days`* con la cantidad de días que desea retener los eventos en su almacén de datos de eventos. Los valores válidos son enteros entre 7 y 3653 si el `--billing-mode` es `EXTENDABLE_RETENTION_PRICING`, o entre 7 y 2557 si el `--billing-mode` está establecido en `FIXED_RETENTION_PRICING`. Si no especifica el `--retention-period`, CloudTrail utiliza el periodo de retención predeterminado para el `--billing-mode`.

Si ha iniciado sesión con la cuenta de administración de una organización de AWS Organizations, incluya el parámetro `--organization-enabled` si desea dar acceso al administrador delegado al almacén de datos de eventos.

```
aws cloudtrail create-event-data-store \
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
```

```
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

Utilizará el ARN (o el sufijo ID del ARN) de la respuesta como valor del parámetro `--insights-destination` en el paso 3.

2. Ejecute el comando aws cloudtrail create-event-data-store para crear un almacén de datos de eventos de origen que registre los eventos de administración. De forma predeterminada, los almacenes de datos de eventos registran eventos de administración. No es necesario que especifique ningún selector de eventos avanzado si desea registrar todos los eventos de administración. Sustituya los *retention-period-days* con la cantidad de días que desea retener los eventos en su almacén de datos de eventos. Los valores válidos son enteros entre 7 y 3653 si el `--billing-mode` es `EXTENDABLE_RETENTION_PRICING`, o entre 7 y 2557 si el `--billing-mode` está establecido en `FIXED_RETENTION_PRICING`. Si no especifica el `--retention-period`, CloudTrail utiliza el periodo de retención predeterminado para el `--billing-mode`. Si va a crear un almacén de datos de eventos de la organización, incluya el parámetro `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
```

```
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

Utilizará el ARN (o el sufijo ID del ARN) de la respuesta como valor del parámetro `--event-data-store` en el paso 3.

3. Ejecute el comando put-insight-selectors para habilitar los eventos de Insights. Los valores del selector de insights pueden ser `ApiCallRateInsight`, `ApiErrorRateInsight` o ambos. Para el parámetro `--event-data-store`, especifique el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos de origen que registra los eventos de administración y habilitará Insights. Para el parámetro `--insights-destination`, especifique el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos de destino que registrará los eventos de Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

En el siguiente resultado, se muestra el selector de eventos de Insights configurado para el almacén de datos de eventos.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
```

```
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Después de que habilite CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en entregar el primer evento de Insights, si se detecta una actividad inusual.

CloudTrail Insights analiza los eventos de administración que se producen en una sola región, no de forma global. Los eventos de CloudTrail Insights se generan en la misma región en la que se generan sus eventos de administración correspondientes.

En el caso de un almacén de datos de eventos de una organización, CloudTrail analiza los eventos de administración de la cuenta de cada miembro en lugar de analizar la agregación de todos los eventos de administración de la organización.

Se aplican cargos adicionales por incorporar eventos de Insights en CloudTrail Lake. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para obtener información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Importar eventos de registros de seguimiento a un almacén de datos de eventos con la AWS CLI

En la AWS CLI, puede importar eventos de registros de seguimiento a un almacén de datos de eventos. El procedimiento de esta sección muestra cómo crear y configurar un almacén de datos de eventos mediante la ejecución del comando create-event-data-store y, a continuación, importando los eventos a ese almacén de datos de eventos mediante el comando start-import. Para obtener más información sobre la importación de eventos de registros de seguimiento, incluida información sobre las consideraciones y los permisos necesarios, consulte Copiar eventos de registro de seguimiento en un almacén de datos de eventos.

Prepararse para importar eventos de registros de seguimiento

Antes de importar los eventos de registro de seguimiento, realice los siguientes preparativos.

- Asegúrese de tener un rol con los permisos necesarios para importar eventos de registros de seguimiento a un almacén de datos de eventos.

- Determine el valor de --billing-mode que desea especificar para el almacén de datos de eventos. El `--billing-mode` determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos.

  Al importar eventos de registros de seguimiento a CloudTrail Lake, CloudTrail descomprime los registros que están almacenados en formato gzip (comprimido). A continuación, CloudTrail copia los eventos contenidos en los registros al almacén de datos de eventos. El tamaño de los datos sin comprimir podría ser mayor que el tamaño real del almacenamiento de Amazon S3. Para obtener una estimación general del tamaño de los datos sin comprimir, multiplique por 10 el tamaño de los registros del bucket de S3. Puede usar esta estimación para elegir el valor de `--billing-mode` para su caso de uso.

- Determine el valor que desea especificar para el `--retention-period`. CloudTrail no copiará un evento si su `eventTime` es anterior al periodo de retención especificado.

  Para determinar el periodo de retención adecuado, tome la suma del evento más antiguo que desea copiar en días y el número de días que desea retener los eventos en el almacén de datos de eventos, como se muestra en esta ecuación:

  Periodo de retención = *el evento más antiguo registrado en días* + *el número de días que se debe retener*

  Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.

- Decida si desea utilizar el almacén de datos de eventos para analizar cualquier evento futuro. Si no desea incorporar ningún evento futuro, incluya el parámetro `--no-start-ingestion` al crear el almacén de datos de eventos. De forma predeterminada, el almacén de datos de eventos comienza a incorporar eventos cuando se crea.

Crear un almacén de datos de eventos e importar eventos de registros de seguimiento al almacén de datos de eventos

1. Ejecute el comando create-event-data-store para crear el nuevo almacén de datos de eventos. En este ejemplo, el `--retention-period` se establece en `120` porque el evento más antiguo que se está copiando tiene 90 días y queremos retener los eventos durante 30 días. El parámetro `--no-start-ingestion` está establecido porque no queremos incorporar ningún evento futuro. En este ejemplo, `--billing-mode` no se estableció porque estamos usando

el valor predeterminado `EXTENDABLE_RETENTION_PRICING` ya que esperamos incorporar menos de 25 TB de datos de eventos.

> **Note**
>
> Si va a crear el almacén de datos de eventos para reemplazar su registro de seguimiento, le recomendamos que configure los `--advanced-event-selectors` de forma que coincidan con los selectores de eventos de su registro de seguimiento para asegurarse de tener la misma cobertura de eventos. De forma predeterminada, los almacenes de datos de eventos registran eventos de administración.

```
aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
 120 --no-start-ingestion
```

Lo que sigue es un ejemplo de respuesta:

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
```

```
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

El primer `Status` es `CREATED` para que ejecutemos el comando get-event-data-store para comprobar que se ha detenido la incorporación.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

La respuesta muestra que el `Status` es ahora `STOPPED_INGESTION`, lo que indica que el almacén de datos de eventos no está incorporando eventos en vivo.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. Ejecute el comando start-import para importar los eventos de registro de seguimiento al almacén de datos de eventos creado en el paso 1. Especifique el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos como valor del parámetro `--destinations`. Para `--start-`

`event-time`, especifique el `eventTime` para el evento más antiguo que desee copiar y, para `--end-event-time`, especifique el `eventTime` del evento más reciente que desee copiar. Para `--import-source`, especifique el URI de S3 para el bucket de S3 que contiene los registros de seguimiento, la Región de AWS del bucket de S3 y el ARN del rol utilizado para importar los eventos de seguimiento.

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

A continuación, se muestra un ejemplo de respuesta.

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
   "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
   "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. Ejecute el comando get-import para obtener información acerca de la importación.

```
aws cloudtrail get-import --import-id import-id
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

Una importación finaliza con un `ImportStatus` `COMPLETED` si no hubo errores o `FAILED` si los hubo.

Si la importación tuvo `FailedEntries`, puede ejecutar el comandolist-import-failures para obtener una lista de errores.

```
aws cloudtrail list-import-failures --import-id import-id
```

Para volver a intentar una importación que tuvo errores, ejecute el comando start-import solo con el parámetro `--import-id`. Cuando vuelva a intentar la importación, CloudTrail reanuda la importación en la ubicación en la que se produjo el error.

```
aws cloudtrail start-import --import-id import-id
```

Crear una integración para registrar eventos externos a AWS con la AWS CLI

En la AWS CLI, se crea una integración que registra los eventos externos a AWS en cuatro comandos (tres si ya dispone de un almacén de datos de eventos que cumple con los criterios). Los almacenes de datos de eventos que utilice como destinos de una integración deben ser para una sola región y una sola cuenta; no pueden ser multirregionales, no pueden registrar eventos para organizaciones en AWS Organizations y solo pueden incluir eventos de actividad. El tipo de evento en la consola debe ser Events from integrations (Eventos de integraciones). En la API, el valor `eventCategory` debe ser `ActivityAuditLog`. Para obtener más información acerca de las integraciones, consulte Creación de una integración con un origen de eventos externo a AWS.

1. Ejecute create-event-data-store para crear un almacén de datos de eventos si aún no tiene uno o varios almacenes de datos de eventos que pueda utilizar para la integración.

   El siguiente comando de la AWS CLI de ejemplo crea un almacén de datos de eventos que registra eventos externos a AWS. Para los eventos de actividad, el valor del selector de campo `eventCategory` es `ActivityAuditLog`. El almacén de datos de eventos tiene establecido un periodo de retención de 90 días. El almacén de datos de eventos recopila eventos de todas las regiones de forma predeterminada, pero como recopila eventos que no son de AWS, configúrelo para una sola región mediante la opción `--no-multi-region-enabled`. La protección contra la terminación está habilitada de forma predeterminada y el almacén de datos de eventos no recopila eventos para cuentas de una organización.

   ```
   aws cloudtrail create-event-data-store \
   --name my-event-data-store \
   --no-multi-region-enabled \
   --retention-period 90\
   --advanced-event-selectors '[
       {
         "Name": "Select all external events",
   ```

```
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Necesitará el ID del almacén de datos de eventos (el sufijo del ARN o `EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE` en el ejemplo de respuesta anterior) para continuar con el siguiente paso y crear el canal.

2. Ejecute el comando create-channel para crear un canal que permita a una aplicación asociada o de origen enviar eventos a un almacén de datos de eventos en CloudTrail.

   Un canal tiene los siguientes componentes:

Origen

CloudTrail utiliza esta información para determinar los socios que envían datos de eventos a CloudTrail en su nombre. Se requiere un origen, que puede ser `Custom` para todos los eventos válidos que no son de AWS, o el nombre de un origen de eventos asociado. Se permite un máximo de un canal por origen.

Para obtener más información sobre los valores `Source` para socios disponibles, consulte Información adicional acerca de los socios de integración.

Estado de la ingesta

El estado del canal muestra cuándo se recibieron los últimos eventos de un origen de canal.

Destinos

Los destinos son los almacenes de datos de eventos de CloudTrail Lake que reciben los eventos del canal. Puede cambiar los almacenes de datos de eventos de destino de un canal.

Para dejar de recibir eventos de un origen, elimine el canal.

Necesita el ID de al menos un almacén de datos de eventos de destino para ejecutar este comando. El tipo de destino válido es `EVENT_DATA_STORE`. Puede enviar los eventos ingeridos a más de un almacén de datos de eventos. El siguiente comando de ejemplo crea un canal que envía eventos a dos almacenes de datos de eventos, representados por sus ID en el atributo `Location` del parámetro `--destinations`. Los parámetros `--destinations`, `--name` y `--source` son obligatorios. Para ingerir los eventos de un socio de CloudTrail, especifique el nombre del socio como el valor de `--source`. Para ingerir los eventos de sus aplicaciones externas a AWS, especifique `Custom` como el valor de `--source`.

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

En la respuesta al comando create-channel, copie el ARN del canal nuevo. Necesitará el ARN para ejecutar los comandos `put-resource-policy` y `put-audit-events` en los siguientes pasos.

3. Ejecute el comando put-resource-policy para asociar una política de recursos al canal. Las políticas de recursos son documentos de política JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso y bajo qué condiciones. Las cuentas definidas como entidades principales en la política de recursos del canal pueden llamar a la API `PutAuditEvents` para enviar eventos.

   > **Note**
   >
   > Si no se crea una política de recursos para el canal, solo el propietario del canal puede llamar a la API `PutAuditEvents` del canal.

   La información necesaria para la política está determinada por el tipo de integración.

   - Para una integración directa, CloudTrail exige que la política contenga los ID de la cuenta de AWS del socio y requiere que ingrese el ID externo único proporcionado por el socio. CloudTrail agrega de forma automática los ID de la cuenta de AWS del socio a la política de recursos cuando se crea una integración mediante la consola de CloudTrail. Consulte la documentación de socios para obtener información sobre cómo obtener los números de cuenta de AWS necesarios para la política.
   - Para la integración de una solución, debe especificar al menos un ID de cuenta de AWS como entidad principal y, si lo desea, puede ingresar un ID externo para evitar un suplente confuso.

   A continuación, se enumeran los requisitos de la política de recursos:

   - El ARN del recurso definido en la política debe coincidir con el ARN del canal al que está asociada la política.
   - La política contiene solo una acción: cloudtrail-data:PutAuditEvents.
   - La política contiene como mínimo una instrucción. La política puede tener como máximo 20 instrucciones.
   - Cada instrucción contiene como mínimo una entidad principal. Una instrucción puede tener como máximo 50 entidades principales.

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

Para obtener más información sobre las políticas de recursos, consulte Ejemplos de políticas basadas en recursos de AWS CloudTrail.

4. Ejecute la API `PutAuditEvents` para ingerir los eventos de actividad en CloudTrail. Necesitará la carga útil de los eventos que desea que agregue CloudTrail. Asegúrese de que no haya información confidencial o de identificación personal en la carga útil del evento antes de incorporarla en CloudTrail. Tenga en cuenta que la API `PutAuditEvents` utiliza el punto de conexión `cloudtrail-data` de la CLI, no el punto de conexión `cloudtrail`.

Los siguientes ejemplos muestran cómo utilizar el comando put-audit-events de la CLI. Los parámetros --audit-events y --channel-arn son obligatorios. El parámetro --external-id es obligatorio si se define un ID externo en la política de recursos. Necesita el ARN del canal que creó en el paso anterior. El valor de --audit-events es una matriz JSON de objetos de eventos. `--audit-events` incluye un ID obligatorio del evento, la carga útil requerida del evento como el valor de `EventData` y una suma de comprobación opcional para ayudar a validar la integridad del evento una vez ingerido en CloudTrail.

```
aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

A continuación, se muestra un comando de ejemplo con dos ejemplos de eventos.

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

El siguiente comando de ejemplo agrega el parámetro `--cli-input-json` para especificar un archivo JSON (`custom-events.json`) de la carga útil del evento.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

A continuación, se presenta el contenido de muestra del archivo JSON de ejemplo, `custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

Puede comprobar que la integración funciona y que CloudTrail está ingiriendo eventos del origen de forma correcta mediante la ejecución del comando get-channel. El resultado de get-channel muestra la marca de tiempo más reciente en la que CloudTrail recibió eventos.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(Opcional) Cálculo de un valor de la suma de comprobación

La suma de comprobación que se especifica como valor de `EventDataChecksum` en una solicitud `PutAuditEvents` ayuda a verificar que CloudTrail recibe el evento que coincide con la suma de comprobación y ayuda a verificar la integridad de los eventos. El valor de la suma de comprobación es un algoritmo base64-SHA256 que se calcula mediante la ejecución del siguiente comando.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
       \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
       \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
       \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
```

```
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

El comando devuelve la suma de comprobación. A continuación, se muestra un ejemplo.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

El valor de la suma de comprobación se convierte en el valor de `EventDataChecksum` en la solicitud `PutAuditEvents`. Si la suma de comprobación no coincide con la del evento proporcionado, CloudTrail rechaza el evento y se produce un error `InvalidChecksum`.

Obtener un almacén de datos de eventos con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI get-event-data-store devuelve información sobre el almacén de datos de eventos especificado por el parámetro `--event-data-store` requerido, el cual acepta un ARN o el sufijo de ID del ARN.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

A continuación, se muestra un ejemplo de respuesta. Las horas de creación y última actualización están en formato `timestamp`.

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Data"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::bucketName"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

Enumerar todos los almacenes de datos de eventos de una cuenta con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI list-event-data-stores devuelve información sobre todos los almacenes de datos de eventos de una cuenta en la región actual. Los parámetros opcionales incluyen `--max-results` para especificar el número máximo de resultados que desea que el comando devuelva en una sola página. Si hay más resultados que el valor `--max-results` especificado, ejecute el comando de nuevo agregando el valor devuelto `NextToken` para obtener la siguiente página de resultados.

```
aws cloudtrail list-event-data-stores
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
}
```

Actualizar un almacén de datos de eventos con la AWS CLI

En los siguientes ejemplos, se muestra cómo actualizar un almacén de datos de eventos.

Temas

- Actualizar el modo de facturación con la AWS CLI

- Actualice el modo de retención, habilite la protección contra la terminación y especifique una AWS KMS key con la AWS CLI
- Deshabilitar la protección contra la terminación con la AWS CLI

Actualizar el modo de facturación con la AWS CLI

El `--billing-mode` para el almacén de datos de eventos determina el costo de la incorporación y el almacenamiento de eventos, así como el periodo de retención máximo y predeterminado del almacén de datos de eventos. Si el `--billing-mode` del almacén de datos de eventos está establecido en `FIXED_RETENTION_PRICING`, puede cambiar el valor a `EXTENDABLE_RETENTION_PRICING`, pero por lo general se recomienda `EXTENDABLE_RETENTION_PRICING` si el almacén de datos de eventos incorpora menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 3653 días. Para obtener información sobre precios, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

> **Note**
>
> No puede cambiar el valor `--billing-mode` de `EXTENDABLE_RETENTION_PRICING` a `FIXED_RETENTION_PRICING`. Si el modo de facturación del almacén de datos de eventos está configurado en `EXTENDABLE_RETENTION_PRICING` y quiere utilizar `FIXED_RETENTION_PRICING` en su lugar, puede detener la incorporación en el almacén de datos de eventos y crear un nuevo almacén de datos de eventos que utilice `FIXED_RETENTION_PRICING`.

El siguiente comando de ejemplo update-event-data-store de la AWS CLI cambia el `--billing-mode` del almacén de datos de eventos de `FIXED_RETENTION_PRICING` a `EXTENDABLE_RETENTION_PRICING`. El valor del parámetro `--event-data-store` requerido es un ARN (o el sufijo ID del ARN) y es obligatorio; los demás parámetros son opcionales.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Actualice el modo de retención, habilite la protección contra la terminación y especifique una AWS KMS key con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI update-event-data-store actualiza un almacén de datos de eventos para cambiar su periodo de retención a 100 días y habilitar la protección contra la terminación. El valor del parámetro `--event-data-store` requerido es un ARN (o el sufijo ID del ARN) y es obligatorio; los demás parámetros son opcionales. En este ejemplo, se agrega el parámetro `--retention-period` para cambiar el periodo de retención a 100 días. Si lo desea, puede optar por habilitar el cifrado de AWS Key Management Service y especificar una AWS KMS key agregando el `--kms-key-id` al comando y especificando el ARN de una clave de KMS como valor. `--termination-protection-enabled` se agrega para habilitar la protección contra la terminación en un almacén de datos de eventos que no tenía habilitada dicha protección.

Un almacén de datos de eventos que registra eventos externos a AWS no se puede actualizar para que registre eventos de AWS. Del mismo modo, un almacén de datos de eventos que registra eventos de AWS no se puede actualizar para que registre eventos externos a AWS.

> **Note**
>
> Si reduce el periodo de retención de un almacén de datos de eventos, CloudTrail eliminará todos los eventos que tengan un periodo de retención de `eventTime` anterior al nuevo. Por ejemplo, si el periodo de retención anterior era de 365 días y lo reduce a 100 días, CloudTrail eliminará los eventos con una antigüedad de `eventTime` superior a 100 días.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
```

```
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Deshabilitar la protección contra la terminación con la AWS CLI

De forma predeterminada, la protección contra la terminación está habilitada en un almacén de datos de eventos para proteger el almacén de datos de eventos de una eliminación accidental. No puede eliminar un almacén de datos de eventos cuando la protección contra la terminación está habilitada. Si desea eliminar el almacén de datos de eventos, primero debe deshabilitar la protección contra la terminación.

El siguiente comando de ejemplo update-event-data-store de la AWS CLI deshabilita la protección contra la terminación pasando el parámetro `--no-termination-protection-enabled`.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
```

```
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Detener la incorporación en un almacén de datos de eventos con la AWS CLI

El siguiente comando de ejemplo de la AWS CLI stop-event-data-store-ingestion impide que un almacén de datos de eventos ingiera eventos. Para detener la ingesta, el `Status` del almacén de datos de eventos debe ser `ENABLED`, mientras que el valor de `eventCategory` debe ser `Management`, `Data` o `ConfigurationItem`. `--event-data-store` o el sufijo de ID del ARN especifican el almacén de datos de eventos, que acepta un ARN de almacén de datos de eventos. Después de ejecutar stop-event-data-store-ingestion, el estado del almacén de datos del evento cambia a `STOPPED_INGESTION`.

El almacén de datos de eventos se cuenta dentro del máximo de diez almacenes de datos de eventos de su cuenta cuando su estado es `STOPPED_INGESTION`.

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Si la operación se realiza correctamente, no se produce ninguna respuesta.

Iniciar la incorporación en un almacén de datos de eventos con la AWS CLI

El siguiente comando de ejemplo de la AWS CLI start-event-data-store-ingestion inicia la ingesta de eventos en un almacén de datos de eventos. Para iniciar la ingesta, el `Status` del almacén de datos de eventos debe ser `STOPPED_INGESTION`, mientras que el valor de `eventCategory` debe ser `Management`, `Data` o `ConfigurationItem`. `--event-data-store` o el sufijo de ID del ARN especifican el almacén de datos de eventos, que acepta un ARN de almacén de datos de eventos. Después de ejecutar start-event-data-store-ingestion, el estado del almacén de datos del evento cambia a `ENABLED`.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

Si la operación se realiza correctamente, no se produce ninguna respuesta.

Habilitar la federación en un almacén de datos de eventos

Para habilitar la federación, ejecute el comando aws cloudtrail enable-federation proporcionando los parámetros `--event-data-store` y `--role` necesarios. En `--event-data-store`, proporcione el ARN del almacén de datos de eventos (o el sufijo de ID del ARN). En `--role`, proporcione el ARN de su rol de federación. El rol debe existir en su cuenta y proporcionar los permisos mínimos necesarios.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

En este ejemplo, se muestra cómo un administrador delegado puede habilitar la federación en un almacén de datos de eventos de la organización especificando el ARN del almacén de datos de eventos en la cuenta de administración y el ARN del rol de federación en la cuenta de administrador delegado.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-
id
```

```
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Deshabilitar la federación en un almacén de datos de eventos

Para deshabilitar la federación en el almacén de datos de eventos, ejecute el comando aws cloudtrail disable-federation. El almacén de datos de eventos especificado por `--event-data-store`, que acepta un ARN de almacén de datos de eventos, o el sufijo de ID del ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Si se trata de un almacén de datos de eventos de la organización, utilice el ID de la cuenta que corresponde a la cuenta de administración.

Eliminar un almacén de datos de eventos con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI delete-event-data-store desactiva el almacén de datos de eventos especificado por `--event-data-store`, que acepta el ARN de un almacén de datos de eventos, o el sufijo de ID del ARN. Después de ejecutar delete-event-data-store, el estado final del almacén de datos de eventos será `PENDING_DELETION` y se eliminará automáticamente después de un periodo de espera de 7 días.

Después de ejecutar delete-event-data-store en un almacén de datos de eventos, no se puede ejecutar list-queries, describe-query o get-query-results en las consultas que están utilizando el almacén de datos desactivado. El almacén de datos de eventos se cuenta dentro del máximo de diez almacenes de datos de eventos de su cuenta cuando está pendiente de eliminación.

> **Note**
>
> No puede eliminar un almacén de datos de eventos si `--termination-protection-enabled` está configurado o si `FederationStatus` está `ENABLED`.

```
aws cloudtrail delete-event-data-store
```

```
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Si la operación se realiza correctamente, no se produce ninguna respuesta.

Restaurar un almacén de datos de eventos con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI restore-event-data-store restaura un almacén de datos de eventos que está pendiente de eliminación. El almacén de datos de eventos especificado por `--event-data-store`, que acepta un ARN de almacén de datos de eventos, o el sufijo de ID del ARN. Únicamente se puede restaurar un almacén de datos de eventos eliminado dentro del periodo de espera de siete días posterior a la eliminación.

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

La respuesta incluye información sobre el almacén de datos de eventos, incluido su ARN, los selectores de eventos avanzados y el estado de la restauración.

Enumerar todos los canales con la AWS CLI

Para enumerar todos los canales de su cuenta, ejecute el comando list-channels. A continuación, se muestra un ejemplo.

```
aws cloudtrail list-channels
```

Actualizar un canal con la AWS CLI

Para actualizar el nombre de un canal o los almacenes de datos de eventos de destino, ejecute el comando update-channel. El parámetro `--channel` es obligatorio. No se puede actualizar el origen de un canal. A continuación, se muestra un ejemplo.

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

Eliminar un canal para eliminar una integración con la AWS CLI

Para detener la ingesta de eventos de socios u otros eventos de actividad externos a AWS, elimine el canal mediante el comando delete-channel. Se requiere el ARN o el ID (el sufijo ARN) del canal que desea eliminar. A continuación, se muestra un ejemplo.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

Iniciar una consulta con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI start-query ejecuta una consulta en el almacén de datos de eventos especificado como ID en la instrucción de consulta y entrega los resultados de la consulta a un bucket de S3 especificado. El parámetro `--query-statement` proporciona una consulta SQL, encerrada entre comillas simples. Los parámetros opcionales incluyen `--delivery-s3uri` para enviar los resultados de la consulta a un bucket de S3 especificado. Para obtener más información sobre el lenguaje de consulta que se puede utilizar en CloudTrail Lake, consulte CloudTrail Restricciones de Lake SQL.

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

La respuesta es una cadena `QueryId`. Para obtener el estado de una consulta, ejecute describe-query utilizando el valor `QueryId` devuelto por start-query. Si la consulta se realiza correctamente, se puede ejecutar get-query-results para obtener resultados.

Salida

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Es posible que las consultas que se ejecuten durante más de una hora agoten el tiempo de espera. Aun así, puede que obtenga resultados parciales que se hayan procesado antes de que se agotara el tiempo de espera de la consulta.

Si va a entregar los resultados de la consulta a un bucket de S3 mediante el parámetro opcional `--delivery-s3uri`, la política del bucket debe conceder permiso a CloudTrail para entregar los resultados de la consulta al bucket. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake.

Obtener metadatos sobre una consulta con la AWS CLI

El siguiente comando describe-query de ejemplo de la AWS CLI obtiene metadatos sobre una consulta, como el tiempo de ejecución de la consulta en milisegundos, el número de eventos analizados y coincidentes, el número total de bytes analizados y el estado de la consulta. El valor de `BytesScanned` coincide con el número de bytes que se facturan a la cuenta por la consulta, a menos que la consulta aún siga en ejecución. Si los resultados de la consulta se enviaron a un bucket de S3, la respuesta también proporciona el URI de S3 y el estado de la entrega.

Puede especificar un valor para `--query-id` o el parámetro `--query-alias`. Al especificar el parámetro `--query-alias`, se devuelve información sobre la última consulta ejecutada para el alias.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

Obtener los resultados de consultas con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI get-query-results obtiene los resultados de los datos de eventos de una consulta. Debe especificar el valor de `--query-id` que devuelve el comando start-query. El valor de `BytesScanned` coincide con el número de bytes que se facturan a la cuenta por la consulta, a menos que la consulta aún siga en ejecución. Los parámetros opcionales incluyen `--max-query-results` para especificar el número máximo de resultados que desea que el comando devuelva en una sola página. Si hay más resultados que el valor `--max-query-results` especificado, ejecute el comando de nuevo agregando el valor devuelto `NextToken` para obtener la siguiente página de resultados.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Salida

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

Enumerar todas las consultas en un almacén de datos de eventos con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI list-queries devuelve una enumeración de las consultas y los estados de consulta en un almacén de datos de eventos especificado para los últimos

siete días. Debe especificar un ARN o el sufijo ID de un valor ARN para `--event-data-store`. De manera opcional, para reducir la lista de resultados, puede especificar un rango de tiempo, formateado como marcas temporales, agregando `--start-time`, los parámetros `--end-time` y un valor `--query-status`. Los valores válidos para `QueryStatus` incluyen: `QUEUED`, `RUNNING`, `FINISHED`, `FAILED`, o `CANCELLED`.

list-queries también tiene parámetros opcionales de paginación. Utilice `--max-results`, para especificar el número máximo de resultados que desea que el comando devuelva en una sola página. Si hay más resultados que el valor `--max-results` especificado, ejecute el comando de nuevo agregando el valor devuelto `NextToken` para obtener la siguiente página de resultados.

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

Salida

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
    "NextToken": "20add42078135EXAMPLE"
}
```

Cancelar una consulta en curso con la AWS CLI

El siguiente ejemplo del comando de la AWS CLI cancel-query cancela una consulta que tiene el estado `RUNNING`. Debe especificar un valor para `--query-id`. Al ejecutar cancel-query, el estado

de la consulta se puede mostrar como CANCELLED aunque la operación cancel-query no haya finalizado.

> **Note**
>
> Una consulta cancelada puede generar gastos. Se cargará en su cuenta la cantidad de datos que se analizaron antes de que cancelara la consulta.

A continuación se muestra un ejemplo de la CLI.

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Salida

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail Restricciones de Lake SQL

CloudTrail Las consultas de Lake son cadenas SQL. En esta sección, se proporciona información sobre las funciones, los operadores y los esquemas compatibles.

Únicamente son compatibles sentencias SELECT. Ninguna cadena de consulta puede modificar o mutar los datos.

CloudTrail Lake admite todas las SELECT instrucciones, funciones y operadores válidos de Presto SQL. Para obtener más información acerca de los operadores y funciones SQL compatibles, consulte Funciones y operadores en el sitio web de documentación de Presto.

La CloudTrail consola proporciona varios ejemplos de consultas que pueden ayudarle a empezar a escribir sus propias consultas. Para obtener más información, consulte Visualización de consultas de ejemplo en la consola de CloudTrail.

Temas

- Funciones, condiciones y operadores join compatibles

- Soporte avanzado de consultas en varias tablas

Funciones, condiciones y operadores join compatibles

Funciones compatibles

CloudTrail Lake es compatible con todas las funciones de Presto. Para obtener más información acerca de otras funciones compatibles, consulte Funciones y operadores en el sitio web de documentación de Presto.

CloudTrail Lake no admite la `INTERVAL` palabra clave.

Operadores de condición compatibles

Se admiten los siguientes operadores de condición.

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

Operadores join compatibles

Se admiten los siguientes operadores `JOIN`. Para obtener más información acerca de la ejecución de consultas en varias tablas, consulte Soporte avanzado de consultas en varias tablas.

```
UNION
UNION ALL
```

```
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

Soporte avanzado de consultas en varias tablas

CloudTrail Lake admite un lenguaje de consulta avanzado en varios almacenes de datos de eventos.

- `UNION|UNION ALL|EXCEPT|INTERSECT`
- `LEFT|RIGHT|INNER JOIN`

Para ejecutar la consulta, utilice el comando start-query de la AWS CLI. A continuación, se presenta un ejemplo en el que se utiliza una de las consultas de muestra de esta sección.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

La respuesta es una cadena `QueryId`. Para obtener el estado de una consulta, ejecute `describe-query` utilizando el valor `QueryId` devuelto por `start-query`. Si la consulta se realiza correctamente, se puede ejecutar `get-query-results` para obtener resultados.

`UNION|UNION ALL|EXCEPT|INTERSECT`

El siguiente es un ejemplo de consulta que utiliza `UNION` y `UNION ALL` para buscar eventos por su ID y nombre de evento en tres almacenes de datos de eventos: EDS1, EDS2 y EDS3. Los resultados se seleccionan primero de cada almacén de datos de eventos y, a continuación, se concatenan, se ordenan por ID de evento y se limitan a diez eventos.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

LEFT|RIGHT|INNER JOIN

El siguiente es un ejemplo de consulta que utiliza `LEFT JOIN` para buscar todos los eventos de un almacén de datos de eventos denominado `eds2`, asignados a `edsB` y que coincidan con los de un almacén de datos de eventos principal (izquierda), `edsA`. Los eventos devueltos se producen el 1 de enero de 2020 o antes, y solo se devuelven los nombres de los eventos.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

Esquemas SQL compatibles con los almacenes de datos de eventos

En las siguientes secciones, se proporciona el esquema SQL compatible con cada tipo de almacén de datos de eventos.

Temas

- Esquema compatible para los campos de registro de eventos de CloudTrail
- Esquema compatible para los campos de registro de eventos de CloudTrail Insights
- Esquema compatible para los campos de registro de elementos de configuración de AWS Config
- Esquema compatible para los campos de registro de evidencia de AWS Audit Manager
- Esquema compatible para campos de eventos que no son de AWS

Esquema compatible para los campos de registro de eventos de CloudTrail

A continuación, se muestra el esquema SQL válido para los campos de registro de eventos de datos y administración de CloudTrail. Para obtener más información acerca de los campos de los registros de eventos de CloudTrail, consulte CloudTrail contenido del registro.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
```

```
    },
    {
        "Name": "useridentity",
        "Type":
"struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
                ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
    {
        "Name": "eventname",
        "Type": "string"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
        "Type": "string"
    },
    {
        "Name": "errorcode",
        "Type": "string"
    },
    {
```

```
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
"array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
```

```
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
```

```
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsonchecksum",
        "Type": "string"
    }
]
```

Esquema compatible para los campos de registro de eventos de CloudTrail Insights

A continuación, se muestra el esquema SQL válido para los campos de registro de eventos de Insights. Para los eventos de Insights, el valor de `eventcategory` es `Insight`, y el valor de `eventtype` es `AwsCloudTrailInsight`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
```

```
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type":
"struct<baselineaverage:double,insightaverage:double,baselineduration:integer,

insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
                insightaverage:double,baselinevalue:string,baselineaverage:double>>"
    }
```

```
]
```

Esquema compatible para los campos de registro de elementos de configuración de AWS Config

A continuación, se muestra el esquema SQL válido para los campos de registro de elementos de configuración. Para los elementos de configuración, el valor de `eventcategory` es `ConfigurationItem` y el valor de `eventtype` es `AwsConfigurationItem`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
```

```
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

Esquema compatible para los campos de registro de evidencia de AWS Audit Manager

A continuación, se muestra el esquema SQL válido para los campos de registro de evidencia de Audit Manager. Para los campos de registro de evidencia de Audit Manager, el valor de `eventcategory` es `Evidence` y el valor de `eventtype` es `AwsAuditManagerEvidence`. Para obtener más información acerca de cómo agregar evidencia en CloudTrail Lake con Audit Manager, consulte Evidence finder (Buscador de evidencia) en la Guía del usuario de AWS Audit Manager.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
```

```
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

Esquema compatible para campos de eventos que no son de AWS

A continuación, se muestra el esquema SQL válido para eventos que no son de AWS. Para los eventos que no son de AWS, el valor de `eventcategory` es `ActivityAuditLog` y el valor de `eventtype` es `ActivityLog`.

```
[
    {
        "Name": "eventversion",
```

```
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
"struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
```

```
    }
]
```

Control de los permisos de usuario para CloudTrail Lake

AWS CloudTrail se integra con AWS Identity and Access Management (IAM) para ayudarle a controlar el acceso a CloudTrail Lake y otros recursos de AWS que requiere CloudTrail. Puede usar IAM para controlar qué usuarios de AWS pueden crear, configurar o eliminar canales o almacenes de datos de eventos de CloudTrail, iniciar y detener la ingesta de eventos, y copiar eventos de registros de seguimiento. Para obtener más información, consulte Administración de identidades y accesos para AWS CloudTrail.

Los siguientes temas le ayudan a comprender los permisos, las políticas y la seguridad de CloudTrail:

- Otorgar permisos de CloudTrail administración
- Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake
- Permisos necesarios para copiar eventos de registro de seguimiento
- Permisos necesarios para habilitar la federación
- Un ejemplo de política que restringe el acceso a un almacén de datos de eventos en función de etiquetas: Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas
- Ejemplos de políticas basadas en recursos de AWS CloudTrail
- Permisos necesarios para designar un administrador delegado
- Política de clave de KMS predeterminada para almacenes de datos de eventos de CloudTrail Lake

Gestión de los costos CloudTrail del lago

AWS CloudTrail Los almacenes de datos y las consultas sobre eventos en Lake conllevan cargos. Como práctica recomendada, recomendamos utilizar Servicios de AWS herramientas que puedan ayudarle a gestionar CloudTrail los costes. También puede configurar los almacenes de datos de eventos que capturen los datos que necesita y, al mismo tiempo, le siga resultando rentable. Para obtener más información acerca de los precios de CloudTrail , consulte Precios de AWS CloudTrail.

Temas

- Opciones de precios del almacén de datos de eventos

- Entendiendo los cargos de CloudTrail Lake
- Recomendaciones sobre cómo reducir los costos
- Herramientas para ayudar a administrar los costos
- Véase también

Opciones de precios del almacén de datos de eventos

Cuando crea un almacén de datos de eventos, elige la opción de precio que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como los periodos de retención predeterminado y máximo del almacén de datos de eventos.

En la tabla siguiente, se describen las opciones de precios disponibles. En la tabla, se muestra la opción de precios en la consola y el valor `BillingMode` correspondiente de la API, y muestra el periodo de retención máximo y predeterminado de cada opción.

Opción de precios (consola)	BillingMode (API)	Descripción
Precios de retención ampliables por un año	`EXTENDABLE_RETENTION_PRICING`	Se recomienda si prevé incorporar menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años. Esta opción también se recomienda si el almacén de datos de eventos recopila elementos de configuración de AWS Config , pruebas de Audit Manager y eventos externos a AWS. Durante los primeros 366 días (el periodo de retención predeterminado), el almacenamiento se incluye sin costo adicional a los precios de incorporación. Después de 366 días, la retención prolongada está disponible a un pay-as-you-go precio determinado.

Opción de precios (consola)	BillingMode (API)	Descripción
		Esta es la opción predeterminada. Periodo de retención predeterminado: 366 días. Periodo máximo de retención: 3653 días.
Precios de retención de siete años	`FIXED_RETENTION_PRICING`	Se recomienda si se prevé incorporar más de 25 TB de datos de eventos al mes y se necesita un periodo de retención de hasta 7 años. La retención está incluida en los precios de incorporación sin costo adicional. Periodo de retención predeterminado: 2557 días. Periodo máximo de retención: 2557 días.

Entendiendo los cargos de CloudTrail Lake

En las siguientes tablas se proporciona información sobre cómo se CloudTrail cobran las consultas y los almacenes de datos de eventos de Lake. Para obtener más información acerca de los precios de CloudTrail , consulte Precios de AWS CloudTrail.

Tipo de cargo	Cómo se incurre en los cargos
Ingesta de datos (datos sin comprimir)	En el CloudTrail caso de Lake, usted paga en función de los datos no comprimidos ingeridos. La opción de precios del almacén de datos de eventos determina el costo de la incorporación de eventos:

Tipo de cargo	Cómo se incurre en los cargos
	• Precios de retención ampliables por un año: ofrecen precios de incorporación en función del tipo de evento. • Precios de retención de siete años: ofrece precios de incorporación basados en el volumen de datos incorporados. Los mayores ahorros se obtienen cuando el volumen de datos incorporados mensualmente supera los 25 TB. Copiar eventos de registro de seguimiento Al copiar los eventos de las rutas en CloudTrail Lake, CloudTrail descomprime los registros que están almacenados en formato gzip (comprimido). A continuación, CloudTrail copia los eventos contenidos en los registros en el almacén de datos de eventos. El tamaño de los datos sin comprimir podría ser mayor que el tamaño real del almacenamiento de Amazon S3. Para obtener una estimación general del tamaño de los datos sin comprimir, multiplique por 10 el tamaño de los registros del bucket de S3. **Note** CloudTrail no copiará un evento si la hora del evento es anterior al período de retención especificado. Para determinar el periodo de retención adecuado, tome la suma del evento más antiguo que desea copiar en días y el número de días que desea retener los eventos en el almacén de datos de eventos, como se muestra en esta ecuación: Periodo de retención = *oldest-event-in-days* + *number-days-to-retain* Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.

Tipo de cargo	Cómo se incurre en los cargos
Retención de datos (datos optimizados y comprimidos)	CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos comprimidos. El período de retención de un almacén de datos de eventos determina cuánto tiempo se guardan los datos de eventos en el almacén de datos de eventos. CloudTrail Lake determina si se debe conservar un evento comprobando si la hora del evento se encuentra dentro del período de retención especific ado. Por ejemplo, si especificas un período de retención de 90 días, CloudTrail eliminará los eventos cuando su duración sea superior a 90 días. En el caso de los almacenes de datos de eventos que utilizan la opción Precios de retención de siete años, el almacenamiento está incluido en los precios de incorporación sin costo adicional. En el caso de los almacenes de datos de eventos que utilizan la opción Precios de retención ampliables por un año, el almacenamiento se incluye sin cargo en los precios de incorpora ción durante los primeros 366 días (el periodo de retención predeterminado). Después de 366 días, el almacenamiento se ofrece pay-as-you-pricing y se cobra en función de los datos optimizados y comprimidos del almacén de datos del evento.
Ejecución de consultas en CloudTrail Lake (datos optimizados y comprimidos)	Cuando ejecuta consultas en CloudTrail Lake, paga en función de la cantidad de datos optimizados y comprimidos escaneados.

Recomendaciones sobre cómo reducir los costos

En esta sección se proporcionan recomendaciones sobre cómo reducir los costes al trabajar con CloudTrail Lake.

Elija una opción de precios en función del tipo de eventos que recopilará su almacén de datos de eventos y de su incorporación mensual prevista

Al crear un almacén de datos de eventos, elija una opción de precios en función del tipo de eventos que recopilará su almacén de datos de eventos y de su incorporación mensual prevista.

Si prevé consumir menos de 25 TB de datos de eventos al mes y desea un periodo de retención flexible de hasta 10 años, elija la opción Precios de retención ampliables por un año. Por lo general, también recomendamos esta opción para los almacenes de datos de eventos que recopilan elementos de AWS Config configuración, pruebas de Audit Manager y eventos externos AWS.

Si prevé incorporar más de 25 TB de datos de eventos al mes y necesita un periodo de retención de 7 años, elija la opción Precios de retención de siete años.

Evalúe la incorporación mensual de su almacén de datos de eventos a lo largo del tiempo

Evalúe el historial mensual de incorporación del almacén de datos de su evento para ver si existe una opción de precios que se adapte mejor a sus necesidades.

Si ya tiene un almacén de datos de eventos que utiliza la opción Precios de retención de siete años e incorpora menos de 25 TB de datos al mes, considere la posibilidad de actualizar el almacén de datos de eventos para que utilice un precio de retención ampliable por un año. En el caso de los almacenes de datos de eventos que utilizan la opción de precios de retención de siete años, puede cambiar la opción de precios mediante la CloudTrail consola o la operación de la UpdateEventDataStoreAPI. AWS CLI

Si ya tiene un almacén de datos de eventos que utiliza la opción Precios de retención ampliables por un año e incorpora más de 25 TB de datos de eventos al mes, considere si Precio de retención de siete años se adaptaría mejor a sus necesidades. Para usar la nueva opción de precios, detenga la incorporación en su almacén de datos de eventos y cree uno nuevo con la opción Precios de retención de siete años.

Use selectores de eventos avanzados para filtrar los eventos que no sean de su interés

Al configurar un banco de datos de eventos para la CloudTrail gestión o los eventos de datos, filtra los eventos que no sean de tu interés mediante selectores de eventos avanzados.

Si va a crear un almacén de datos de eventos para recopilar eventos de administración, puede filtrar los eventos de la API de datos de Amazon Relational Database Service AWS Key

Management Service (Amazon RDS AWS KMS) o Amazon Relational Database Service (Amazon RDS). Normalmente, AWS KMS acciones como `EncryptDecrypt`, y `GenerateDataKey` generan más del 99 por ciento de los eventos.

Si va a crear un almacén de datos de eventos para recopilar eventos de datos, puede utilizar selectores de eventos avanzados para filtrar los campos `eventName`, `resources.type`, `resources.ARN` y `readOnly`. Para ver un ejemplo, consulte Tutorial: Creación de un almacén de datos de eventos para eventos de datos de S3.

Elija un periodo más reducido al copiar los eventos de los registros de seguimientos

Al copiar eventos de senderos en CloudTrail Lake, especifique una hora de inicio y una hora de finalización más limitadas para reducir la cantidad de datos ingeridos.

Si está copiando eventos de senderos a CloudTrail Lake para su análisis histórico y no quiere ingerir eventos futuros, desactive la opción de ingerir eventos para no incurrir en cargos por la ingestión de eventos adicionales.

Formatee las consultas para que utilicen un **`eventTime`** de inicio y final

Cuando ejecuta consultas en Lake, paga según la cantidad de datos escaneados. Puede limitar los costos especificando el `eventTime` de inicio y final de la consulta.

Herramientas para ayudar a administrar los costos

AWS Los presupuestos, una función de esta aplicación AWS Billing and Cost Management, te permiten establecer presupuestos personalizados que te avisan cuando tus costes o tu consumo superan (o se prevé que superen) el importe presupuestado.

Al crear almacenes de datos de eventos, la mejor práctica recomendada es crear un presupuesto CloudTrail mediante AWS presupuestos, que puede ayudarte a llevar un registro de tus CloudTrail gastos. Los presupuestos basados en los costes ayudan a dar a conocer cuánto te podrían facturar por el uso que hagas CloudTrail . Las alertas de presupuesto le notifican el momento en que su factura alcanza el límite que ha definido. Cuando reciba una alerta de presupuesto, puede realizar cambios antes de que finalice el ciclo de facturación para administrar los costos.

Después de crear un presupuesto, puedes usarlo AWS Cost Explorer para ver cómo influyen tus CloudTrail costos en tu factura general AWS . En AWS Cost Explorer, después de añadirlo CloudTrail al filtro de servicios, puede comparar sus CloudTrail gastos históricos con los de sus gastos actuales month-to-date (MTD), tanto por región como por cuenta. Esta función le

ayuda a supervisar y detectar los costes inesperados de sus CloudTrail gastos mensuales. Las funciones adicionales de Cost Explorer le permiten comparar los CloudTrail gastos con los gastos mensuales en el nivel de recurso específico, lo que proporciona información sobre lo que podría estar provocando aumentos o disminuciones de los costos en su factura.

Para empezar con AWS los presupuestos, abra y AWS Billing and Cost Management, a continuación, seleccione Presupuestos en la barra de navegación izquierda. Te recomendamos configurar las alertas de presupuesto al crear un presupuesto para hacer un seguimiento de CloudTrail los gastos. Para obtener más información sobre cómo usar AWS los presupuestos, consulte Administrar sus costos con presupuestos y Mejores prácticas para AWS los presupuestos.

Creación de etiquetas de asignación de costes definidas por el usuario para los almacenes de datos de eventos de CloudTrail Lake

Puede crear etiquetas de asignación de costes definidas por el usuario para realizar un seguimiento de los costes de consulta e ingesta de sus almacenes de datos de eventos de CloudTrail Lake. Una etiqueta de asignación de costos definida por el usuario es un par de clave-valor que puede asociar a un almacén de datos de eventos. Tras activar las etiquetas de asignación de costes, las AWS utiliza para organizar los costes de los recursos en el informe de asignación de costes.

- Para crear etiquetas en la consola, consulte el paso 9 del procedimiento Para crear un almacén de datos de eventos para eventos CloudTrail de administración o de datos.
- Para crear etiquetas con la CloudTrail API, consulte CreateEventDataStorey AddTagsen la referencia de la AWS CloudTrail API.
- Para crear etiquetas con ella AWS CLI, consulte create-event-data-storey añada etiquetas en la Referencia de AWS CLI comandos.

Para obtener más información, consulte Activación de etiquetas de asignación de costos definidas por el usuario.

Véase también

- Precios de AWS CloudTrail
- Métricas compatibles CloudWatch
- Gestione sus costes con AWS Budgets
- Introducción al Explorador de costos

Métricas de CloudWatch compatibles

CloudTrail Lake admite las métricas de Amazon CloudWatch. CloudWatch es un servicio de monitoreo de los recursos de AWS. Puede utilizar CloudWatch para recopilar y realizar un seguimiento de las métricas, establecer alarmas y reaccionar de forma automática a los cambios de los recursos de AWS.

El espacio de nombres de `AWS/CloudTrail` incluye las siguientes métricas para CloudTrail Lake.

Métrica	Descripción	Unidades
`HourlyDataIngested`	La cantidad de datos ingeridos en el almacén de datos de eventos durante la última hora. Esta métrica se actualiza cada hora. Esta métrica está disponibl e para todos los tipos de almacenes de datos de eventos.	Bytes
`TotalDataRetained`	La cantidad de datos retenidos en el almacén de datos de eventos durante todo su periodo de retención. Esta métrica se actualiza todas las noches. Esta métrica está disponibl e para todos los tipos de almacenes de datos de eventos.	Bytes
`TotalStorageBytes`	El total de bytes comprimid os en el almacén de datos de eventos en el día actual.	Bytes

Métrica	Descripción	Unidades
	Esta métrica está disponible para todos los tipos de almacenes de datos de eventos.	

Métrica	Descripción	Unidades
`TotalPaidStorageBytes`	Para los almacenes de datos de eventos que utilizan la opción de precio de retención ampliable por un año, este es el total de bytes comprimidos después de 366 días hasta el periodo de retención máximo configurado para el almacén de datos de eventos. En el caso de los almacenes de datos de eventos que utilizan la opción de precios de retención ampliables por un año, el almacenamiento se incluye sin costo adicional en los precios de incorporación durante los primeros 366 días, que es el periodo de retención predeterminado para el almacén de datos de eventos. Después de 366 días, el almacenamiento es de pago por uso. Para obtener más información acerca de los precios, consulte Precios de AWS CloudTrail. Esta métrica solo está disponible para los almacenes de datos de eventos que utilizan la opción de precios de retención ampliables por un año.	Bytes

Métrica	Descripción	Unidades
`HourlyEventsAnalyzed`	El número total de eventos analizados por CloudTrai l Insights en el almacén de datos de eventos. Esta métrica se actualiza cada hora. Esta métrica es para los almacenes de datos de eventos de CloudTrail que habilitan CloudTrail Insights.	Recuento

Para obtener más información sobre las métricas de CloudWatch, consulte los siguientes temas.

- Uso de métricas de Amazon CloudWatch
- Uso de las alarmas de Amazon CloudWatch

Trabajar con registros de seguimiento de CloudTrail

Para mantener un registro continuo de los eventos de la cuenta de AWS, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS de la partición de AWS en la que trabaja. 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.

Si ha creado una organización en AWS Organizations, puede crear un registro de seguimiento que registrará todos los eventos de todas las Cuentas de AWS en dicha organización. La creación de un registro de seguimiento de organización lo ayuda a definir una estrategia uniforme de registro de eventos para su organización.

Temas

- Creación de un registro de seguimiento para su Cuenta de AWS
- Creación de un registro de seguimiento para una organización
- Visualizar eventos de CloudTrail Insights para registros de seguimiento
- Copiar los eventos del sendero al CloudTrail lago
- Obtención y visualización de archivos de registros de CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Consejos para la administración de registros de seguimiento
- Controlar los permisos de usuario para los registros de seguimiento de CloudTrail
- Uso de AWS CloudTrail con los puntos de enlace de la VPC de la interfaz
- Cuenta de AWS cierre y senderos

Creación de un registro de seguimiento para su Cuenta de AWS

Al crear un registro de seguimiento, se habilita la entrega continua de eventos como archivos de registros a un bucket de Amazon S3 especificado. La creación de un registro de seguimiento tiene muchos beneficios, entre ellos:

- Un registro de eventos que se extiende más allá de los 90 días.
- La opción de monitorear y enviar alarmas de forma automática de los eventos especificados mediante el envío de los eventos de registro a Amazon CloudWatch Logs.
- La opción de consultar los registros y analizar la actividad de servicio de AWS con Amazon Athena.

A partir del 12 de abril de 2019, solo puede ver los registros de seguimiento en las regiones de AWS en las que se registren eventos. Si crea un registro de seguimiento que registra eventos en todas las regiones de AWS, aparecerá en la consola en todas las regiones de la partición de AWS en la que trabaja. Si crea un registro de seguimiento que solo registra los eventos en una región, solo podrá verlo y administrarlo en esa región. Crear un registro de seguimiento de varias regiones es la opción predeterminada si crea un registro de seguimiento mediante la consola de AWS CloudTrail, lo que es una práctica recomendada. Para crear un registro de seguimiento de una sola región, debe utilizar la AWS CLI.

Si usa AWS Organizations, puede crear un registro de seguimiento que registrará los eventos de todas las cuentas de AWS en la organización. Se creará un registro de seguimiento con el mismo nombre en cada cuenta miembro y los eventos de cada registro de seguimiento se entregarán al bucket de Amazon S3 que especifique.

> **Note**
>
> Solo la cuenta de administración o la cuenta del administrador delegado de una organización pueden crear un registro de seguimiento para la organización. La creación de un registro de seguimiento para una organización habilita de forma automática la integración entre CloudTrail y Organizations. Para obtener más información, consulte Creación de un registro de seguimiento para una organización.

Temas

- Creación y actualización de un registro de seguimiento con la consola
- Creación, actualización y gestión de senderos con AWS Command Line Interface

Creación y actualización de un registro de seguimiento con la consola

Puede usar la consola de CloudTrail para crear, actualizar o eliminar sus registros de seguimiento. Los registros de seguimiento que cree con la consola son de varias regiones. Para crear un registro de seguimiento que registre los eventos en una sola Región de AWS, utilice la AWS CLI.

Puede crear hasta cinco registros de seguimiento en cada región. Después de crear un registro de seguimiento, CloudTrail comienza de forma automática a registrar las llamadas a la API y los eventos relacionados de su cuenta en el bucket de Amazon S3 que especifique. Para detener el registro, puede desactivar el registro del registro de seguimiento o eliminarlo.

El uso de la consola de CloudTrail para crear o actualizar un registro de seguimiento ofrece las siguientes ventajas.

- Si es la primera vez que crea un registro de seguimiento, la consola de CloudTrail le permite ver las características y opciones disponibles.
- En caso de que esté configurando un registro de seguimiento para registrar eventos de datos, la consola de CloudTrail le permite ver los tipos de datos disponibles. Para obtener más información sobre el registro de eventos de datos, consulte Registro de eventos de datos.

Para obtener información específica sobre la creación de un registro de seguimiento para una organización en AWS Organizations, consulte Creación de un registro de seguimiento para una organización.

Temas

- Creación de un registro de seguimiento
- Actualización de un registro de seguimiento
- Eliminación de un registro de seguimiento
- Desactivación del registro de un registro de seguimiento

Creación de un registro de seguimiento

Como práctica recomendada se aconseja crear un registro de seguimiento que se aplica a todas las Regiones de AWS. Esta es la configuración predeterminada al crear una ruta en la CloudTrail consola. Cuando un registro se aplica a todas las regiones, CloudTrail envía los archivos de registro de todas las regiones de la AWS partición en la que está trabajando a un bucket de S3 que

especifique. Tras crear la ruta, comienza a registrar AWS CloudTrail automáticamente los eventos que especificó.

> **Note**
>
> Después de crear un rastro, puede configurar otro Servicios de AWS para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte AWS integraciones de servicios con registros CloudTrail .

Temas

- Creación de un registro de seguimiento en la consola
- Siguientes pasos

Creación de un registro de seguimiento en la consola

Utilice el siguiente procedimiento para crear un registro que registre todos los Regiones de AWS eventos de la AWS partición en la que esté trabajando. Esta es una práctica recomendada. Para registrar eventos en una sola región (no recomendado), utilice la AWS CLI.

Para crear una CloudTrail ruta con AWS Management Console

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En la página de inicio del CloudTrail servicio, la página Rutas o la sección Rutas de la página del panel de control, selecciona Crear ruta.
3. En la página Create Trail, escriba el nombre del registro de seguimiento en Trail name. Para obtener más información, consulte Requisitos de nomenclatura.
4. Si se trata de un registro de AWS Organizations la organización, puede habilitar el registro para todas las cuentas de su organización. Para ver esta opción, debe iniciar sesión en la consola con un usuario o un rol de la cuenta de administración o la de administrador delegado. Para crear correctamente un registro de seguimiento de organización, asegúrese de que el usuario o el rol tengan permisos suficientes. Para obtener más información, consulte Creación de un registro de seguimiento para una organización.

5. En Storage location (Ubicación del almacenamiento), elija Create new S3 bucket (Crear un bucket de S3 nuevo) para crear un bucket. Al crear un bucket, CloudTrail crea y aplica las políticas de bucket requeridas.

   > **Note**
   >
   > Si seleccionó Utilizar bucket de S3 existente, especifique un bucket en Nombre del bucket de registro de seguimiento o seleccione Examinar para seleccionar un bucket de su propia cuenta. Si desea utilizar un bucket en otra cuenta, deberá especificar el nombre del bucket. La política de bucket debe conceder CloudTrail permiso para escribir en él. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Política de bucket de Amazon S3 para CloudTrail.

   Para facilitar la búsqueda de tus registros, crea una nueva carpeta (también conocida como prefijo) en un depósito existente para almacenar tus CloudTrail registros. Ingrese el prefijo en Prefix (Prefijo).

6. En Log file SSE-KMS encryption (Cifrado SSE-KMS de archivos de registro), elija Enabled (Habilitado) si desea cifrar sus archivos de registro con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los registros se cifrarán mediante el cifrado SSE-S3. Para obtener más información sobre el cifrado SSE-KMS, consulte Uso del cifrado del lado del servidor con (SSE-KMS). AWS Key Management Service Para obtener más información sobre el cifrado SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 [SSE-S3]).

   Si habilita el cifrado SSE-KMS, elija uno nuevo o existente. AWS KMS key En AWS KMS Alias, especifique un alias en el formato. `alias/` *`MyAliasName`* Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

   > **Note**
   >
   > También puede escribir el ARN de una clave de otra cuenta. Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS.

La política de claves debe CloudTrail permitir el uso de la clave para cifrar los archivos de registro y permitir que los usuarios que especifique lean los archivos de registro sin cifrar. Para obtener más información sobre cómo editar manualmente la política de claves, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

7. En Additional settings (Configuración adicional), configure lo siguiente.

   a. En Log file validation (Validación de archivo de registros), elija Enabled (Habilitado) para que se envíen los resúmenes de archivos de registros a su bucket de S3. Puede utilizar los archivos de resumen para comprobar que los archivos de registro no han cambiado después de CloudTrail entregarlos. Para obtener más información, consulte Validar la integridad de los archivos de registros de CloudTrail.

   b. Para la entrega de notificaciones de SNS, selecciona Activado para recibir una notificación cada vez que se entregue un registro a tu depósito. CloudTrail almacena varios eventos en un archivo de registro. Las notificaciones de SNS se envían para cada archivo de registro, no para cada evento. Para obtener más información, consulte Configuración de notificaciones de Amazon SNS para CloudTrail.

      Si habilita las notificaciones SNS, en Create a new SNS topic (Crear un tema de SNS nuevo), elija New (Nuevo) para crear un tema o elija Existing (Existente) a fin de utilizar un tema existente. Si va a crear un registro de seguimiento que se aplica a todas las regiones, las notificaciones de SNS de los envíos de archivos de registro de todas las regiones se envían al tema de SNS que cree.

      Si elige Nuevo, CloudTrail especifica un nombre para el nuevo tema o puede escribir un nombre. Si elige Existing (Existente), elija un tema de SNS en la lista desplegable. También puede especificar el ARN de un tema de otra región o de una cuenta con los permisos adecuados. Para obtener más información, consulte Política temática de Amazon SNS para CloudTrail.

      Si crea un tema, deberá suscribirse al tema para recibir una notificación del envío de archivos de registro. Puede suscribirse en la consola de Amazon SNS. Debido a la frecuencia de las notificaciones, recomendamos que configure la suscripción para que se utilice una cola de Amazon SQS a fin de administrar las notificaciones mediante programación. Para obtener más información, consulte la Guía de introducción de Amazon Simple Notification Service.

8. Si lo desea, configure CloudTrail el envío de archivos de registro a CloudWatch Logs seleccionando Activado en CloudWatch los registros. Para obtener más información, consulte Envío de eventos a Amazon CloudWatch Logs.

   a. Si habilita la integración con CloudWatch los registros, elija Nuevo para crear un nuevo grupo de registros o Existente para usar uno existente. Si elige Nuevo, CloudTrail especifique un nombre para el nuevo grupo de registros o puede escribir un nombre.

   b. Si elige Existing (Existente), elija un grupo de registros en la lista desplegable.

   c. Elija Nuevo para crear un nuevo rol de IAM con los permisos necesarios para enviar CloudWatch registros a Logs. Elija Existing (Existente) para elegir un rol de IAM en la lista desplegable. La instrucción de la política para el rol nuevo o existente se muestra al expandir Policy document (Documento de política). Para obtener más información acerca de este rol, consulte Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear.

   > **Note**
   >
   > - Cuando configura un registro de seguimiento, puede elegir un bucket de S3 y un tema de SNS que pertenezcan a otra cuenta. Sin embargo, si desea CloudTrail enviar eventos a un grupo de CloudWatch registros, debe elegir un grupo de registros que exista en su cuenta actual.
   > - Solo la cuenta de administración puede configurar un grupo de CloudWatch registros para un registro de la organización mediante la consola. El administrador delegado puede configurar un grupo de CloudWatch registros mediante las operaciones de la `UpdateTrail` API AWS CLI CloudTrail `CreateTrail` o o.

9. En Tags (Etiquetas), agregue una o más etiquetas personalizadas (pares clave-valor) a su registro de seguimiento. Las etiquetas pueden ayudarle a identificar tanto sus CloudTrail senderos como los depósitos de Amazon S3 que contienen archivos de CloudTrail registro. A continuación, puede utilizar grupos de recursos para sus CloudTrail recursos. Para más información, consulte AWS Resource Groups y ¿Por qué usar etiquetas para CloudTrail los recursos?.

10. En la página Choose log events (Elegir eventos de registro), elija los tipos de eventos que desea registrar. En Management events (Eventos de administración), haga lo siguiente.

a. En API activity (Actividad de la API), elija si desea que su registro de seguimiento registre eventos de Read (Lectura), Write (Escritura) o ambos. Para obtener más información, consulte Eventos de administración.

b. Elige Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) los eventos de tu ruta. La configuración predeterminada es incluir todos los AWS KMS eventos.

   La opción de registrar o excluir AWS KMS eventos solo está disponible si registra los eventos de administración en su ruta. Si decide no registrar los eventos de administración, los AWS KMS eventos no se registran y no puede cambiar la configuración AWS KMS del registro de eventos.

   AWS KMS acciones como `EncryptDecrypt`, y `GenerateDataKey` suelen generar un gran volumen (más del 99%) de eventos. Estas acciones se registran ahora como eventos de lectura. AWS KMS Las acciones relevantes de bajo volumen, como `DisableDelete`, y `ScheduleKey` (que normalmente representan menos del 0,5% del volumen de AWS KMS eventos) se registran como eventos de escritura.

   Para excluir eventos de gran volumen**`Encrypt`**, como**`Decrypt`**, y**`GenerateDataKey`**, sin dejar de registrar eventos relevantes**`Disable`**, como **`Delete`** y**`ScheduleKey`**, elija registrar eventos de administración de escritura y desactive la casilla Excluir eventos. AWS KMS

c. Elija Exclude Amazon RDS Data API events (Excluir eventos de API de datos de Amazon RDS) para quitar del registro de seguimiento los eventos de API de datos de Amazon Relational Database Service. La configuración predeterminada es incluir a todos los eventos de la API de datos de Amazon RDS. A fin de obtener más información sobre los eventos de API de datos de Amazon RDS, consulte Registro de llamadas a la API de datos con AWS CloudTrail en la Guía del usuario de Amazon RDS para Aurora.

11. Para registrar eventos de datos, elija Data events (Eventos de datos). Se aplican cargos adicionales para registrar eventos de datos. Para obtener más información, consulte AWS CloudTrail Precios.

12. **Important**

    Los pasos del 12 al 16 son para configurar los eventos de datos mediante selectores de eventos avanzados, que son los predeterminados. Los selectores de eventos avanzados le permiten configurar más tipos de eventos de datos y ofrecen un control detallado de los eventos de datos que captura su registro de seguimiento. Si ha optado por utilizar selectores de eventos básicos, complete los pasos que se indican en Configurar los

ajustes de eventos de datos mediante selectores de eventos básicos y, a continuación, vuelva al paso 17 de este procedimiento.

En Data event type (Tipo de evento de datos), elija el tipo de recurso en el que desea registrar los eventos de datos. Para obtener más información sobre los tipos de eventos de datos disponibles, consulte Eventos de datos.

> **Note**
>
> Para registrar los eventos de datos de AWS Glue las tablas creadas por Lake Formation, elija Lake Formation.

13. Elija una plantilla de selección de registros. CloudTrail incluye plantillas predefinidas que registran todos los eventos de datos del tipo de recurso. Para crear una plantilla de selector de registros personalizada, elija Custom (Personalizado).

> **Note**
>
> Si eliges una plantilla predefinida para los depósitos de S3, podrás registrar los eventos de datos de todos los depósitos que hay actualmente en tu AWS cuenta y de los que crees una vez que hayas terminado de crear el registro. También permite registrar la actividad de eventos de datos realizada por cualquier identidad de IAM de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
> Si el registro de seguimiento solo aplica a una región, elegir una plantilla predefinida que registra todos los buckets de S3 permite el registro de eventos de datos de todos los buckets en la misma región que el registro de seguimiento, así como de cualquier otro bucket que cree posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de su AWS cuenta.
> Si va a crear un registro para todas las regiones, al elegir una plantilla predefinida para las funciones de Lambda se habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en su AWS cuenta y para cualquier función de Lambda que pueda crear en cualquier región una vez que haya terminado de crear el registro. Si va a crear una ruta para una sola región (mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de

Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
El registro de los eventos de datos para todas las funciones también permite registrar la actividad de los eventos de datos realizada por cualquier identidad de IAM de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

14. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo opcional para un selector de eventos avanzado, como “Registrar eventos de datos para solo dos buckets de S3”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
15. En Advanced event selectors (Selectores de eventos avanzados), cree una expresión para los recursos específicos en los que desea registrar eventos de datos. Puede omitir este paso si utiliza una plantilla de registro predefinida.

    a. Elija uno de los siguientes campos.

    - **`readOnly`**- se `readOnly` puede configurar para que sea igual a un valor de `true` o`false`. Los eventos de datos de solo lectura son eventos que no cambian el estado de un recurso, como eventos `Get*` o `Describe*`. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`. Para registrar eventos `read` y `write`, no agregue un selector de `readOnly`.
    - **`eventName`**: `eventName` puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de datos registrado CloudTrail, como `PutBucketPutItem`, o`GetSnapshotBlock`.
    - **`resources.ARN`**- Puede usar cualquier operador con`resources.ARN`, pero si usa valores iguales o no iguales, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo que especificó en la plantilla como valor de. `resources.type`

      En la siguiente tabla, se muestra el formato de ARN de cada `resources.type`.

      > **Note**
      >
      > No puede usar el `resources.ARN` campo para filtrar los tipos de recursos que no tienen ARN.

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*

resources.type	resources.ARN
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*

resources.type	resources.ARN
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_c omponent_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemake r: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_I D* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespac e/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_I D*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_I D* :endpoint/ *endpoint_type* /*endpoint_ name* /*endpoint_ID*

resources.type	resources.ARN
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	El ARN debe estar en uno de los siguientes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir los eventos de streaming, añade un filtro en el `eventName` campo.

[2] Para registrar todos los eventos de datos de todos los objetos en un bucket de S3 específico, utilice el operador `StartsWith` e incluya solo el ARN del bucket como valor coincidente. La barra diagonal final es intencional; no la excluya.

[3] Para registrar eventos en todos los objetos de un punto de acceso de S3, se recomienda que utilice solo el ARN del punto de acceso. No incluya la ruta de acceso del objeto y utilice los operadores `StartsWith` o `NotStartsWith`.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte Acciones, recursos y claves de condición en la Guía del usuario de AWS Identity and Access Management .

b. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones. Por ejemplo, para excluir los eventos de datos de dos cubos de S3 de los eventos de datos que se registran en su ruta, puede establecer el campo en Resources.ARN, configurar el operador

para no comienza por y, a continuación, pegar el ARN de un bucket de S3 o buscar los cubos de S3 para los que no desea registrar eventos.

Para agregar el segundo bucket de S3, seleccione + Condición y, a continuación, repita la instrucción anterior, pegue el ARN o busque un bucket diferente.

> **Note**
>
> Puede tener un máximo de 500 valores para todos los selectores de un registro de seguimiento. Esto incluye matrices de varios valores para un selector como `eventName`. Si tiene valores únicos para todos los selectores, puede agregar un máximo de 500 condiciones a un selector.
> Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Puede registrar todas las funciones con una plantilla de selector predefinida, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear la ruta en la consola y, a continuación, utilizar el put-event-selectors comando AWS CLI and the para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Administrar senderos con el AWS CLI.

c. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos. Por ejemplo, no especifique un ARN en un selector para que sea igual a un valor y luego especifique que el ARN no sea igual al mismo valor en otro selector.

16. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos). Repita los pasos, desde el número 12 a este paso, a fin de configurar selectores de eventos avanzados para el tipo de evento de datos.
17. Elija los eventos de Insights si quiere que su ruta registre los eventos de CloudTrail Insights.

    En Event type (Tipo de evento), seleccione Insights events (Eventos de Insights). Debe registrar los eventos de administración de escritura para registrar los eventos de Insights para calcular la tasa de llamadas a la API. Debe registrar los eventos de administración de lectura o escritura para registrar los eventos de Insights para calcular la tasa de errores de la API.

    CloudTrail Insights analiza los eventos de administración para detectar actividades inusuales y los registra cuando se detectan anomalías. De forma predeterminada, los registros de

seguimiento no registran eventos de Insights. Para obtener más información acerca de los eventos de Insights, consulte Registro de eventos de Insights. Se aplican cargos adicionales por registrar eventos de Insights. Para CloudTrail conocer los precios, consulte AWS CloudTrail Precios.

Los eventos de Insights se envían a una carpeta diferente con el nombre `/CloudTrail-Insight` del mismo depósito de S3 que se especifica en el área de ubicación de almacenamiento de la página de detalles de la ruta. CloudTrailcrea el nuevo prefijo para usted. Por ejemplo, si el bucket de S3 de destino actual se denomina `S3bucketName/AWSLogs/CloudTrail/`, el nombre del bucket de S3 con un nuevo prefijo se denomina `S3bucketName/AWSLogs/CloudTrail-Insight/`.

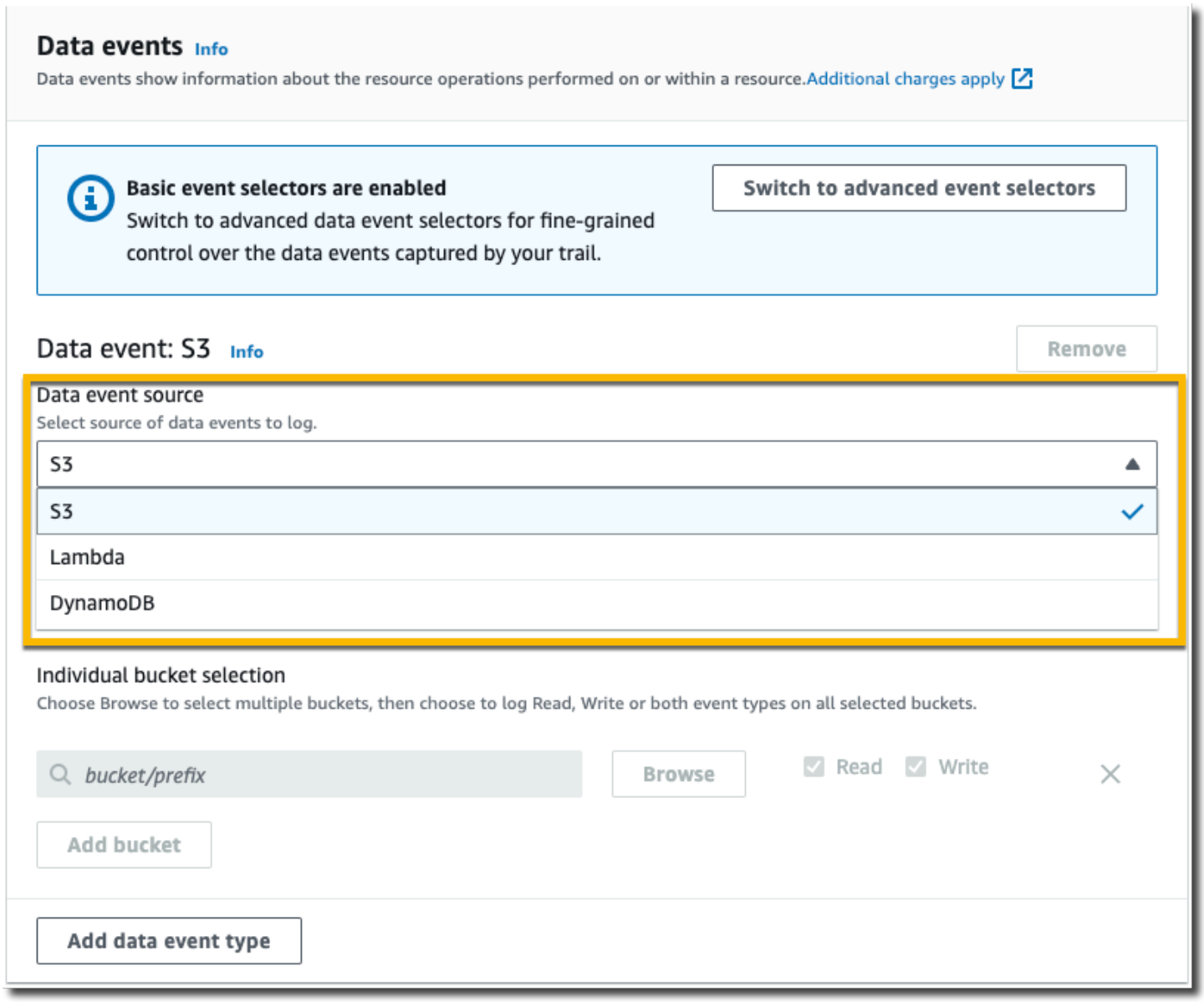
18. Cuando haya terminado de elegir los tipos de eventos para registrar, elija Next (Siguiente).
19. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) en una sección para cambiar la configuración del registro de seguimiento que se muestra en esa sección. Cuando esté listo para crear el registro de seguimiento, elija Create trail (Crear registro de seguimiento).
20. El nuevo registro de seguimiento aparece en la página Trails. En unos 5 minutos, CloudTrail publica los archivos de registro que muestran las llamadas a la AWS API realizadas en tu cuenta. Puede ver los archivos de registro del bucket de S3 especificado. La entrega del primer evento de Insights puede tardar hasta 36 horas si ha activado el registro de eventos de Insights y se detecta una actividad inusual. CloudTrail

> **Note**
>
> CloudTrail Por lo general, entrega los registros en una media de unos 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el Acuerdo de nivel de servicios de AWS CloudTrail.
> Si configuras mal la ruta (por ejemplo, si no se puede acceder al depósito de S3), CloudTrail intentarás volver a enviar los archivos de registro a tu depósito de S3 durante 30 días. Estos attempted-to-deliver eventos estarán sujetos a los cargos estándar. CloudTrail Para evitar que se le cobre por un registro de seguimiento mal configurado, debe eliminarlo.

Configurar los ajustes de eventos de datos mediante selectores de eventos básicos

Puede utilizar selectores de eventos avanzados para configurar todos los tipos de eventos de datos. Los selectores de eventos avanzados le permiten crear selectores detallados para registrar solo los eventos de interés.

Si utiliza selectores de eventos básicos para registrar eventos de datos, está limitado a registrar eventos de datos para buckets, AWS Lambda funciones y tablas de Amazon DynamoDB de Amazon S3. No puede filtrar el `eventName` campo con selectores de eventos básicos.



Use el procedimiento siguiente para configurar los ajustes de eventos de datos mediante selectores de eventos básicos.

Para configurar los ajustes de eventos de datos mediante selectores de eventos básicos

1. En Eventos, seleccione Eventos de datos para registrar eventos de datos. Se aplican cargos adicionales para registrar eventos de datos. Para obtener más información, consulte AWS CloudTrail Precios.
2. Para buckets de Amazon S3:

   a. En Data event source (Fuente de evento de datos), elija S3.

   b. Puede registrar All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) o bien, especificar buckets o funciones individuales. De forma predeterminada, los eventos de datos se registran para todos los buckets de S3 actuales y futuros.

   > **Note**
   >
   > Si mantiene la opción predeterminada Todos los depósitos de S3 actuales y futuros, se permite registrar los eventos de datos de todos los depósitos que se encuentren actualmente en su AWS cuenta y de todos los depósitos que cree una vez que haya terminado de crear la ruta. También permite registrar la actividad de eventos de datos realizada por cualquier identidad de IAM de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
   > Si va a crear un sendero para una sola región (lo hace con AWS CLI), si selecciona Todos los depósitos de S3 actuales y futuros, se habilita el registro de eventos de datos para todos los grupos de la misma región que su ruta y para cualquier grupo que cree más adelante en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de su AWS cuenta.

   c. Si conserva la opción predeterminada, All current and future S3 buckets (Todos los buckets de S3 actuales y futuros), elija registrar eventos de Read (Lectura), Write (Escritura) o ambos.

   d. Para seleccionar buckets individuales, desmarque las casillas de verificación Read (Lectura) y Write (Escritura) en All current and future S3 buckets (Todos los buckets de S3 actuales y futuros). En Individual bucket selection (Selección de bucket individual), busque un bucket en el que registrar los eventos de datos. Busque buckets específicos al escribir un prefijo de bucket para el bucket que desee. En esta ventana puede seleccionar varios buckets. Elija Add bucket (Agregar bucket) para registrar eventos de datos en más buckets. Elija registrar eventos de Read (Lectura), como `GetObject`, Write (Escritura), como `PutObject`, o de ambos.

Esta configuración tiene prioridad sobre la configuración individual de cada bucket. Por ejemplo, si establece la configuración para que se registren los eventos de tipo Read de todos los buckets de S3 y posteriormente decide agregar un determinado bucket en el registro de eventos de datos, la opción Read ya aparecerá seleccionada en el bucket que agregue. Esta selección no se puede anular. Solo se puede configurar la opción Write.

Para eliminar un bucket del registro, elija X.

3. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos).
4. Para funciones Lambda:

   a. En Data event source (Fuente de evento de datos), elija Lambda.

   b. En Lambda function (Función Lambda), elija All regions (Todas las regiones) para registrar todas las funciones Lambda, o Input function as ARN (Función de entrada como ARN) a fin de registrar eventos de datos en una función específica.

   Para registrar los eventos de datos de todas las funciones de Lambda de su AWS cuenta, seleccione Registrar todas las funciones actuales y futuras. Esta configuración tiene prioridad sobre la configuración individual de cada función. Se registran todas las funciones aunque no se muestren.

   > **Note**
   >
   > Si va a crear un registro de seguimiento para todas las regiones, esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en la cuenta de AWS , así como de cualquier función Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear una ruta para una sola región (mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
   > El registro de los eventos de datos para todas las funciones también permite registrar la actividad de los eventos de datos realizada por cualquier identidad de IAM de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

c. Si elige Input function as ARN (Función de entrada como ARN), ingrese el ARN de una función Lambda.

> **Note**
>
> Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Sí que puede seleccionar la opción para registrar todas las funciones, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear la ruta en la consola y, a continuación, utilizar el put-event-selectors comando AWS CLI and the para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Administrar senderos con el AWS CLI.

5. Para tablas de DynamoDB:

   a. En Data event source (Fuente de evento de datos), elija DynamoDB.

   b. En DynamoDB table selection (Selección de tabla de DynamoDB), elija Browse (Examinar) para seleccionar una tabla o pegue el ARN de una tabla de DynamoDB a la que tenga acceso. El ARN de la tabla de DynamoDB utiliza el siguiente formato:

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   Para agregar otra tabla, elija Add row (Agregar fila) y busque una tabla o pegue el ARN de una tabla a la que tenga acceso.

6. A fin de configurar eventos de Insights y otras configuraciones para su registro de seguimiento, vuelva al procedimiento anterior en este tema, ???.

Siguientes pasos

Después de crear el registro de seguimiento, puede volver a él para realizar cambios:

- Si aún no lo ha hecho, puede configurarlo CloudTrail para enviar los archivos de registro a CloudWatch Logs. Para obtener más información, consulte Envío de eventos a Amazon CloudWatch Logs.

- Cree una tabla y utilícela para ejecutar una consulta en Amazon Athena con el fin de analizar su actividad de servicio de AWS . Para obtener más información, consulte Creación de una tabla de CloudTrail registros en la CloudTrail consola en la Guía del usuario de Amazon Athena.
- Agregar etiquetas personalizadas (pares de clave-valor) al registro de seguimiento
- Para crear otro registro de seguimiento, abra la página Registros de seguimiento y seleccione Crear registro de seguimiento.

Actualización de un registro de seguimiento

En esta sección se describe cómo cambiar la configuración del registro de seguimiento.

Para actualizar un registro de una sola región para registrar los eventos Regiones de AWS en toda la AWS partición en la que está trabajando, o actualizar un registro de varias regiones para registrar los eventos en una sola región, debe usar el. AWS CLI Para obtener más información sobre cómo actualizar un registro de seguimiento de una sola región a fin de registrar eventos en todas las regiones, consulte Conversión de un registro de seguimiento que se aplica a una sola región en uno que se aplique a todas las regiones. Para obtener más información sobre cómo actualizar un registro de seguimiento de varias regiones a fin de registrar eventos en una sola región, consulte Conversión de un registro de seguimiento de varias regiones en un registro de seguimiento de una sola región.

Si ha habilitado los eventos CloudTrail de administración en Amazon Security Lake, debe mantener al menos un registro organizativo que sea multirregional y registre tanto `read` los eventos de administración como los eventos `write` de administración. No puede actualizar un registro de seguimiento válido de forma que no cumpla con el requisito de Security Lake. Por ejemplo, si cambia el registro de seguimiento a uno de una sola región o desactiva el registro de los eventos de administración de `read` o `write`.

> **Note**
>
> CloudTrail actualiza los registros de la organización en las cuentas de los miembros incluso si se produce un error en la validación de un recurso. Algunos ejemplos de errores de validación son:
>
> - una política de bucket de Amazon S3 incorrecta
> - una política de temas de Amazon SNS incorrecta
> - incapacidad para realizar envíos a un grupo CloudWatch de registros
> - permiso insuficiente para cifrar mediante una clave KMS

Una cuenta de miembro con CloudTrail permisos puede ver cualquier error de validación del registro de una organización consultando la página de detalles del registro en la CloudTrail consola o ejecutando el AWS CLI get-trail-statuscomando.

Para actualizar una ruta con el AWS Management Console

1. Inicia sesión en la CloudTrail consola AWS Management Console y ábrela en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, elija Trails (Registros de seguimiento) y, a continuación, elija un nombre de registro de seguimiento.
3. En General details (Detalles generales), elija Edit (Editar) para cambiar la siguiente configuración. No puede cambiar el nombre de un registro de seguimiento.

   - Aplicar un registro a mi organización: cambie si este registro es un registro de AWS Organizations la organización.

     > **Note**
     >
     > Solo la cuenta de administración de la organización puede convertir un registro de seguimiento de la organización en un registro de seguimiento que no sea de la organización o convertir un registro de seguimiento que no es de la organización en un registro de seguimiento de la organización.

   - Ubicación del registro de seguimiento: cambie el nombre del prefijo o bucket de S3 en el que se almacenan los registros para este registro de seguimiento.
   - Cifrado SSE-KMS de archivos de registros: elija habilitar o desactivar el cifrado de los archivos de registro con SSE-KMS en vez de con SSE-S3.
   - Validación de archivos de registros: elija habilitar o desactivar la validación de la integridad de los archivos de registros.
   - Entrega de notificaciones SNS: elija habilitar o desactivar las notificaciones de Amazon Simple Notification Service (Amazon SNS) que indican que los archivos de registros se han enviado al bucket especificado para el registro de seguimiento.

a. Para cambiar el registro por un registro de AWS Organizations la organización, puede optar por habilitar el registro para todas las cuentas de su organización. Para obtener más información, consulte Creación de un registro de seguimiento para una organización.

b. Para cambiar el bucket especificado en Storage location (Ubicación de almacenamiento), elija Create new S3 bucket (Crear un bucket de S3 nuevo) a fin de crear un bucket. Al crear un grupo, CloudTrail crea y aplica las políticas de grupo requeridas.

> **Note**
>
> Si eligió Use existing S3 bucket (Utilizar bucket de S3 existente), especifique un bucket en Trail log bucket name (Nombre del bucket de registro de seguimiento), o elija Browse (Examinar) para elegir un bucket. La política de bucket debe conceder CloudTrail permiso para escribir en él. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Política de bucket de Amazon S3 para CloudTrail.

Para facilitar la búsqueda de tus registros, crea una nueva carpeta (también conocida como prefijo) en un depósito existente para almacenar tus CloudTrail registros. Ingrese el prefijo en Prefix (Prefijo).

c. En Log file SSE-KMS encryption (Cifrado SSE-KMS de archivos de registro), elija Enabled (Habilitado) si desea cifrar sus archivos de registro con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los registros se cifrarán mediante el cifrado SSE-S3. Para obtener más información sobre el cifrado SSE-KMS, consulte Uso del cifrado del lado del servidor con (SSE-KMS). AWS Key Management Service Para obtener más información sobre el cifrado SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 [SSE-S3]).

Si habilita el cifrado SSE-KMS, elija uno nuevo o existente. AWS KMS key En AWS KMS Alias, especifique un alias en el formato. `alias/` *`MyAliasName`* Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS. CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

> **Note**
>
> También puede escribir el ARN de una clave de otra cuenta. Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS. La política de claves debe CloudTrail permitir el uso de la clave para cifrar los archivos de registro y permitir que los usuarios que especifique lean los archivos de registro sin cifrar. Para obtener más información sobre cómo editar manualmente la política de claves, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

d. En Log file validation (Validación de archivo de registros), elija Enabled (Habilitado) para que se envíen los resúmenes de archivos de registros a su bucket de S3. Puede utilizar los archivos de resumen para comprobar que los archivos de registro no han cambiado después de CloudTrail entregarlos. Para obtener más información, consulte Validar la integridad de los archivos de registros de CloudTrail.

e. Para la entrega de notificaciones de SNS, selecciona Activado para recibir una notificación cada vez que se entregue un registro a tu depósito. CloudTrail almacena varios eventos en un archivo de registro. Las notificaciones de SNS se envían para cada archivo de registro, no para cada evento. Para obtener más información, consulte Configuración de notificaciones de Amazon SNS para CloudTrail.

   Si habilita las notificaciones SNS, en Create a new SNS topic (Crear un tema de SNS nuevo), elija New (Nuevo) para crear un tema o elija Existing (Existente) a fin de utilizar un tema existente. Si va a crear un registro de seguimiento que se aplica a todas las regiones, las notificaciones de SNS de los envíos de archivos de registro de todas las regiones se envían al tema de SNS que cree.

   Si elige Nuevo, CloudTrail especifica un nombre para el nuevo tema o puede escribir un nombre. Si elige Existing (Existente), elija un tema de SNS en la lista desplegable. También puede especificar el ARN de un tema de otra región o de una cuenta con los permisos adecuados. Para obtener más información, consulte Política temática de Amazon SNS para CloudTrail.

   Si crea un tema, deberá suscribirse al tema para recibir una notificación del envío de archivos de registro. Puede suscribirse en la consola de Amazon SNS. Debido a la frecuencia de las notificaciones, recomendamos que configure la suscripción para que se utilice una cola de Amazon SQS a fin de administrar las notificaciones mediante

programación. Para obtener más información, consulte la Guía de introducción de Amazon Simple Notification Service.

4. En CloudWatch Registros, elija Editar para cambiar la configuración de envío de archivos de CloudTrail registro a CloudWatch Registros. Seleccione Activado en CloudWatch los registros para activar el envío de archivos de registro. Para obtener más información, consulte Envío de eventos a Amazon CloudWatch Logs.

   a. Si habilita la integración con CloudWatch los registros, elija Nuevo para crear un nuevo grupo de registros o Existente para usar uno existente. Si elige Nuevo, CloudTrail especifique un nombre para el nuevo grupo de registros o puede escribir un nombre.

   b. Si elige Existing (Existente), elija un grupo de registros en la lista desplegable.

   c. Elija Nuevo para crear un nuevo rol de IAM con los permisos necesarios para enviar CloudWatch registros a Logs. Elija Existing (Existente) para elegir un rol de IAM en la lista desplegable. La instrucción de la política para el rol nuevo o existente se muestra al expandir Policy document (Documento de política). Para obtener más información acerca de este rol, consulte Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear.

   > **Note**
   >
   > - Cuando configura un registro de seguimiento, puede elegir un bucket de S3 y un tema de SNS que pertenezcan a otra cuenta. Sin embargo, si desea CloudTrail enviar eventos a un grupo de CloudWatch registros, debe elegir un grupo de registros que exista en su cuenta actual.
   > - Solo la cuenta de administración puede configurar un grupo de CloudWatch registros para un registro de la organización mediante la consola. El administrador delegado puede configurar un grupo de CloudWatch registros mediante las operaciones de la `UpdateTrail` API AWS CLI CloudTrail `CreateTrail` o o.

5. En Tags (Etiquetas), elija Edit (Editar) para cambiar, agregar o eliminar etiquetas en el registro de seguimiento. Agregue una o más etiquetas personalizadas (pares de valor de clave) a su registro de seguimiento. Las etiquetas pueden ayudarle a identificar tanto sus CloudTrail senderos como los depósitos de Amazon S3 que contienen archivos de CloudTrail registro. A continuación, puede utilizar grupos de recursos para sus CloudTrail recursos. Para más información, consulte AWS Resource Groups y ¿Por qué usar etiquetas para CloudTrail los recursos?.

6. En Management events (Eventos de administración), elija Edit (Editar) para cambiar la configuración de registro de eventos de administración.

   a. En API activity (Actividad de la API), elija si desea que su registro de seguimiento registre eventos de Read (Lectura), Write (Escritura) o ambos. Para obtener más información, consulte Eventos de administración.

   b. Elige Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) los eventos de tu ruta. La configuración predeterminada es incluir a todos los eventos de AWS KMS .

      La opción de registrar o excluir AWS KMS eventos solo está disponible si registras los eventos de administración en tu ruta. Si elige no registrar los eventos de administración, los AWS KMS eventos no se registran y no puede cambiar la configuración AWS KMS del registro de eventos.

      AWS KMS acciones como `EncryptDecrypt`, y `GenerateDataKey` suelen generar un gran volumen (más del 99%) de eventos. Estas acciones se registran ahora como eventos de lectura. AWS KMS Las acciones relevantes de bajo volumen, como `DisableDelete`, y `ScheduleKey` (que normalmente representan menos del 0,5% del volumen de AWS KMS eventos) se registran como eventos de escritura.

      Para excluir eventos de gran volumen como `Encrypt`, `Decrypt` y `GenerateDataKey`, y seguir registrando eventos relevantes como `Disable`, `Delete` y `ScheduleKey`, elija registrar eventos de administración Write (Escritura) y desmarque la casilla de verificación Exclude AWS KMS events (Excluir eventos de KMS).

   c. Elija Exclude Amazon RDS Data API events (Excluir eventos de API de datos de Amazon RDS) para quitar del registro de seguimiento los eventos de API de datos de Amazon Relational Database Service. La configuración predeterminada es incluir a todos los eventos de la API de datos de Amazon RDS. A fin de obtener más información sobre los eventos de API de datos de Amazon RDS, consulte Registro de llamadas a la API de datos con AWS CloudTrail en la Guía del usuario de Amazon RDS para Aurora.

7.

> **Important**
>
> Los pasos del 7 al 11 son para configurar los eventos de datos mediante selectores de eventos avanzados. Los selectores de eventos avanzados le permiten configurar más tipos de eventos de datos y ofrecen un control detallado de los eventos de datos que captura su registro de seguimiento. Si utiliza selectores de eventos básicos, consulte

Actualización de la configuración de eventos de datos con selectores de eventos básicos y, a continuación, vuelva al paso 12 de este procedimiento.

En Data events (Eventos de datos), elija Edit (Editar) para cambiar la configuración de registro de eventos de datos. De forma predeterminada, los registros de seguimiento no registran eventos de datos. Se aplican cargos adicionales para registrar eventos de datos. Para obtener información acerca de los precios de CloudTrail, consulte Precios de AWS CloudTrail.

En Data event type (Tipo de evento de datos), elija el tipo de recurso en el que desea registrar los eventos de datos. Para obtener más información sobre los tipos de eventos de datos disponibles, consulte Eventos de datos.

> **Note**
>
> Para registrar los eventos de datos de AWS Glue las tablas creadas por Lake Formation, elija Lake Formation.

8. Elija una plantilla de selección de registros. CloudTrail incluye plantillas predefinidas que registran todos los eventos de datos del tipo de recurso. Para crear una plantilla de selector de registros personalizada, elija Custom (Personalizado).

> **Note**
>
> Si eliges una plantilla predefinida para los depósitos de S3, podrás registrar los eventos de datos de todos los depósitos que hay actualmente en tu AWS cuenta y de los que crees una vez que hayas terminado de crear el registro. También permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
> Si el registro de seguimiento solo aplica a una región, elegir una plantilla predefinida que registra todos los buckets de S3 permite el registro de eventos de datos de todos los buckets en la misma región que el registro de seguimiento, así como de cualquier otro bucket que cree posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de la cuenta de AWS .
> Si va a crear un registro para todas las regiones, al elegir una plantilla predefinida para las funciones de Lambda se habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en su AWS cuenta y para cualquier función de Lambda que pueda crear en cualquier región una vez que haya terminado

de crear el registro. Si va a crear una ruta para una sola región (mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
El registro de los eventos de datos para todas las funciones también permite registrar la actividad de los eventos de datos realizada por cualquier usuario o función de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

9. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo opcional para un selector de eventos avanzado, como “Registrar eventos de datos para solo dos buckets de S3”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
10. En Advanced event selectors (Selectores de eventos avanzados), cree una expresión para los recursos específicos en los que desea recopilar eventos de datos. Puede omitir este paso si utiliza una plantilla de registro predefinida.

    a. Elija uno de los siguientes campos.

    - **`readOnly`**- se `readOnly` puede configurar para que sea igual a un valor de `true` o`false`. Para registrar eventos `read` y `write`, no agregue un selector de `readOnly`.
    - **`eventName`**: `eventName` puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de datos registrado CloudTrail, como `PutBucket` o`GetSnapshotBlock`.
    - **`resources.ARN`**- Puede usar cualquier operador con`resources.ARN`, pero si usa valores iguales o no iguales, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo que especificó en la plantilla como valor de. `resources.type`

      En la siguiente tabla, se muestra el formato de ARN de cada `resources.type`.

      > **Note**
      >
      > No puede usar el `resources.ARN` campo para filtrar los tipos de recursos que no tienen ARN.

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*

resources.type	resources.ARN
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*

resources.type	resources.ARN
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_c omponent_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemake r: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_I D* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespac e/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_I D*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_I D* :endpoint/ *endpoint_type* /*endpoint_ name* /*endpoint_ID*

resources.type	resources.ARN
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	El ARN debe estar en uno de los siguientes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir los eventos de streaming, añade un filtro en el `eventName` campo.

[2] Para registrar todos los eventos de datos de todos los objetos en un bucket de S3 específico, utilice el operador `StartsWith` e incluya solo el ARN del bucket como valor coincidente. La barra diagonal final es intencional; no la excluya.

[3] Para registrar eventos en todos los objetos de un punto de acceso de S3, se recomienda que utilice solo el ARN del punto de acceso. No incluya la ruta de acceso del objeto y utilice los operadores `StartsWith` o `NotStartsWith`.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte Acciones, recursos y claves de condición en la Guía del usuario de AWS Identity and Access Management .

b. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones. Por ejemplo, para excluir los eventos de datos de dos cubos de S3 de los eventos de datos que se registran en su ruta, puede establecer el campo en Resources.ARN, configurar el operador

para no comienza por y, a continuación, pegar el ARN de un depósito de S3 o buscar los cubos de S3 para los que no desea registrar eventos.

Para agregar el segundo bucket de S3, seleccione + Condición y, a continuación, repita la instrucción anterior, pegue el ARN o busque un bucket diferente.

> **Note**
>
> Puede tener un máximo de 500 valores para todos los selectores de un registro de seguimiento. Esto incluye matrices de varios valores para un selector como `eventName`. Si tiene valores únicos para todos los selectores, puede agregar un máximo de 500 condiciones a un selector.
> Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Puede registrar todas las funciones con una plantilla de selector predefinida, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear la ruta en la consola y, a continuación, utilizar el put-event-selectors comando AWS CLI and the para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Administrar senderos con el AWS CLI.

c. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos. Por ejemplo, no especifique un ARN en un selector para que sea igual a un valor y luego especifique que el ARN no sea igual al mismo valor en otro selector.

11. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos). Repita los pasos, desde el número 3 a este paso, a fin de configurar selectores de eventos avanzados para el tipo de evento de datos.
12. En los eventos de Insights, elija Editar si desea que su registro registre los eventos de CloudTrail Insights.

    En Event type (Tipo de evento), seleccione Insights events (Eventos de Insights).

    En Insights events (Eventos de Insights), elija API call rate (Tasa de llamada a la API), API error rate (Tasa de errores de API), o ambos. Debe registrar los eventos de administración de escritura para registrar los eventos de Insights para calcular la tasa de llamadas a la API.

Debe registrar los eventos de administración de lectura o escritura para registrar los eventos de Insights para calcular la tasa de errores de la API.

CloudTrail Insights analiza los eventos de administración para detectar actividades inusuales y los registra cuando se detectan anomalías. De forma predeterminada, los registros de seguimiento no registran eventos de Insights. Para obtener más información acerca de los eventos de Insights, consulte Registro de eventos de Insights. Se aplican cargos adicionales por registrar eventos de Insights. Para CloudTrail conocer los precios, consulte AWS CloudTrail Precios.

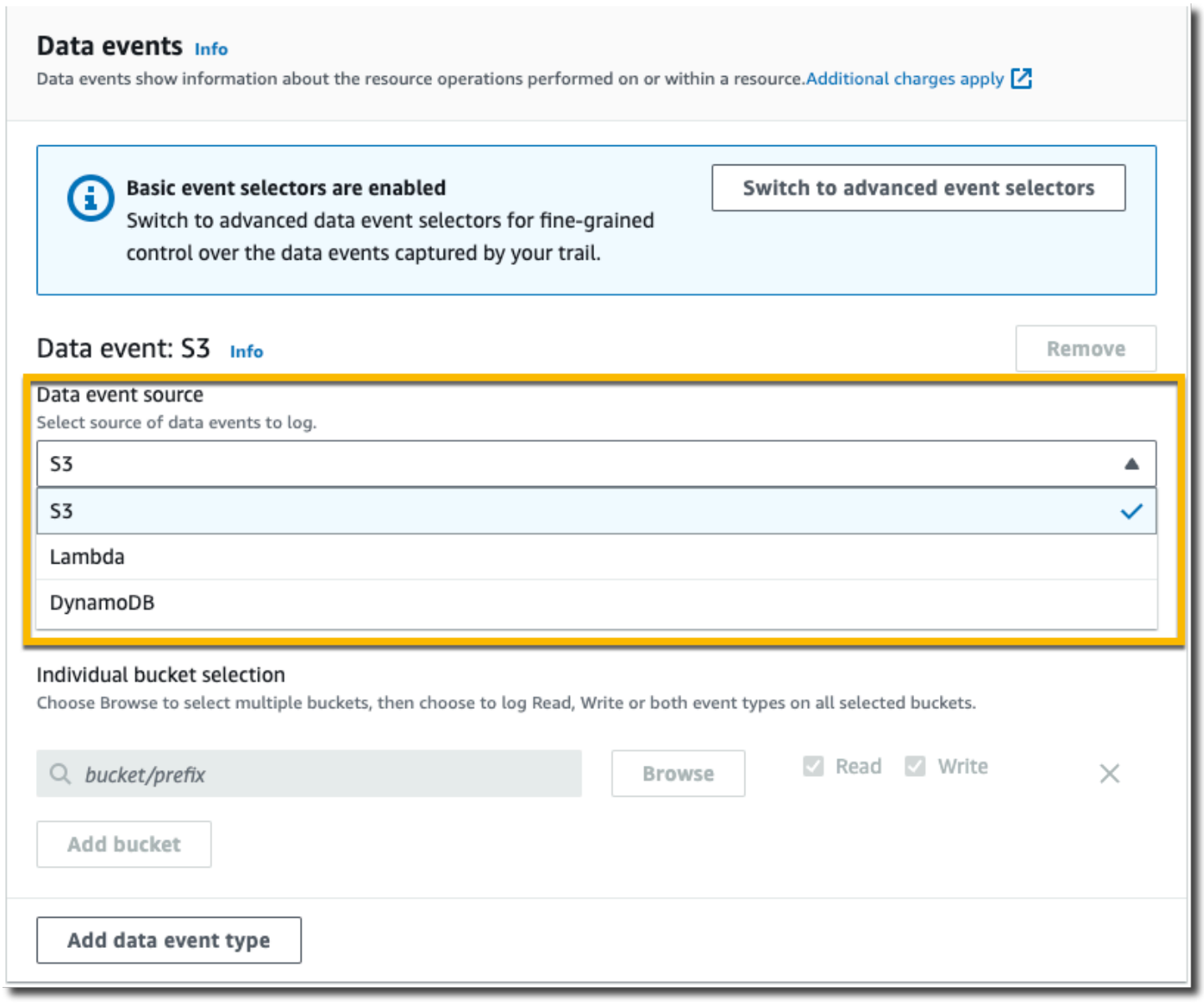
Los eventos de Insights se envían a una carpeta diferente con el nombre `/CloudTrail-Insight` del mismo depósito de S3 que se especifica en el área de ubicación de almacenamiento de la página de detalles de la ruta. CloudTrailcrea el nuevo prefijo para usted. Por ejemplo, si el bucket de S3 de destino actual se denomina `S3bucketName/AWSLogs/CloudTrail/`, el nombre del bucket de S3 con un nuevo prefijo se denomina `S3bucketName/AWSLogs/CloudTrail-Insight/`.

13. Cuando haya terminado de cambiar la configuración de su registro de seguimiento, elija Update trail (Actualizar registro de seguimiento).

Actualización de la configuración de eventos de datos con selectores de eventos básicos

Puede utilizar selectores de eventos avanzados para configurar todos los tipos de eventos de datos. Los selectores de eventos avanzados le permiten crear selectores detallados para registrar solo los eventos de interés.

Si utiliza selectores de eventos básicos para registrar eventos de datos, está limitado a registrar eventos de datos para buckets, AWS Lambda funciones y tablas de Amazon DynamoDB de Amazon S3. No puede filtrar el `eventName` campo con selectores de eventos básicos.



Use el procedimiento siguiente para configurar los ajustes de eventos de datos mediante selectores de eventos básicos.

1. En Data events (Eventos de datos), elija Edit (Editar) para cambiar la configuración de registro de eventos de datos. Con los selectores de eventos básicos, puede especificar eventos de datos de registro para buckets, AWS Lambda funciones, DynamoDBTables de Amazon S3 o una combinación de esos recursos. Se admiten tipos de eventos de datos adicionales con selectores de eventos avanzados. De forma predeterminada, los registros de seguimiento no registran eventos de datos. Se aplican cargos adicionales para registrar eventos de datos. Para obtener más información, consulte Eventos de datos. Para obtener información acerca de los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Para buckets de Amazon S3:

a. En Data event source (Fuente de evento de datos), elija S3.

b. Puede registrar All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) o bien, especificar buckets o funciones individuales. De forma predeterminada, los eventos de datos se registran para todos los buckets de S3 actuales y futuros.

> **Note**
>
> Si mantiene la opción predeterminada Todos los depósitos de S3 actuales y futuros, se permite registrar los eventos de datos de todos los depósitos que se encuentren actualmente en su AWS cuenta y de todos los depósitos que cree una vez que haya terminado de crear la ruta. También permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
> Si el registro de seguimiento solo aplica a una región, elegir All current and future S3 buckets (Todos los buckets de S3 actuales o futuros) permite el registro de eventos de datos de todos los buckets en la misma región que el registro de seguimiento, así como de cualquier otro bucket que cree posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de su AWS cuenta.

c. Si conserva la opción predeterminada, All current and future S3 buckets (Todos los buckets de S3 actuales y futuros), elija registrar eventos de Read (Lectura), Write (Escritura) o ambos.

d. Para seleccionar buckets individuales, desmarque las casillas de verificación Read (Lectura) y Write (Escritura) en All current and future S3 buckets (Todos los buckets de S3 actuales y futuros). En Individual bucket selection (Selección de bucket individual), busque un bucket en el que registrar los eventos de datos. Para buscar buckets específicos, escriba un prefijo de bucket para el bucket que desee. En esta ventana puede seleccionar varios buckets. Elija Add bucket (Agregar bucket) para registrar eventos de datos en más buckets. Elija registrar eventos de Read (Lectura), como `GetObject`, Write (Escritura), como `PutObject`, o de ambos.

   Esta configuración tiene prioridad sobre la configuración individual de cada bucket. Por ejemplo, si establece la configuración para que se registren los eventos de tipo Read de todos los buckets de S3 y posteriormente decide agregar un determinado bucket en el

registro de eventos de datos, la opción Read ya aparecerá seleccionada en el bucket que agregue. Esta selección no se puede anular. Solo se puede configurar la opción Write.

Para eliminar un bucket del registro, elija X.

2. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos).
3. Para funciones Lambda:

   a. En Data event source (Fuente de evento de datos), elija Lambda.

   b. En Lambda function (Función Lambda), elija All regions (Todas las regiones) para registrar todas las funciones Lambda, o Input function as ARN (Función de entrada como ARN) a fin de registrar eventos de datos en una función específica.

   Para registrar los eventos de datos de todas las funciones de Lambda de su AWS cuenta, seleccione Registrar todas las funciones actuales y futuras. Esta configuración tiene prioridad sobre la configuración individual de cada función. Se registran todas las funciones aunque no se muestren.

   > **Note**
   >
   > Si va a crear una ruta para todas las regiones, esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en su AWS cuenta y para cualquier función de Lambda que pueda crear en cualquier región una vez que haya terminado de crear la ruta. Si va a crear una ruta para una sola región (mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
   > El registro de los eventos de datos para todas las funciones también permite registrar la actividad de los eventos de datos realizada por cualquier usuario o función de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

   c. Si elige Input function as ARN (Función de entrada como ARN), ingrese el ARN de una función Lambda.

> **Note**
>
> Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Sí que puede seleccionar la opción para registrar todas las funciones, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede finalizar la creación del registro de seguimiento en la consola y, a continuación, utilizar la AWS CLI y el comando put-event-selectors a fin de configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Administrar senderos con el AWS CLI.

4. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos).
5. Para tablas de DynamoDB:

   a. En Data event source (Fuente de evento de datos), elija DynamoDB.

   b. En DynamoDB table selection (Selección de tabla de DynamoDB), elija Browse (Examinar) para seleccionar una tabla o pegue el ARN de una tabla de DynamoDB a la que tenga acceso. El ARN de la tabla de DynamoDB tiene el siguiente formato:

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   Para agregar otra tabla, elija Add row (Agregar fila) y busque una tabla o pegue el ARN de una tabla a la que tenga acceso.
6. A fin de configurar eventos de Insights y otras configuraciones para su registro de seguimiento, vuelva al procedimiento anterior en este tema, Actualización de un registro de seguimiento.

Eliminación de un registro de seguimiento

Puede eliminar registros de seguimiento con la consola de CloudTrail. Si la cuenta de administración o la cuenta del administrador delegado de una organización elimina un registro de seguimiento de organización, el registro se elimina de todas las cuentas miembro de la organización.

Si ha activado los eventos de administración de CloudTrail en Amazon Security Lake, debe mantener al menos un registro de seguimiento de la organización que sea de varias regiones y que registre

tanto los eventos de administración de `read` como de `write`. No puede eliminar un registro de seguimiento si es el único que tiene que cumpla este requisito, a menos que desactive los eventos de administración de CloudTrail en Security Lake.

Para eliminar registros de seguimiento con la consola de CloudTrail.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. Abra la página Trails (Registros de seguimiento) de la consola de CloudTrail.
3. Elija el nombre del registro de seguimiento.
4. En la parte superior de la página de detalles del registro de seguimiento, elija Delete (Eliminar).
5. Cuando se le pida confirmación, elija Delete (Eliminar) para eliminar el registro de seguimiento de forma permanente. El registro de seguimiento se elimina de la lista de registros de seguimiento. Los archivos de registros que ya se hayan entregado al bucket de Amazon S3 no se eliminarán.

> **Note**
>
> El contenido entregado a los buckets de Amazon S3 puede contener contenido del cliente. Para obtener más información sobre la eliminación de información confidencial, consulte ¿Cómo puedo vaciar un bucket de S3? o ¿Cómo elimino un bucket de S3?.

Desactivación del registro de un registro de seguimiento

Cuando crea un registro de seguimiento, el registro está activado de forma automática. Puede desactivar el registro de un registro de seguimiento.

Al desactivar el registro, los registros existentes todavía se almacenan en el bucket de Amazon S3 del registro de seguimiento y sigue generando cargos de S3.

Para desactivar el registro de un registro de seguimiento con la consola de CloudTrail.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, elija Trails (Registros de seguimiento) y, a continuación, elija el nombre del registro de seguimiento.

3. En la parte superior de la página de detalles del registro de seguimiento, elija Stop logging (Detener registro) para desactivar el registro del registro de seguimiento.
4. Cuando se le pida confirmación, elija Stop logging (Detener registro). CloudTrail detiene la actividad de registro de ese registro de seguimiento.
5. Para reanudar el registro de dicho registro de seguimiento, elija Start logging (Comenzar registro) en la página de configuración del registro de seguimiento.

Creación, actualización y gestión de senderos con AWS Command Line Interface

Puedes usar el AWS CLI para crear, actualizar y administrar tus senderos. Cuando utilices el AWS CLI, recuerda que tus comandos se ejecutan en la AWS región configurada para tu perfil. Si desea ejecutar los comandos en otra región, cambie la región predeterminada de su perfil o utilice el parámetro --region con el comando.

> **Note**
>
> Necesita las herramientas de línea de AWS comandos para ejecutar los comandos AWS Command Line Interface (AWS CLI) de este tema. Asegúrese de tener AWS CLI instalada una versión reciente del. Para más información, consulte la Guía del usuario de AWS Command Line Interface. Para obtener ayuda con CloudTrail los comandos de la línea de AWS CLI comandos, escribaaws cloudtrail help.

Comandos de uso frecuente para la creación, la administración y el estado de los registros de seguimiento

Algunos de los comandos más utilizados para crear y actualizar rutas CloudTrail incluyen:

- create-trail para crear un registro de seguimiento.
- update-trail para cambiar la configuración de un registro de seguimiento existente.
- add-tags para añadir una o varias etiquetas (pares clave-valor) a un registro de seguimiento existente.
- remove-tags para quitar una o varias etiquetas de un registro de seguimiento.
- list-tags para devolver la lista de etiquetas asociadas a un registro de seguimiento.

- put-event-selectors para añadir o modificar selectores de eventos para un registro de seguimiento.
- put-insight-selectors para añadir o modificar selectores de eventos de Insights para un registro de seguimiento existente, y habilitar o deshabilitar eventos de Insights.
- start-logging para comenzar a registrar eventos con un registro de seguimiento.
- stop-logging poner en pausa el registro de eventos con el registro de seguimiento.
- delete-trail para eliminar un registro de seguimiento. Este comando no elimina el bucket de Amazon S3 que contiene los archivos de registros de dicho registro de seguimiento, si lo hay.
- describe-trailspara devolver información sobre los senderos de una AWS región.
- get-trail para devolver la información de configuración de un registro de seguimiento.
- get-trail-status para devolver información sobre el estado actual de un registro de seguimiento.
- get-event-selectors para devolver información sobre los selectores de eventos configurados para un registro de seguimiento.
- get-insight-selectors para devolver información sobre los selectores de eventos de Insights configurados para un registro de seguimiento.

Comandos admitidos para crear y actualizar registros de seguimiento: create-trail y update-trail

Los comandos `create-trail` y `update-trail` ofrecen diversas funciones para la creación y administración de registros de seguimiento, entre las que se incluyen:

- Crear un registro de seguimiento que reciba archivos de registro de distintas regiones o actualizar un registro de seguimiento con la opción `--is-multi-region-trail`. En la mayoría de los casos, debes crear senderos que registren los eventos en todas AWS las regiones.
- Crear un registro que reciba los registros de todas AWS las cuentas de una organización con la --is-organization-trail opción.
- Convertir un registro de seguimiento de varias regiones en un registro de seguimiento de una sola región con la opción `--no-is-multi-region-trail`.
- Habilitar o deshabilitar el cifrado de archivos de registro con la opción `--kms-key-id`. La opción especifica una AWS KMS clave que ya ha creado y a la que ha adjuntado una política que CloudTrail permite cifrar sus registros. Para obtener más información, consulte Habilitar y deshabilitar el cifrado de archivos de registros de CloudTrail con la AWS CLI.
- Habilitar o deshabilitar la validación de archivos de registro con las opciones `--enable-log-file-validation` y `--no-enable-log-file-validation`. Para obtener más información, consulte Validar la integridad de los archivos de registros de CloudTrail.

- Especificar un grupo y un rol de CloudWatch registros para CloudTrail poder entregar eventos a un grupo de CloudWatch registros. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Comandos obsoletos: create-subscription y update-subscription

> **Important**
>
> Los comandos `create-subscription` y `update-subscription` se usaban para crear y actualizar registros de seguimiento, pero ya no están disponibles. No utilice estos comandos. No proporcionan funcionalidad completa para la creación y administración de registros de seguimiento.
> Si ha configurado una automatización que utilice uno de estos comandos o ambos, le recomendamos que actualice el código o los scripts para que utilicen los comandos admitidos, como create-trail.

Uso de create-trail

Puede ejecutar el comando `create-trail` para crear registros de seguimiento configurados específicamente a fin de satisfacer sus necesidades empresariales. Cuando utilice el AWS CLI, recuerde que sus comandos se ejecutan en la AWS región configurada para su perfil. Si desea ejecutar los comandos en otra región, cambie la región predeterminada de su perfil o utilice el parámetro --region con el comando.

Creación de un registro de seguimiento que se aplique a todas las regiones

Para crear un registro de seguimiento que se aplique a todas las regiones, utilice la opción `--is-multi-region-trail`. De forma predeterminada, el comando `create-trail` crea un registro de seguimiento que registra los eventos únicamente en la región de AWS donde se creó el registro de seguimiento. Para asegurarte de registrar los eventos de servicio globales y registrar toda la actividad de los eventos de gestión en tu AWS cuenta, debes crear rutas que registren los eventos en todas AWS las regiones.

> **Note**
>
> Al crear una ruta, si especificas un bucket de Amazon S3 con el que no se creó CloudTrail, tendrás que adjuntar la política correspondiente. Consulte Política de bucket de Amazon S3 para CloudTrail.

En el siguiente ejemplo, se crea un registro de seguimiento denominado *my-trail* y una etiqueta con una clave denominada *Group* con el valor *Marketing* que envía los archivos de registro de todas las regiones a un bucket existente denominado *my-bucket*.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --tags-list [key=Group,value=Marketing]
```

Para confirmar que el registro de seguimiento existe en todas las regiones, el elemento `IsMultiRegionTrail` del resultado muestra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Utilice el comando `start-logging` para empezar a ejecutar el registro de seguimiento.

Iniciar el registro de seguimiento

Cuando el comando `create-trail` termine de ejecutarse, ejecute el comando `start-logging` para empezar a ejecutar ese registro de seguimiento.

> **Note**
>
> Al crear un rastro con la CloudTrail consola, el registro se activa automáticamente.

En el ejemplo siguiente, se inicia el registro para un registro de seguimiento.

```
aws cloudtrail start-logging --name my-trail
```

Este comando no devuelve ningún resultado, pero puede utilizar el comando `get-trail-status` para verificar que ha comenzado el registro.

```
aws cloudtrail get-trail-status --name my-trail
```

Para confirmar que el registro de seguimiento está funcionando, el elemento `IsLogging` del resultado muestra `true`.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Crear un registro de seguimiento para una sola región

El siguiente comando crea un registro de seguimiento para una única región. El bucket de Amazon S3 especificado debe existir ya y tener los CloudTrail permisos correspondientes aplicados. Para obtener más información, consulte Política de bucket de Amazon S3 para CloudTrail.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

Para obtener más información, consulte Requisitos de nomenclatura.

A continuación, se muestra un ejemplo del resultado.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Creación de un registro de seguimiento que se aplica a todas las regiones y que tiene activada la validación de archivos de registro

Para habilitar la validación de archivos de registro cuando se utiliza `create-trail`, use la opción `--enable-log-file-validation`.

Para obtener información sobre la validación de archivos de registro, consulte Validar la integridad de los archivos de registros de CloudTrail.

El ejemplo siguiente crea un registro de seguimiento que envía los archivos de registro de todas las regiones al bucket especificado. El comando utiliza la opción `--enable-log-file-validation`.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --enable-log-file-validation
```

Para confirmar que la validación de archivos de registro está activada, el elemento `LogFileValidationEnabled` del resultado muestra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Uso de update-trail

> **Important**
>
> A partir del 22 de noviembre de 2021, se AWS CloudTrail modificó la forma en que los senderos capturan los eventos de servicio globales. Ahora, los eventos creados por Amazon CloudFront AWS STS se registran en la región en la que se crearon, la región de EE. UU. Este (Virginia del Norte), us-east-1. AWS Identity and Access Management Esto hace que la forma en que se CloudTrail tratan estos servicios sea coherente con la de otros servicios AWS globales. Para continuar recibiendo eventos de servicios globales fuera de Este de EE. UU. (Norte de Virginia), asegúrese de convertir los registros de seguimiento de una sola región con el uso de eventos de servicio globales fuera de Este de EE. UU. (Norte de Virginia) en los registros de seguimiento de varias regiones. Para obtener más información acerca de la captura de eventos de servicios globales, consulte Habilitación y desactivación del registro de eventos de servicios globales más adelante en esta sección.
> Por el contrario, el historial de eventos de la CloudTrail consola y el aws cloudtrail lookup-events comando mostrarán estos eventos en el lugar Región de AWS donde ocurrieron.

Puede utilizar el comando `update-trail` para cambiar las opciones de configuración de un registro de seguimiento. También puede utilizar los comandos add-tags y remove-tags para añadir y eliminar etiquetas para un registro de seguimiento. Solo puedes actualizar las rutas de la AWS región en la que se creó la ruta (su región de origen). Cuando utilices el AWS CLI, recuerda que tus comandos se ejecutan en la AWS región configurada para tu perfil. Si desea ejecutar los comandos en otra región, cambie la región predeterminada de su perfil o utilice el parámetro --region con el comando.

Si ha habilitado los eventos CloudTrail de administración en Amazon Security Lake, debe mantener al menos un registro organizativo que sea multirregional y registre tanto `read` los eventos de administración como los eventos `write` de administración. No puede actualizar un registro de seguimiento válido de forma que no cumpla con el requisito de Security Lake. Por ejemplo, si cambia el registro de seguimiento a uno de una sola región o desactiva el registro de los eventos de administración de `read` o `write`.

> **Note**
>
> Si utiliza uno de los AWS SDK AWS CLI o uno de ellos para modificar una ruta, asegúrese de que la política de segmentos de la ruta lo sea. up-to-date Para que tu bucket reciba automáticamente los eventos de un nuevo segmento Región de AWS, la política debe

incluir el nombre completo del servicio,`cloudtrail.amazonaws.com`. Para obtener más información, consulte Política de bucket de Amazon S3 para CloudTrail.

Temas

- Conversión de un registro de seguimiento que se aplica a una sola región en uno que se aplique a todas las regiones
- Conversión de un registro de seguimiento de varias regiones en un registro de seguimiento de una sola región
- Habilitación y desactivación del registro de eventos de servicios globales
- Habilitación de la validación de archivos de registro
- Desactivar la validación de archivos de registro

Conversión de un registro de seguimiento que se aplica a una sola región en uno que se aplique a todas las regiones

Para cambiar un registro de seguimiento existente de forma que se aplique a todas las regiones, utilice la opción `--is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Para confirmar que el registro de seguimiento se aplica ahora a todas las regiones, el elemento `IsMultiRegionTrail` del resultado muestra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Conversión de un registro de seguimiento de varias regiones en un registro de seguimiento de una sola región

Para cambiar un registro de seguimiento de varias regiones de forma que se aplique solamente a la región en la que se creó, utilice la opción `--no-is-multi-region-trail`.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

Para confirmar que el registro de seguimiento se aplica ahora a una sola región, el elemento `IsMultiRegionTrail` del resultado muestra `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Habilitación y desactivación del registro de eventos de servicios globales

Para cambiar un registro de seguimiento de forma que no registre eventos de servicios globales, utilice la opción `--no-include-global-service-events`.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

Para confirmar que el registro de seguimiento ya no registra eventos de servicios globales, el elemento `IncludeGlobalServiceEvents` del resultado muestra `false`.

```
{
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Para cambiar un registro de seguimiento de forma que registre eventos de servicios globales, utilice la opción `--include-global-service-events`.

Los registros de seguimiento de una región ya no recibirán eventos de servicios globales a partir del 22 de noviembre de 2021, a menos que estos aparezcan en la región Este de EE. UU. (Norte de Virginia), us-east-1. Para continuar con la captura de eventos de servicios globales, actualice la configuración de registros de seguimiento a uno de varias regiones. Por ejemplo, este comando actualiza un registro de seguimiento para una sola región en Este de EE. UU. (Ohio), us-east-2, en un registro de seguimiento de varias regiones. Sustituya *myExistingSingleRegionTrailWithGSE* por el nombre de ruta adecuado para su configuración.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

Dado que los eventos de servicios globales solo están disponibles en Este de EE. UU. (Norte de Virginia) a partir del 22 de noviembre de 2021, también puede crear un registro de seguimiento de una región para suscribirse a eventos de servicios globales en la región Este de EE. UU. (Norte de Virginia), us-east-1. El siguiente comando crea un rastro de una sola región en us-east-1 para recibir CloudFront, realizar IAM y eventos: AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

Habilitación de la validación de archivos de registro

Para activar la validación de archivos de registro para un registro de seguimiento, utilice la opción `--enable-log-file-validation`. Los archivos de resumen se envían al bucket de Amazon S3 para dicho registro de seguimiento.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

Para confirmar que la validación de archivos de registro está activada, el elemento `LogFileValidationEnabled` del resultado muestra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
```

```
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Desactivar la validación de archivos de registro

Para desactivar la validación de archivos de registro para un registro de seguimiento, utilice la opción `--no-enable-log-file-validation`.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

Para confirmar que la validación de archivos de registro está desactivada, el elemento `LogFileValidationEnabled` del resultado muestra `false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Para validar los archivos de registro con el, consulte. AWS CLIValidación de la integridad de los archivos de registros de CloudTrail con la AWS CLI

Administrar senderos con el AWS CLI

AWS CLI Incluye varios otros comandos que te ayudan a gestionar tus senderos. Estos comandos permiten agregar etiquetas a los registros de seguimiento, obtener su estado, iniciar y detener el registro en ellos y eliminarlos. Debes ejecutar estos comandos desde la misma AWS región en la que se creó el sendero (su región de origen). Cuando utilices el AWS CLI, recuerda que tus comandos se ejecutan en la AWS región configurada para tu perfil. Si desea ejecutar los comandos en otra región, cambie la región predeterminada de su perfil o utilice el parámetro --region con el comando.

Temas

- Adición de una o varias etiquetas a un registro de seguimiento
- Listado de las etiquetas de uno o varios registros de seguimiento
- Eliminación de una o varias etiquetas de un registro de seguimiento
- Recuperación de la configuración de registros de seguimiento y del estado de un registro de seguimiento
- Configuración de los selectores de eventos de CloudTrail Insights
- Configuración de selectores de eventos
- Configuración de selectores de eventos avanzados
- Detención e inicio del registro de un registro de seguimiento
- Eliminación de un registro de seguimiento

Adición de una o varias etiquetas a un registro de seguimiento

Para agregar una o varias etiquetas a un registro de seguimiento existente, ejecute el comando add-tags.

En el siguiente ejemplo, se agrega una etiqueta denominada *Owner* (Propietario) con el valor *Mary* a una registro de seguimiento con el ARN *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* en la región Este de EE. UU. (Ohio).

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

Si se ejecuta correctamente, este comando no devuelve nada.

Listado de las etiquetas de uno o varios registros de seguimiento

Para ver las etiquetas asociadas a uno o varios registros de seguimiento existentes, utilice el comando list-tags.

En el ejemplo siguiente, se muestran las etiquetas de *Trail1* y *Trail2*.

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

Si se ejecuta correctamente, este comando proporciona información similar a la siguiente.

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "Name"
             },
             {
                 "Value": "Ohio",
                 "Key": "Location"
             }
         ]
     },
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
         "TagsList": [
             {
                 "Value": "Bob",
                 "Key": "Name"
             }
         ]
     }
  ]
}
```

Eliminación de una o varias etiquetas de un registro de seguimiento

Para eliminar una o varias etiquetas de un registro de seguimiento existente, ejecute el comando remove-tags.

En el siguiente ejemplo, se eliminan las etiquetas denominadas *Location* (Ubicación) y *Name* (Nombre) de un registro de seguimiento con el ARN *arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1* en la región Este de EE. UU. (Ohio).

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

Si se ejecuta correctamente, este comando no devuelve nada.

Recuperación de la configuración de registros de seguimiento y del estado de un registro de seguimiento

Ejecute el `describe-trails` comando para recuperar información sobre los senderos de una AWS región. En el siguiente ejemplo, se devuelve información sobre los registros de seguimiento configurados en la región EE. UU. Este (Ohio).

```
aws cloudtrail describe-trails --region us-east-2
```

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
```

```
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
    }
  ]
}
```

Ejecute el comando `get-trail` para recuperar información de configuración sobre un registro de seguimiento específico. En el ejemplo siguiente se devuelve la información de configuración de un registro de seguimiento denominado *my-trail*.

```
aws cloudtrail get-trail - -name my-trail
```

Si se ejecuta correctamente, este comando proporciona información similar a la siguiente.

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

Ejecute el comando `get-trail-status` para recuperar el estado de un registro de seguimiento. Debe ejecutar este comando desde la AWS región en la que se creó (la región de origen) o debe especificar esa región añadiendo el --region parámetro.

> **Note**
>
> Si el sendero es un sendero de una organización y usted es miembro de la cuenta de la organización en AWS Organizations, debe proporcionar el ARN completo de ese sendero y no solo el nombre.

```
aws cloudtrail get-trail-status --name my-trail
```

Si el comando se ejecuta correctamente, verá un resultado similar al siguiente.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Además de los campos que se muestran en el código JSON anterior, el estado contiene los siguientes campos si hay errores de Amazon SNS o Amazon S3:

- `LatestNotificationError`. Contiene el error emitido por Amazon SNS si se produce un error en una suscripción a un tema.
- `LatestDeliveryError`. Contiene el error emitido por Amazon S3 si CloudTrail no puede entregar un archivo de registro a un bucket.

Configuración de los selectores de eventos de CloudTrail Insights

Habilite los eventos de Insights en una traza ejecutando put-insight-selectors y especificando `ApiCallRateInsight`, `ApiErrorRateInsight` como valor del atributo `InsightType`. Para ver la configuración de los selectores de Insights de un registro de seguimiento, ejecute el comando `get-insight-selectors`. Debe ejecutar este comando desde la AWS región en la que se creó la ruta (la región de origen) o debe especificar esa región añadiendo el --region parámetro al comando.

> **Note**
>
> Para registrar los eventos de Insights para `ApiCallRateInsight`, el registro de seguimiento debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights para `ApiErrorRateInsight`, el registro de seguimiento debe registrar los eventos de administración de `read` o `write`.

Ejemplo de registro de seguimiento que registra eventos de Insights

En el siguiente ejemplo, se utiliza put-insight-selectors la creación de un selector de eventos de Insights para una ruta denominada *`TrailName3`*. Esto permite la recopilación de eventos de Insights para los *`TrailNametres`* senderos. El selector de eventos de Insights registra ambos `ApiErrorRateInsight` y `ApiCallRateInsight` tipos de eventos de Insights.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

El ejemplo devuelve el selector de eventos de Insights configurado para el registro de seguimiento.

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Ejemplo: Desactivar la recopilación de eventos de Insights

En el siguiente ejemplo, put-insight-selectors se utiliza para eliminar el selector de eventos de Insights de una ruta denominada *`TrailName3`*. Al borrar la cadena JSON de los selectores de Insights, se deshabilita la recopilación de eventos de Insights para las *`TrailNametres`* rutas.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

El ejemplo devuelve el selector de eventos de Insights ahora vacío que está configurado para el registro de seguimiento.

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Configuración de selectores de eventos

Para ver la configuración de los selectores de eventos de un registro de seguimiento, ejecute el comando `get-event-selectors`. Debe ejecutar este comando desde la AWS región en la que se creó (la región de origen) o debe especificar esa región mediante el --region parámetro.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Si el sendero es un sendero de una organización y usted es miembro de la cuenta de la organización en AWS Organizations, debe proporcionar el ARN completo de ese sendero y no solo el nombre.

El ejemplo siguiente devuelve la configuración predeterminada de un selector de eventos de un registro de seguimiento.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para crear un selector de eventos, ejecute el comando `put-event-selectors`. Si desea registrar los eventos de Insights en el registro de seguimiento, asegúrese de que el selector de eventos

permita registrar los tipos de Insights que desea configurar para el registro de seguimiento. Para obtener más información sobre cómo registrar los eventos de Insights, consulte Registro de eventos de Insights.

Cuando se produce un evento en tu cuenta, CloudTrail evalúa la configuración de tus senderos. Si el evento coincide con algún selector de eventos de un registro de seguimiento, se procesa el registro de seguimiento y se registra el evento. Puede configurar hasta cinco selectores de eventos para un registro de seguimiento y hasta 250 recursos de datos para un registro de seguimiento. Para obtener más información, consulte Registro de eventos de datos.

Temas

- Ejemplo de registro de seguimiento con selectores de eventos específicos
- Ejemplo de registro de seguimiento que registra todos los eventos de administración y datos
- Ejemplo de ruta que no registra eventos AWS Key Management Service
- Ejemplo de ruta que registra eventos relevantes de bajo volumen AWS Key Management Service
- Ejemplo de registro de seguimiento que no registra eventos de la API de datos de Amazon RDS

Ejemplo de registro de seguimiento con selectores de eventos específicos

En el siguiente ejemplo, se crea un selector de eventos para una ruta cuyo nombre *TrailName* incluye eventos de administración de solo lectura y solo escritura, eventos de datos para dos combinaciones de bucket y prefijo de Amazon S3 y eventos de datos para una sola función denominada. AWS Lambda *hello-world-python-function*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix","arn:aws:s3:::mybucket2/prefix2"]},{"Type": "AWS::Lambda::Function","Values":
 ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]}]}]'
```

El ejemplo devuelve el selector de eventos configurado para el registro de seguimiento.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
```

```
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Ejemplo de registro de seguimiento que registra todos los eventos de administración y datos

En el siguiente ejemplo, se crea un selector de eventos para una ruta denominada *TrailName2* que incluye todos los eventos, incluidos los eventos de administración de solo lectura y solo escritura, y todos los eventos de datos de todos los buckets, funciones AWS Lambda y tablas de Amazon DynamoDB de la cuenta. AWS Como este ejemplo utiliza selectores de eventos básicos, no puede configurar el registro de eventos de S3 en AWS Outposts, llamadas JSON-RPC de Amazon Managed Blockchain en nodos de Ethereum ni otros tipos de recursos de selector de eventos avanzados. Debe utilizar selectores de eventos avanzados a fin de registrar eventos de datos para esos recursos. Para obtener más información, consulte Configuración de selectores de eventos avanzados.

> **Note**
>
> Si el registro de seguimiento solo aplica a una región, solo se registrarán los eventos de dicha región, aunque los parámetros del selector de eventos especifiquen todos los buckets de Amazon S3 y las funciones Lambda. Los selectores de eventos solo se aplican a las regiones en las que se crea el registro de seguimiento.

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

El ejemplo devuelve los selectores de eventos configurados para el registro de seguimiento.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

Ejemplo de ruta que no registra eventos AWS Key Management Service

En el siguiente ejemplo, se crea un selector de eventos para una ruta cuyo nombre *TrailName* incluye los eventos de administración de solo lectura y solo escritura, pero los eventos exclude AWS Key Management Service ().AWS KMS Como AWS KMS los eventos se consideran eventos de gestión y puede haber un gran volumen de ellos, pueden tener un impacto sustancial en su CloudTrail factura si tiene más de un registro que capture los eventos de administración. El usuario de este ejemplo ha optado por excluir los eventos de AWS KMS de todos los registros de seguimiento menos uno. Para excluir un origen de eventos, añada `ExcludeManagementEventSources` a los selectores de eventos y especifique un origen de eventos en el valor de cadena.

Si decide no registrar los eventos de administración, los AWS KMS eventos no se registrarán y no podrá cambiar la configuración AWS KMS del registro de eventos.

Para volver a iniciar el registro de AWS KMS eventos en una ruta, pase una matriz vacía como valor de`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

El ejemplo devuelve el selector de eventos configurado para el registro de seguimiento:

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para volver a iniciar el registro de AWS KMS eventos en una ruta, pase una matriz vacía como el valor de`ExcludeManagementEventSources`, tal y como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Ejemplo de ruta que registra eventos relevantes de bajo volumen AWS Key Management Service

En el siguiente ejemplo, se crea un selector de eventos para una ruta cuyo nombre *TrailName* incluye eventos y eventos de administración de solo escritura. AWS KMS Como AWS KMS los eventos se consideran eventos de gestión y puede haber un gran volumen de ellos, pueden tener un impacto sustancial en su CloudTrail factura si tiene más de un registro que capture los eventos de administración. En este ejemplo, el usuario ha optado por incluir los eventos de AWS KMS escritura `Disable`, que incluirán `Delete` y `ScheduleKey` dejarán de incluir acciones de gran volumen `Encrypt`, como `Decrypt`, y `GenerateDataKey` (ahora se consideran eventos de lectura).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

El ejemplo devuelve el selector de eventos configurado para el registro de seguimiento: Esto registra los eventos de administración de solo escritura, incluidos los eventos. AWS KMS

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Ejemplo de registro de seguimiento que no registra eventos de la API de datos de Amazon RDS

En el siguiente ejemplo, se crea un selector de eventos para una ruta cuyo nombre *TrailName* incluye eventos de administración de solo lectura y solo escritura, pero excluye los eventos de la API de datos de Amazon RDS. Como los eventos de la API de datos de Amazon RDS se tratan como eventos de administración y puede haber un gran volumen de ellos, pueden tener un impacto sustancial en su CloudTrail factura si tiene más de un registro que capture los eventos de

administración. El usuario de este ejemplo ha optado por excluir los eventos de la API de datos de Amazon RDS de todos los registros de seguimiento menos uno. Para excluir un origen de eventos, agregue `ExcludeManagementEventSources` a los selectores de eventos y especifique un origen de eventos de la API de datos de Amazon RDS en el valor de cadena: `rdsdata.amazonaws.com`.

Si elige no registrar eventos de administración, no se registran eventos de la API de datos de Amazon RDS y no podrá cambiar la configuración del registro de eventos.

Para volver a iniciar el registro de los eventos de administración de la API de datos de Amazon RDS en una ruta, pase una matriz vacía como el valor de`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

El ejemplo devuelve el selector de eventos configurado para el registro de seguimiento:

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para volver a iniciar el registro de los eventos de administración de la API de datos de Amazon RDS en una ruta, pase una matriz vacía con el valor de`ExcludeManagementEventSources`, como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Configuración de selectores de eventos avanzados

Para utilizar selectores de eventos avanzados a fin de incluir o excluir eventos de datos en lugar de selectores de eventos básicos, use selectores de eventos avanzados en la página de detalles

de la traza. Los selectores de eventos avanzados permiten registrar eventos de datos en más tipos de recursos que los selectores de eventos básicos. Los selectores básicos registran la actividad de objetos de S3, la actividad de ejecución de funciones de AWS Lambda y las tablas de DynamoDB.

En los selectores de eventos avanzados, cree una expresión para recopilar eventos de datos en tipos de recursos específicos, como depósitos S3, AWS Lambda funciones, tablas de DynamoDB, puntos de acceso S3 Object Lambda, API directas de Amazon EBS en instantáneas de EBS, puntos de acceso S3, transmisiones de DynamoDB, tablas creadas por Lake Formation y más. AWS Glue

Para obtener más información sobre los selectores de eventos avanzados, consulte Configuración de selectores de eventos avanzados.

Para ver la configuración de los selectores de eventos avanzados de un registro de seguimiento, ejecute el siguiente comando `get-event-selectors`. Debe ejecutar este comando desde la AWS región en la que se creó la ruta (la región de origen) o debe especificar esa región añadiendo el --region parámetro.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Si la ruta es una ruta de una organización y has iniciado sesión con una cuenta de miembro de la organización AWS Organizations, debes proporcionar el ARN completo de la ruta y no solo el nombre.

El siguiente ejemplo devuelve la configuración predeterminada de un selector de eventos avanzados de un registro de seguimiento. De forma predeterminada, no hay selectores de eventos avanzados configurados para un registro de seguimiento.

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para crear un selector de eventos avanzados, ejecute el comando `put-event-selectors`. Cuando se produce un evento de datos en tu cuenta, CloudTrail evalúa la configuración de tus senderos. Si el evento coincide con algún selector de eventos avanzados de un registro de seguimiento, se procesa el registro de seguimiento y se registra el evento. Puede configurar hasta

500 condiciones en un registro de seguimiento, incluido todos los valores especificados para todos los selectores de eventos avanzados del registro de seguimiento. Para obtener más información, consulte Registro de eventos de datos.

Temas

- Ejemplo de registro de seguimiento con selectores de eventos avanzados específicos
- Ejemplo de ruta que utiliza selectores de eventos avanzados personalizados para registrar Amazon S3 en eventos de AWS Outposts datos
- Ejemplo de ruta que utiliza selectores de eventos avanzados para excluir AWS Key Management Service eventos
- Ejemplo de ruta que utiliza selectores de eventos avanzados para excluir los eventos de administración de Amazon RDS Data API

Ejemplo de registro de seguimiento con selectores de eventos avanzados específicos

En el siguiente ejemplo, se crean selectores de eventos avanzados personalizados para una ruta cuyo nombre *TrailName* incluye eventos de administración de lectura y escritura (omitiendo el `readOnly` selector) y eventos de `DeleteObject` datos para todas las combinaciones de bucket `PutObject` y prefijo de Amazon S3, excepto para un bucket con nombre `sample_bucket_name` y eventos de datos para una función denominada. AWS Lambda `MyLambdaFunction` Dado que se trata de selectores de eventos avanzados personalizados, cada conjunto de selectores tiene un nombre descriptivo. Tenga en cuenta que una barra diagonal final forma parte del valor de ARN para los buckets de S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
```

```
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

El ejemplo devuelve los selectores de eventos avanzados configurados para el registro de seguimiento.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
```

```
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Ejemplo de ruta que utiliza selectores de eventos avanzados personalizados para registrar Amazon S3 en eventos de AWS Outposts datos

El siguiente ejemplo muestra cómo configurar su ruta para incluir todos los eventos de datos de todos los Amazon S3 en los AWS Outposts objetos de su puesto de avanzada. En esta versión, el valor admitido para S3 en AWS Outposts los eventos del `resources.type` campo es`AWS::S3Outposts::Object`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
```

```
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

Ejemplo de ruta que utiliza selectores de eventos avanzados para excluir AWS Key Management Service eventos

El siguiente ejemplo crea un selector de eventos avanzado para una ruta cuyo nombre *TrailName*incluye eventos de administración de solo lectura y solo escritura (omitiendo el `readOnly` selector), pero excluye eventos (). AWS Key Management Service AWS KMS Como AWS KMS los eventos se consideran eventos de gestión y puede haber un gran volumen de ellos, pueden tener un impacto sustancial en su CloudTrail factura si tiene más de un registro que capture los eventos de administración.

Si decide no registrar los eventos de administración, los AWS KMS eventos no se registrarán y no podrá cambiar la configuración AWS KMS del registro de eventos.

Para volver a iniciar el registro de AWS KMS eventos en una ruta, quite el `eventSource` selector y vuelva a ejecutar el comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

El ejemplo devuelve los selectores de eventos avanzados configurados para el registro de seguimiento.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para comenzar de nuevo el registro de eventos excluidos en un registro de seguimiento, quite el selector `eventSource`, como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Ejemplo de ruta que utiliza selectores de eventos avanzados para excluir los eventos de administración de Amazon RDS Data API

El siguiente ejemplo crea un selector de eventos avanzado para una ruta cuyo nombre *TrailName*incluye eventos de administración de solo lectura y solo escritura (omitiendo el `readOnly` selector), pero excluye los eventos de administración de Amazon RDS Data API. Para excluir los eventos de administración de la API de datos de Amazon RDS, especifique la fuente de eventos de la API de datos de Amazon RDS en el valor de cadena del `eventSource` campo:. `rdsdata.amazonaws.com`

Si decide no registrar los eventos de administración, los eventos de administración de la API de datos de Amazon RDS no se registran y no puede cambiar la configuración del registro de eventos de la API de datos de Amazon RDS.

Para volver a iniciar el registro de los eventos de administración de la API de datos de Amazon RDS en una ruta, quite el `eventSource` selector y vuelva a ejecutar el comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

El ejemplo devuelve los selectores de eventos avanzados configurados para el registro de seguimiento.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para comenzar de nuevo el registro de eventos excluidos en un registro de seguimiento, quite el selector `eventSource`, como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Detención e inicio del registro de un registro de seguimiento

Los siguientes comandos inician y detienen el CloudTrail registro.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> Antes de eliminar un bucket, ejecute el comando `stop-logging` para detener el envío de eventos al bucket. Si no detiene el registro, CloudTrail intentará entregar los archivos de registro a un depósito con el mismo nombre durante un período de tiempo limitado.
> Si dejas de registrar o eliminas una ruta, CloudTrail Insights se deshabilita en esa ruta.

Eliminación de un registro de seguimiento

Si ha habilitado los eventos CloudTrail de administración en Amazon Security Lake, debe mantener al menos un registro organizativo que sea multirregional y registre tanto `read` los eventos de administración como los eventos `write` de administración. No puede eliminar una ruta si es la única que tiene que cumple este requisito, a menos que desactive la CloudTrail administración de eventos en Security Lake.

Puede eliminar un registro de seguimiento con el siguiente comando. Puede eliminar un registro de seguimiento únicamente en la región en la que lo creó (la región principal).

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Cuando se elimina un registro de seguimiento, no se elimina el bucket de Amazon S3 ni el tema de Amazon SNS asociados. Utilice la API AWS Management Console AWS CLI, o de servicio para eliminar estos recursos por separado.

Creación de un registro de seguimiento para una organización

Si ha creado una organización en AWS Organizations, puede crear un registro que registre todos los eventos de todos los miembros Cuentas de AWS de esa organización. En ocasiones, esto se denomina traza de organización.

La cuenta de administración de la organización puede asignar un administrador delegado para que cree nuevos registros de seguimiento de la organización o administre los registros de seguimiento de la organización existentes. Para obtener más información acerca de cómo agregar un administrador delegado, consulte Agrega un administrador delegado CloudTrail .

La cuenta de administración de la organización puede editar un registro de seguimiento existente en su cuenta y aplicarlo a una organización, lo que lo convertirá en un registro de seguimiento de la organización. La organización realiza un seguimiento de los eventos de registro de la cuenta de administración y de todas las cuentas miembro de la organización. Para obtener más información AWS Organizations, consulte Terminología y conceptos de Organizations.

> **Note**
>
> Debe iniciar sesión con la cuenta de administración o la de un administrador delegado asociado a una organización para poder crear un registro de seguimiento de la organización. También debe tener permisos suficientes para que el usuario o el rol de la cuenta de administración o la de administrador delegado pueda crear el registro de seguimiento. Si no tiene permisos suficientes, no podrá ver la opción para aplicar un registro de seguimiento a una organización.

Todos los registros organizativos creados con la consola son registros organizativos multirregionales que registran los eventos de las cuentas habilitadas Regiones de AWS en cada miembro de la organización. Para registrar los eventos en todas las AWS particiones de su organización, cree un registro de organización multirregional en cada partición. Puede crear un registro organizativo de una o varias regiones mediante el. AWS CLI Si crea un sendero de una sola región, registrará la actividad únicamente en el sendero Región de AWS (también denominado región de origen).

Aunque la mayoría Regiones de AWS están habilitadas de forma predeterminada Cuenta de AWS, debes habilitar manualmente determinadas regiones (también denominadas regiones de suscripción). Para obtener información sobre qué regiones están habilitadas de forma predeterminada, consulte Consideraciones antes de habilitar o deshabilitar las regiones en la Guía de AWS Account Management referencia. Para ver la lista de regiones CloudTrail compatibles, consulteCloudTrail regiones compatibles.

Cuando crea un registro de la organización, se crea una copia del registro con el nombre que le dé en las cuentas de los miembros que pertenecen a su organización.

- Si el registro de la organización es para una sola región y la región de origen de la ruta no es una región opcional, se crea una copia de la ruta en la región de origen de la ruta de la organización, en la cuenta de cada miembro.

- Si el registro de la organización es para una región única y la región de origen del sendero es una región opcional, se crea una copia del registro en la región de origen del sendero de la organización, en las cuentas de los miembros que han habilitado esa región.
- Si la ruta organizativa es multirregional y la región de origen de la ruta no es una región opcional, se crea una copia de la ruta en cada una de las cuentas habilitadas Región de AWS en cada cuenta de miembro. Cuando la cuenta de un miembro habilita una región opcional, se crea una copia del recorrido multiregional en la región que acaba de registrarse para la cuenta del miembro una vez que se haya completado la activación de esa región.
- Si el registro de la organización es multirregional y la región de origen es una región opcional, las cuentas de los miembros no enviarán la actividad al registro de la organización a menos que opten por hacerlo en el Región de AWS lugar en el que se creó el registro multirregional. Por ejemplo, si creas una ruta multirregional y eliges la región de Europa (España) como región de origen de la ruta, solo las cuentas de los miembros que hayan habilitado la región de Europa (España) en su cuenta enviarán la actividad de su cuenta a la ruta de la organización.

> **Note**
>
> CloudTrail crea registros organizativos en las cuentas de los miembros incluso si se produce un error en la validación de un recurso. Algunos ejemplos de errores de validación son los siguientes:
>
> - una política de bucket de Amazon S3 incorrecta
> - una política de temas de Amazon SNS incorrecta
> - incapacidad para realizar la entrega a un CloudWatch grupo de registros
> - permiso insuficiente para cifrar mediante una clave KMS
>
> Una cuenta de miembro con CloudTrail permisos puede ver cualquier error de validación del registro de una organización consultando la página de detalles del registro en la CloudTrail consola o ejecutando el AWS CLI get-trail-statuscomando.

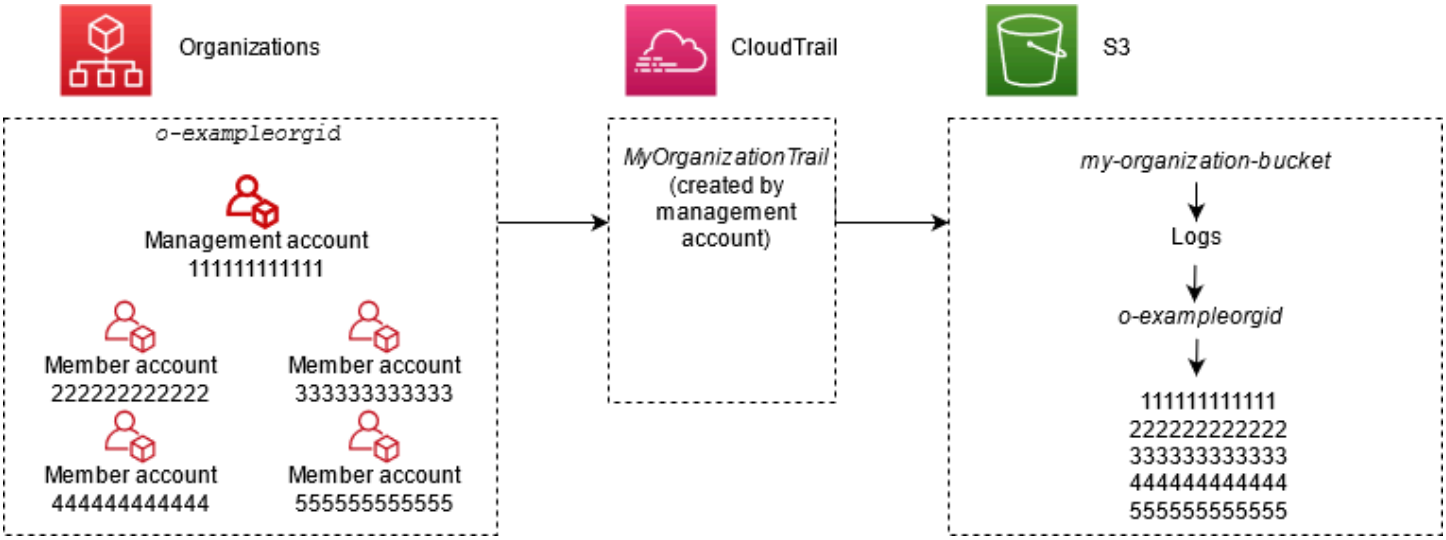
Los usuarios con CloudTrail permisos en las cuentas de los miembros pueden ver los registros de la organización cuando inician sesión en la AWS CloudTrail consola desde sus cuentas o cuando ejecutan AWS CLI comandos como Cuentas de AWS, por ejemplo`describe-trails`. Sin embargo, los usuarios de las cuentas de los miembros no tienen permisos suficientes para eliminar los

registros de la organización, activar o desactivar el inicio de sesión, cambiar los tipos de eventos que se registran o cambiar de algún otro modo el registro de la organización.

Al crear un registro de la organización en la consola o al habilitarlo CloudTrail como servicio de confianza en Organizations, se crea un rol vinculado al servicio para realizar tareas de registro en las cuentas de los miembros de la organización. Esta función recibe un nombre AWSServiceRoleForCloudTraily es necesaria CloudTrail para registrar los eventos de una organización. Si Cuenta de AWS se agrega un elemento a una organización, se le agregan el registro de la organización y el rol vinculado al servicio Cuenta de AWS, y el registro de esa cuenta se inicia automáticamente en el registro de la organización. Si Cuenta de AWS se elimina un elemento de una organización, el registro de la organización y el rol vinculado al servicio se eliminan de la organización Cuenta de AWS que ya no forma parte de la organización. Sin embargo, los archivos de registros de la cuenta eliminada creados antes de la eliminación de la cuenta permanecerán en el bucket de Amazon S3, donde se almacenan los archivos de registros del traza.

Si la cuenta de administración de una AWS Organizations organización crea un registro de la organización, pero luego se elimina como cuenta de administración de la organización, cualquier registro de la organización creado con esa cuenta pasa a ser un registro no organizacional.

En el siguiente ejemplo, la cuenta de administración de la organización, 1111, crea un registro con el nombre o-exampleorgid MyOrganizationTrailde la organización. El registro de seguimiento registra la actividad de todas las cuentas de la organización en el mismo bucket de Amazon S3. Todas las cuentas de la organización pueden ver *MyOrganizationTrail*en su lista de rutas, pero las cuentas de los miembros no pueden eliminar ni modificar la ruta de la organización. Solo la cuenta de administración o la de administrador delegado pueden modificar o eliminar los registros de seguimiento de la organización. Solo la cuenta de administración puede eliminar una cuenta miembro de una organización. Del mismo modo, de forma predeterminada, solo la cuenta de administración tiene acceso al bucket *my-organization-bucket*de Amazon S3 de la ruta y a los registros que contiene. La estructura de bucket de alto nivel para los archivos de registro contiene una carpeta con el nombre del ID de la organización, y subcarpetas con el nombre de los ID de cada cuenta de la organización. Los eventos de cada cuenta miembro se registran en la carpeta correspondiente al ID de la cuenta miembro. Si la cuenta de miembro 444444444444 se elimina de la organización *MyOrganizationTrail*y el rol vinculado al servicio deja de aparecer en la AWS cuenta 444444444444 y el registro de la organización no registra más eventos para esa cuenta. Sin embargo, la carpeta 444444444444 permanece en el bucket de Amazon S3, con todos los registros creados antes de la eliminación de la cuenta de la organización.



En este ejemplo, el ARN del registro de seguimiento creado en la cuenta de administración es `aws:cloudtrail:us-east-2:111111111111:trail/MyOrganizationTrail`. Este ARN también es el ARN del registro de seguimiento en todas las cuentas miembro.

Los registros de seguimiento de organización son similares a los normales en muchos aspectos. Puede crear varios registros de seguimiento para su organización y elegir si desea crear uno de organización en todas las regiones o en una sola región, y qué tipo de eventos desea que se guarden en el registro de seguimiento de organización, al igual que en cualquier otro registro de seguimiento. Sin embargo, hay algunas diferencias. Por ejemplo, cuando crea un registro en la consola y decide si desea registrar los eventos de datos para los buckets o AWS Lambda funciones de Amazon S3, los únicos recursos que aparecen en la CloudTrail consola son los de la cuenta de administración, pero puede añadir los ARN de los recursos de las cuentas de los miembros. Los eventos de datos para los recursos de cuenta miembro especificados se registran sin tener que configurar manualmente el acceso entre cuentas a dichos recursos. Para obtener más información sobre el registro de eventos de administración, eventos de Insights y eventos de datos, consulte Trabajar con archivos de registros de CloudTrail.

> **Note**
>
> En la consola, cree un registro de seguimiento que registre todas las regiones. Esta es la mejor práctica recomendada; registrar la actividad en todas las regiones le ayuda a mantener su AWS entorno más seguro. Para crear un registro de seguimiento de una sola región, utilice la AWS CLI.

También puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros de una organización y actuar en función de ellos, del mismo modo que lo haría con cualquier otro registro. Por ejemplo, puede analizar los datos en un registro de seguimiento de organización mediante Amazon Athena. Para obtener más información, consulte AWS integraciones de servicios con registros CloudTrail .

Temas

- Historial de eventos y registros de seguimiento de organización
- Prácticas recomendadas para pasar de los registros de seguimiento de cuentas miembro a los registros de seguimiento de la organización
- Prepararse a fin de crear un registro de seguimiento para la organización
- Creación de un registro de seguimiento para la organización en la consola
- Crear un registro para una organización con AWS Command Line Interface
- Solución de problemas

Historial de eventos y registros de seguimiento de organización

Cuando consultas los eventos de una organización en la que has iniciado sesión en el historial de eventos AWS Organizations, solo podrás ver los eventos de la organización Cuenta de AWS con la que hayas iniciado sesión. Por ejemplo, si ha iniciado sesión con la cuenta de administración de la organización, en Event history (Historial de eventos) se muestran los eventos de administración de los últimos 90 días para la cuenta de administración. Los eventos de la cuenta miembro de la organización no se muestran en Event history (Historial de eventos) para la cuenta de administración. Para ver los eventos de la cuenta miembro en Event history (Historial de eventos), inicie sesión con la cuenta miembro.

Prácticas recomendadas para pasar de los registros de seguimiento de cuentas miembro a los registros de seguimiento de la organización

Si ya tienes los registros CloudTrail configurados para las cuentas de los miembros individuales, pero quieres pasar a un registro de la organización para registrar los eventos en todas las cuentas, no querrás perder los eventos eliminando los registros de las cuentas de los miembros individuales antes de crear un registro de la organización. Pero cuando tiene dos registros de seguimiento, genera costos más altos debido a la copia adicional de los eventos enviados al registro de seguimiento de la organización.

Para ayudar a administrar los costos, pero evitar que se pierdan eventos antes de que comience la entrega del registro en el registro de seguimiento de la organización, plantéese mantener tanto los registros de seguimiento de la cuenta de miembro individual como el registro de seguimiento de la organización durante un día. Esto garantiza que el registro de seguimiento de la organización registre todos los eventos, pero solo genere costos de eventos duplicados durante un día. Después del primer día, puede dejar de iniciar sesión (o eliminar) cualquier registro de seguimiento de cuenta de miembro individual.

Prepararse a fin de crear un registro de seguimiento para la organización

Antes de crear un registro de seguimiento para su organización, deberá asegurarse de que la cuenta de administración o la de administrador delegado se encuentren configuradas correctamente para la creación de registros de seguimiento.

- Su organización debe tener todas las características habilitadas para poder crear un registro de seguimiento para ella. Para obtener más información, consulte Habilitar todas las características en la organización.
- La cuenta de administración debe tener el rol de AWSServiceRoleForOrganizations. Organizations crea automáticamente este rol al crear la organización y es necesario CloudTrail para registrar los eventos de una organización. Para obtener más información, consulte Organizations y roles vinculados a servicios.
- El usuario o el rol que crea el registro de seguimiento de la organización en la cuenta de administración o la cuenta de administrador delegado deben tener permisos suficientes para crear un registro de seguimiento de organización. Debe aplicar al menos la política AWSCloudTrail_FullAccess, o una política equivalente, a ese rol o usuario. También debe tener permisos suficientes en IAM y Organizations para crear el rol vinculado a servicios y habilitar el acceso de confianza. La siguiente política de ejemplo muestra los permisos mínimos necesarios.

> **Note**
>
> No debes compartir la AWSCloudTrail_FullAccesspolítica de forma amplia entre todos tus miembros Cuenta de AWS. En su lugar, deberías restringirla a Cuenta de AWS los administradores debido a la naturaleza altamente confidencial de la información recopilada por ellos CloudTrail. Los usuarios con este rol tienen la capacidad de desactivar o reconfigurar las funciones de auditoría más importantes y confidenciales de su Cuentas de AWS. Por este motivo, debe supervisar y controlar de cerca el acceso a esta política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

- Para usar las API AWS CLI o las CloudTrail API para crear un registro de la organización, debe habilitar el acceso confiable para CloudTrail In Organizations y debe crear manualmente un bucket de Amazon S3 con una política que permita registrar un registro de la organización. Para obtener más información, consulte Crear un registro para una organización con AWS Command Line Interface.
- Para usar una función de IAM existente para añadir la supervisión de un registro de la organización a Amazon CloudWatch Logs, debe modificar manualmente la función de IAM para permitir la entrega de CloudWatch los registros de las cuentas de los miembros al grupo de CloudWatch registros de la cuenta de administración, como se muestra en el siguiente ejemplo.

> **Note**
>
> Debe utilizar un rol de IAM y un grupo de CloudWatch registros que existan en su propia cuenta. No puede usar un rol de IAM ni un grupo de CloudWatch registros que pertenezca a una cuenta diferente.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Puedes obtener más información sobre Amazon CloudTrail y cómo CloudWatch inicia sesiónMonitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs. Además, tenga en cuenta los límites de CloudWatch los registros y las consideraciones de precio del servicio antes de decidir habilitar la experiencia para un registro organizacional. Para obtener más información, consulta CloudWatch Logs Limits y Amazon CloudWatch Pricing.

- Si desea registrar eventos de datos en el registro de seguimiento de organización para determinados recursos en las cuentas miembro, prepare la lista de nombres de recursos de Amazon (ARN) para cada uno de esos recursos. Los recursos de las cuentas de los miembros no se muestran en la CloudTrail consola al crear una ruta; puede buscar los recursos de la cuenta de administración en los que se admite la recopilación de eventos de datos, como los buckets de S3.

Del mismo modo, si desea agregar recursos miembro específicos al crear o actualizar un registro de seguimiento de organización en la línea de comandos, necesitará los ARN de dichos recursos.

> **Note**
>
> Se aplican cargos adicionales para registrar eventos de datos. Para CloudTrail conocer los precios, consulte AWS CloudTrail Precios.

También deberías considerar revisar cuántos registros existen ya en la cuenta de administración y en las cuentas de los miembros antes de crear un registro de la organización. CloudTrail limita el número de senderos que se pueden crear en cada región. No puede superar este límite en la región en la que cree el registro de seguimiento de organización en la cuenta de administración. Sin embargo, el registro de seguimiento se creará en las cuentas miembro, incluso si estas han alcanzado el límite de registros de seguimiento en una región. Aunque el primer registro de seguimiento de los eventos de administración en cualquier región es gratuito, se aplican cargos a los registros de seguimiento adicionales. Para reducir el costo potencial de un registro de seguimiento de organización, considere la posibilidad de eliminar cualquier registro de seguimiento innecesario en las cuentas miembro y de administración. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail los precios.

Prácticas recomendadas de seguridad para las trazas de organización

Como práctica recomendada de seguridad, le recomendamos que agregue la clave de condición `aws:SourceArn` de las políticas de recursos (como las de buckets de S3, claves KMS o temas SNS) que utiliza con una traza de la organización. El valor de `aws:SourceArn` es el ARN de la traza de organización (o ARN, si está utilizando el mismo recurso para más de una traza, como el mismo bucket de S3 para almacenar registros de más de una traza). Esto garantiza que el recurso, como un bucket de S3, solo acepta datos asociados a la traza específica. El ARN de seguimiento debe utilizar el ID de cuenta de la cuenta de administración. El siguiente fragmento de política muestra un ejemplo en el que más de una traza utiliza el recurso.

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

Para obtener información acerca de cómo agregar claves de condición a las políticas de recursos, consulte lo siguiente:

- Política de bucket de Amazon S3 para CloudTrail
- Configurar políticas de clave de AWS KMS para CloudTrail
- Política temática de Amazon SNS para CloudTrail

Creación de un registro de seguimiento para la organización en la consola

Para crear un registro de la organización desde la CloudTrail consola, debe iniciar sesión en la consola como usuario o rol en la cuenta de administración o administrador delegado que tenga permisos suficientes. Si no inicias sesión con la cuenta de administración o de administrador delegado, no verás la opción de aplicar una ruta a una organización al crear o editar una ruta desde la CloudTrail consola.

Puede configurar un registro de seguimiento de organización de varias maneras. Por ejemplo, puede configurar los siguientes detalles para el registro de seguimiento de organización:

- De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento registra todas las Regiones de AWS de la partición de AWS en la que trabaja. Como práctica recomendada, te recomendamos encarecidamente que registres los eventos en todas las regiones de tu Cuenta de AWS país. Para crear un registro de seguimiento para una sola región, utilice la AWS CLI. Para obtener más información, consulte Cómo CloudTrail funciona.
- Especifique si desea aplicar el registro de seguimiento a su organización. De forma predeterminada, los registros de seguimiento no se aplican a las organizaciones. Debe seleccionar esta opción para crear un registro de seguimiento de organización.
- Especifique qué bucket de Amazon S3 recibirá los archivos de registros de seguimiento para el registro de seguimiento de organización. Puede elegir un bucket de Amazon S3 existente o crear uno específicamente para el registro de seguimiento de organización.
- Para los eventos de administración y datos, especifique si desea registrar los eventos de Read (Lectura), Write (Escritura) o ambos. CloudTrailLos eventos de Insights se registran solo en los eventos de administración. Puede especificar registrar eventos de datos para recursos en la cuenta de administración al elegirlos en las listas de la consola y en las cuentas miembro si especifica los ARN de cada recurso para el que desea habilitar el registro de eventos de datos. Para obtener más información, consulte Eventos de datos.

Para crear un registro de la organización con AWS Management Console

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.

   Debe iniciar sesión con una identidad de IAM de la cuenta de administración o la de administrador delegado que tenga permisos suficientes para crear un registro de seguimiento de organización.
2. Elija Trails (Registros de seguimiento) y, a continuación, elija Create trail (Crear registro de seguimiento).
3. En la página Create Trail, escriba el nombre del registro de seguimiento en Trail name. Para obtener más información, consulte Requisitos de nomenclatura.
4. Seleccione Enable for all accounts in my organization (Habilitar para todas las cuentas de mi organización). Solo verá esta opción si inició sesión en la consola con un usuario o un rol de la cuenta de administración o la de administrador delegado. Para crear correctamente un registro de seguimiento de organización, asegúrese de que el usuario o el rol tengan permisos suficientes.
5. En Storage location (Ubicación del almacenamiento), elija Create new S3 bucket (Crear un bucket de S3 nuevo) para crear un bucket. Al crear un bucket, CloudTrail crea y aplica las políticas de bucket requeridas.

   > **Note**
   >
   > Si eligió Use existing S3 bucket (Utilizar bucket de S3 existente), especifique un bucket en Trail log bucket name (Nombre del bucket de registro de seguimiento), o elija Browse (Examinar) para elegir un bucket. Puedes elegir un bucket que pertenezca a cualquier cuenta; sin embargo, la política del bucket debe conceder CloudTrail permiso para escribir en él. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Política de bucket de Amazon S3 para CloudTrail.

   Para facilitar la búsqueda de tus registros, crea una nueva carpeta (también conocida como prefijo) en un depósito existente para almacenar tus CloudTrail registros. Ingrese el prefijo en Prefix (Prefijo).
6. En Log file SSE-KMS encryption (Cifrado SSE-KMS de archivos de registro), elija Enabled (Habilitado) si desea cifrar sus archivos de registro con cifrado SSE-KMS en vez de SSE-S3. El

valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los registros se cifrarán mediante el cifrado SSE-S3. Para obtener más información sobre el cifrado SSE-KMS, consulte Uso del cifrado del lado del servidor con AWS Key Management Service (SSE-KMS). Para obtener más información sobre el cifrado SSE-S3, consulte Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3) (Uso de cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 [SSE-S3]).

Si habilita el cifrado SSE-KMS, elija uno nuevo o existente. AWS KMS key En AWS KMS Alias, especifique un alias en el formato. `alias/` *`MyAliasName`* Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS.

> **Note**
>
> También puede escribir el ARN de una clave de otra cuenta. Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS. La política de claves debe CloudTrail permitir el uso de la clave para cifrar los archivos de registro y permitir que los usuarios que especifique lean los archivos de registro sin cifrar. Para obtener más información sobre cómo editar manualmente la política de claves, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

7. En Additional settings (Configuración adicional), configure lo siguiente.

   a. En Log file validation (Validación de archivo de registros), elija Enabled (Habilitado) para que se envíen los resúmenes de archivos de registros a su bucket de S3. Puede utilizar los archivos de resumen para comprobar que los archivos de registro no han cambiado después de CloudTrail entregarlos. Para obtener más información, consulte Validar la integridad de los archivos de registros de CloudTrail.

   b. Para la entrega de notificaciones de SNS, selecciona Activado para recibir una notificación cada vez que se entregue un registro a tu depósito. CloudTrail almacena varios eventos en un archivo de registro. Las notificaciones de SNS se envían para cada archivo de registro, no para cada evento. Para obtener más información, consulte Configuración de notificaciones de Amazon SNS para CloudTrail.

      Si habilita las notificaciones SNS, en Create a new SNS topic (Crear un tema de SNS nuevo), elija New (Nuevo) para crear un tema o elija Existing (Existente) a fin de utilizar un tema existente. Si va a crear un registro de seguimiento que se aplica a todas las regiones, las notificaciones de SNS de los envíos de archivos de registro de todas las regiones se envían al tema de SNS que cree.

Si elige Nuevo, CloudTrail especifica un nombre para el nuevo tema o puede escribir un nombre. Si elige Existing (Existente), elija un tema de SNS en la lista desplegable. También puede especificar el ARN de un tema de otra región o de una cuenta con los permisos adecuados. Para obtener más información, consulte Política temática de Amazon SNS para CloudTrail.

Si crea un tema, deberá suscribirse al tema para recibir una notificación del envío de archivos de registro. Puede suscribirse en la consola de Amazon SNS. Debido a la frecuencia de las notificaciones, recomendamos que configure la suscripción para que se utilice una cola de Amazon SQS a fin de administrar las notificaciones mediante programación. Para obtener más información, consulte la Guía de introducción de Amazon Simple Notification Service.

8. Si lo desea, configure CloudTrail el envío de archivos de registro a CloudWatch Logs seleccionando Activado en CloudWatch los registros. Para obtener más información, consulte Envío de eventos a Amazon CloudWatch Logs.

> **Note**
>
> Solo la cuenta de administración puede configurar un grupo de CloudWatch registros para un registro de la organización mediante la consola. El administrador delegado puede configurar un grupo de CloudWatch registros mediante las operaciones de la `UpdateTrail` API AWS CLI CloudTrail `CreateTrail` o o.

   a. Si habilita la integración con CloudWatch los registros, elija Nuevo para crear un nuevo grupo de registros o Existente para usar uno existente. Si elige Nuevo, CloudTrail especifique un nombre para el nuevo grupo de registros o puede escribir un nombre.
   b. Si elige Existing (Existente), elija un grupo de registros en la lista desplegable.
   c. Elija Nuevo para crear un nuevo rol de IAM con los permisos necesarios para enviar CloudWatch registros a Logs. Elija Existing (Existente) para elegir un rol de IAM en la lista desplegable. La instrucción de la política para el rol nuevo o existente se muestra al expandir Policy document (Documento de política). Para obtener más información acerca de este rol, consulte Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear.

> **Note**
>
> Cuando configure un registro de seguimiento, podrá seleccionar un bucket de S3 y un tema de Amazon SNS que pertenezcan a otra cuenta. Sin embargo, si desea CloudTrail enviar eventos a un grupo de CloudWatch registros, debe elegir un grupo de registros que exista en su cuenta actual.

9. En Tags (Etiquetas), agregue una o más etiquetas personalizadas (pares clave-valor) a su registro de seguimiento. Las etiquetas pueden ayudarle a identificar tanto sus CloudTrail senderos como los depósitos de Amazon S3 que contienen archivos de CloudTrail registro. A continuación, puede utilizar grupos de recursos para sus CloudTrail recursos. Para más información, consulte AWS Resource Groups y ¿Por qué usar etiquetas para CloudTrail los recursos?.
10. En la página Choose log events (Elegir eventos de registro), elija los tipos de eventos que desea registrar. En Management events (Eventos de administración), haga lo siguiente.

    a. En API activity (Actividad de la API), elija si desea que su registro de seguimiento registre eventos de Read (Lectura), Write (Escritura) o ambos. Para obtener más información, consulte Eventos de administración.

    b. Elige Excluir AWS KMS eventos para filtrar AWS Key Management Service (AWS KMS) los eventos de tu ruta. La configuración predeterminada es incluir a todos los eventos de AWS KMS .

       La opción de registrar o excluir AWS KMS eventos solo está disponible si registras los eventos de administración en tu ruta. Si elige no registrar los eventos de administración, los AWS KMS eventos no se registran y no puede cambiar la configuración AWS KMS del registro de eventos.

       AWS KMS acciones como `EncryptDecrypt`, y `GenerateDataKey` suelen generar un gran volumen (más del 99%) de eventos. Estas acciones se registran ahora como eventos de lectura. AWS KMS Las acciones relevantes de bajo volumen, como `DisableDelete`, y `ScheduleKey` (que normalmente representan menos del 0,5% del volumen de AWS KMS eventos) se registran como eventos de escritura.

       Para excluir eventos de gran volumen como `Encrypt`, `Decrypt` y `GenerateDataKey`, y seguir registrando eventos relevantes como `Disable`, `Delete` y `ScheduleKey`, elija

registrar eventos de administración Write (Escritura) y desmarque la casilla de verificación Exclude AWS KMS events (Excluir eventos de KMS).

c. Elija Exclude Amazon RDS Data API events (Excluir eventos de API de datos de Amazon RDS) para quitar del registro de seguimiento los eventos de API de datos de Amazon Relational Database Service. La configuración predeterminada es incluir a todos los eventos de la API de datos de Amazon RDS. A fin de obtener más información sobre los eventos de API de datos de Amazon RDS, consulte Registro de llamadas a la API de datos con AWS CloudTrail en la Guía del usuario de Amazon RDS para Aurora.

11. Para registrar eventos de datos, elija Data events (Eventos de datos). Se aplican cargos adicionales para registrar eventos de datos. Para obtener más información, consulte AWS CloudTrail Precios.

12. **Important**

    Los pasos del 12 al 16 son para configurar los eventos de datos mediante selectores de eventos avanzados, que son los predeterminados. Los selectores de eventos avanzados le permiten configurar más tipos de eventos de datos y ofrecen un control detallado de los eventos de datos que captura su registro de seguimiento. Si ha optado por utilizar selectores de eventos básicos, complete los pasos que se indican en Configurar los ajustes de eventos de datos mediante selectores de eventos básicos y, a continuación, vuelva al paso 17 de este procedimiento.

    En Data event type (Tipo de evento de datos), elija el tipo de recurso en el que desea registrar los eventos de datos. Para obtener más información sobre los tipos de eventos de datos disponibles, consulte Eventos de datos.

    Note

    Para registrar los eventos de datos de AWS Glue las tablas creadas por Lake Formation, elija Lake Formation.

13. Elija una plantilla de selección de registros. CloudTrail incluye plantillas predefinidas que registran todos los eventos de datos del tipo de recurso. Para crear una plantilla de selector de registros personalizada, elija Custom (Personalizado).

> **Note**
>
> Si eliges una plantilla predefinida para los depósitos de S3, podrás registrar los eventos de datos de todos los depósitos que hay actualmente en tu AWS cuenta y de los que crees una vez que hayas terminado de crear el registro. También permite registrar la actividad de eventos de datos realizada por cualquier identidad de IAM de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
>
> Si el registro de seguimiento solo aplica a una región, elegir una plantilla predefinida que registra todos los buckets de S3 permite el registro de eventos de datos de todos los buckets en la misma región que el registro de seguimiento, así como de cualquier otro bucket que cree posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de la cuenta de AWS .
>
> Si va a crear un registro para todas las regiones, al elegir una plantilla predefinida para las funciones de Lambda se habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en su AWS cuenta y para cualquier función de Lambda que pueda crear en cualquier región una vez que haya terminado de crear el registro. Si va a crear una ruta para una sola región (mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
>
> El registro de los eventos de datos para todas las funciones también permite registrar la actividad de los eventos de datos realizada por cualquier identidad de IAM de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

14. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo opcional para un selector de eventos avanzado, como “Registrar eventos de datos para solo dos buckets de S3”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
15. En Advanced event selectors (Selectores de eventos avanzados), cree una expresión para los recursos específicos en los que desea registrar eventos de datos. Puede omitir este paso si utiliza una plantilla de registro predefinida.

a. Elija uno de los siguientes campos.

- **`readOnly`**- se `readOnly` puede configurar para que sea igual a un valor de `true` o`false`. Los eventos de datos de solo lectura son eventos que no cambian el estado de un recurso, como eventos `Get*` o `Describe*`. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`. Para registrar eventos `read` y `write`, no agregue un selector de `readOnly`.
- **`eventName`**: `eventName` puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de datos registrado CloudTrail, como `PutBucketPutItem`, o`GetSnapshotBlock`.
- **`resources.ARN`**- Puede usar cualquier operador con`resources.ARN`, pero si usa valores iguales o no iguales, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo que especificó en la plantilla como valor de. `resources.type`

  En la siguiente tabla, se muestra el formato de ARN de cada `resources.type`.

  > **Note**
  >
  > No puede usar el `resources.ARN` campo para filtrar los tipos de recursos que no tienen ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*

resources.type	resources.ARN
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*

resources.type	resources.ARN
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	El ARN debe estar en uno de los siguientes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	resources.ARN
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir los eventos de streaming, añade un filtro en el `eventName` campo.

[2] Para registrar todos los eventos de datos de todos los objetos en un bucket de S3 específico, utilice el operador `StartsWith` e incluya solo el ARN del bucket como valor coincidente. La barra diagonal final es intencional; no la excluya.

[3] Para registrar eventos en todos los objetos de un punto de acceso de S3, se recomienda que utilice solo el ARN del punto de acceso. No incluya la ruta de acceso del objeto y utilice los operadores `StartsWith` o `NotStartsWith`.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte Acciones, recursos y claves de condición en la Guía del usuario de AWS Identity and Access Management .

b. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones. Por ejemplo, para excluir los eventos de datos de dos cubos de S3 de los eventos de datos que se registran en su ruta, puede establecer el campo en Resources.ARN, configurar el operador para no comienza por y, a continuación, pegar el ARN de un depósito de S3 o buscar los cubos de S3 para los que no desea registrar eventos.

   Para agregar el segundo bucket de S3, seleccione + Condición y, a continuación, repita la instrucción anterior, pegue el ARN o busque un bucket diferente.

> **Note**
>
> Puede tener un máximo de 500 valores para todos los selectores de un registro de seguimiento. Esto incluye matrices de varios valores para un selector como `eventName`. Si tiene valores únicos para todos los selectores, puede agregar un máximo de 500 condiciones a un selector.
> Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Puede registrar todas las funciones con una plantilla de selector predefinida, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear la ruta en la consola y, a continuación, utilizar el put-event-selectors comando AWS CLI and the para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Administrar senderos con el AWS CLI.

c. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos. Por ejemplo, no especifique un ARN en un selector para que sea igual a un valor y luego especifique que el ARN no sea igual al mismo valor en otro selector.

16. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos). Repita los pasos, desde el número 12 a este paso, a fin de configurar selectores de eventos avanzados para el tipo de evento de datos.
17. Elija los eventos de Insights si quiere que su ruta registre los eventos de CloudTrail Insights.

    En Event type (Tipo de evento), seleccione Insights events (Eventos de Insights). En Insights events (Eventos de Insights), elija API call rate (Tasa de llamada a la API), API error rate (Tasa de errores de API), o ambos. Debe registrar los eventos de administración de escritura para registrar los eventos de Insights para calcular la tasa de llamadas a la API. Debe registrar los eventos de administración de lectura o escritura para registrar los eventos de Insights para calcular la tasa de errores de la API.

    CloudTrail Insights analiza los eventos de administración para detectar actividades inusuales y los registra cuando se detectan anomalías. De forma predeterminada, los registros de seguimiento no registran eventos de Insights. Para obtener más información acerca de los eventos de Insights, consulte Registro de eventos de Insights. Se aplican cargos adicionales

por registrar eventos de Insights. Para CloudTrail conocer los precios, consulte AWS CloudTrail Precios.

Los eventos de Insights se envían a una carpeta diferente con el nombre `/CloudTrail-Insight` del mismo depósito de S3 que se especifica en el área de ubicación de almacenamiento de la página de detalles de la ruta. CloudTrailcrea el nuevo prefijo para usted. Por ejemplo, si el bucket de S3 de destino actual se denomina `S3bucketName/AWSLogs/CloudTrail/`, el nombre del bucket de S3 con un nuevo prefijo se denomina `S3bucketName/AWSLogs/CloudTrail-Insight/`.

18. Cuando haya terminado de elegir los tipos de eventos para registrar, elija Next (Siguiente).
19. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Elija Edit (Editar) en una sección para cambiar la configuración del registro de seguimiento que se muestra en esa sección. Cuando esté listo para crear el registro de seguimiento, elija Create trail (Crear registro de seguimiento).
20. El nuevo registro de seguimiento aparece en la página Trails. Un registro de seguimiento de organización puede tardar hasta 24 horas en crearse en todas las regiones de todas las cuentas miembro. La página Trails (Registros de seguimiento) muestra los registros de seguimiento de su cuenta de todas las regiones. En unos 5 minutos, CloudTrail publica los archivos de registro que muestran las llamadas a la AWS API realizadas en su organización. Puede ver los archivos de registros del bucket de Amazon S3 especificado.

> **Note**
>
> No se puede cambiar el nombre de un registro de seguimiento una vez creado. En su lugar, puede eliminar el registro de seguimiento y crear uno nuevo.

Siguientes pasos

Después de crear el registro de seguimiento, puede volver a él para realizar cambios:

- Cambie la configuración de su registro de seguimiento editándolo. Para obtener más información, consulte Actualización de un registro de seguimiento.
- En caso necesario, configure el bucket de Amazon S3 para permitir que usuarios específicos de las cuentas miembro puedan leer los archivos de registros de la organización. Para obtener más información, consulte Compartir archivos de registro de CloudTrail entre cuentas de AWS.

- Configure CloudTrail para enviar archivos de registro a CloudWatch Logs. Para obtener más información, consulte Envío de eventos a Amazon CloudWatch Logs y el elemento CloudWatch Registros enPrepararse a fin de crear un registro de seguimiento para la organización.

  > **Note**
  >
  > Solo la cuenta de administración puede configurar un grupo de CloudWatch registros para un registro de la organización.

- Cree una tabla y utilícela para ejecutar una consulta en Amazon Athena con el fin de analizar su actividad de servicio de AWS . Para obtener más información, consulte Creación de una tabla de CloudTrail registros en la CloudTrail consola en la Guía del usuario de Amazon Athena.
- Agregar etiquetas personalizadas (pares de clave-valor) al registro de seguimiento
- Para crear otro registro de seguimiento de organización, vuelva a la página Trails (Registros de seguimiento) y elija Create trail (Crear registro de seguimiento).

> **Note**
>
> Cuando configure un registro de seguimiento, podrá elegir un bucket de Amazon S3 y un tema de SNS que pertenezcan a otra cuenta. Sin embargo, si desea CloudTrail enviar eventos a un grupo de CloudWatch registros, debe elegir un grupo de registros que exista en su cuenta corriente.

Crear un registro para una organización con AWS Command Line Interface

Puede crear un registro de seguimiento de organización mediante la AWS CLI. Se AWS CLI actualiza periódicamente con funciones y comandos adicionales. Para garantizar el éxito, asegúrese de haber instalado o actualizado a una AWS CLI versión reciente antes de empezar.

> **Note**
>
> Los ejemplos de esta sección son específicos para la creación y actualización de registros de seguimiento de organización. Para ver ejemplos del uso de la AWS CLI para gestionar senderos, consulte Administrar senderos con el AWS CLI yConfiguración del monitoreo de CloudWatch Logs con la AWS CLI. Al crear o actualizar un registro de la organización con la AWS CLI, debes usar un AWS CLI perfil en la cuenta de administración o en la cuenta de

administrador delegado con permisos suficientes. Si va a convertir un registro de seguimiento de organización en un registro de seguimiento que no sea de la organización, debe utilizar la cuenta de administración de la organización.
Debe configurar el bucket de Amazon S3 utilizado para una registro de seguimiento de organización con permisos suficientes.

Creación o actualización de un bucket de Amazon S3 para utilizarlo a fin de almacenar los archivos de registros de un registro de seguimiento de organización

Debe especificar un bucket de Amazon S3 para recibir los archivos de registros de un registro de seguimiento de organización. Este depósito debe tener una política que permita CloudTrail colocar los archivos de registro de la organización en el depósito.

El siguiente es un ejemplo de política para un bucket de Amazon S3 denominado *myOrganizationBucket*, que es propiedad de la cuenta de administración de la organización. Sustituya *myOrganizationBucket*, *region*, *managementAccountID*, *TrailName* y *O-OrganizationID por los valores de su organización*

Esta política de bucket contiene tres instrucciones.

- La primera afirmación permite llamar CloudTrail a la `GetBucketAcl` acción de Amazon S3 en el bucket de Amazon S3.
- La segunda instrucción permite el registro en caso de que se cambie el registro de seguimiento de uno de organización a otro solo para esa cuenta.
- La tercera instrucción permite registrar el registro de seguimiento de una organización.

La política de ejemplo incluye una clave de condición `aws:SourceArn` para la política de bucket de Amazon S3. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que solo se CloudTrail escriba en el bucket de S3 para una o varias rutas específicas. En una traza de organización, el valor de `aws:SourceArn` debe ser un ARN de seguimiento que pertenece a la cuenta de administración y utilice el ID de cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
```

```
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Esta política de ejemplo no permite que ningún usuario de las cuentas miembro obtenga acceso a los archivos de registro creados para la organización. De forma predeterminada, solo la cuenta de administración tendrá acceso a los archivos de registros de organización. Para obtener información sobre cómo permitir a los usuarios de IAM de las cuentas miembro el acceso de lectura al bucket de Amazon S3, consulte Compartir archivos de registro de CloudTrail entre cuentas de AWS.

Se habilita CloudTrail como un servicio confiable en AWS Organizations

Para poder crear un registro de seguimiento de organización, primero debe habilitar todas las características en Organizations. Para obtener más información, consulte Habilitar todas las características en la organización o ejecute el siguiente comando mediante un perfil con permisos suficientes en la cuenta de administración:

```
aws organizations enable-all-features
```

Después de habilitar todas las funciones, debe configurar Organizations para que confíe CloudTrail como un servicio de confianza.

Para crear una relación de servicio de confianza entre AWS Organizations y CloudTrail, abra un terminal o una línea de comandos y utilice un perfil en la cuenta de administración. Ejecute el comando `aws organizations enable-aws-service-access`, como se muestra en el ejemplo siguiente.

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

Uso de create-trail

Creación de un registro de seguimiento de organización que se aplique a todas las regiones

Para crear un registro de seguimiento de organización que se aplique a todas las regiones, agregue las opciones `--is-organization-trail` y `--is-multi-region-trail`.

> **Note**
>
> Al crear un registro organizativo con la AWS CLI, debe utilizar un AWS CLI perfil en la cuenta de administración o en la cuenta de administrador delegado con permisos suficientes.

En el ejemplo siguiente, se crea un registro de seguimiento de organización que envía registros de todas las regiones a un bucket existente denominado *my-bucket*:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail --is-multi-region-trail
```

Para confirmar que el registro de seguimiento exista en todas las regiones, los parámetros `IsOrganizationTrail` e `IsMultiRegionTrail` en la salida se establecen en `true`:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Ejecute el comando `start-logging` para comenzar a ejecutar el registro de seguimiento. Para obtener más información, consulte Detención e inicio del registro de un registro de seguimiento.

Creación de un registro de seguimiento de organización como registro de seguimiento de una sola región

El siguiente comando crea un registro de la organización que solo registra los eventos en un único registro Región de AWS, también conocido como registro de una sola región. La AWS región en la que se registran los eventos es la región especificada en el perfil de configuración de AWS CLI.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail
```

Para obtener más información, consulte Requisitos de nomenclatura.

Resultado de ejemplo:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

De forma predeterminada, el comando `create-trail` crea un registro de seguimiento para una sola región que no permite la validación de archivos de registros.

> **Note**
>
> Ejecute el comando `start-logging` para comenzar a ejecutar el registro de seguimiento.

Ejecución de update-trail para actualizar un registro de seguimiento de organización

Puede ejecutar el comando `update-trail` para cambiar las opciones de configuración de un registro de seguimiento de organización o para aplicar un registro de seguimiento existente para una sola cuenta de AWS a toda una organización. Recuerde que puede ejecutar el comando `update-trail` únicamente desde la región en la que se creó el registro de seguimiento.

> **Note**
>
> Si utilizas el AWS CLI o uno de los AWS SDK para actualizar una ruta, asegúrate de que la política de segmentos de la ruta lo sea up-to-date. Para obtener más información, consulte Crear un registro para una organización con AWS Command Line Interface.
> Al actualizar el registro de una organización con el AWS CLI, debes usar un AWS CLI perfil en la cuenta de administración o en la cuenta de administrador delegado con permisos suficientes. Si desea convertir un registro de seguimiento de la organización en un registro de seguimiento que no sea de la organización, debe utilizar la cuenta de administración de la organización, ya que la cuenta de administración es la propietaria de todos los recursos de la organización.
> CloudTrail actualiza los registros de la organización en las cuentas de los miembros incluso si se produce un error en la validación de un recurso. Algunos ejemplos de errores de validación son los siguientes:
>
> - una política de bucket de Amazon S3 incorrecta
> - una política de temas de Amazon SNS incorrecta
> - incapacidad para realizar la entrega a un CloudWatch grupo de registros
> - permiso insuficiente para cifrar mediante una clave KMS
>
> Una cuenta de miembro con CloudTrail permisos puede ver cualquier error de validación del registro de una organización consultando la página de detalles del registro en la CloudTrail consola o ejecutando el AWS CLI get-trail-statuscomando.

Aplicación de un registro de seguimiento existente a una organización

Para cambiar un registro existente para que también se aplique a una organización en lugar de a una sola AWS cuenta, añade la `--is-organization-trail` opción, como se muestra en el siguiente ejemplo.

> **Note**
>
> Use la cuenta de administración para cambiar un registro de seguimiento existente que no es de la organización por un registro de seguimiento de la organización.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

Para confirmar que el registro de seguimiento se aplica ahora a la organización, el parámetro `IsOrganizationTrail` del resultado tiene el valor `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

En el ejemplo anterior, el registro de seguimiento se configuró para que se aplicara a todas las regiones (`"IsMultiRegionTrail": true`). Un registro de seguimiento que solo se aplica a una sola región mostrará `"IsMultiRegionTrail": false` en el resultado.

Conversión de un registro de seguimiento de organización que se aplica a una sola región en uno que se aplique a todas las regiones

Para cambiar un registro de seguimiento de organización existente de forma que se aplique a todas las regiones, agregue la opción `--is-multi-region-trail` como se muestra en el siguiente ejemplo.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Para confirmar que el registro de seguimiento se aplica ahora a todas las regiones, el parámetro `IsMultiRegionTrail` del resultado tiene el valor `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
```

```
}
```

Solución de problemas

En esta sección se proporciona información sobre cómo solucionar problemas relacionados con un registro de la organización.

Temas

- CloudTrail no está distribuyendo eventos
- CloudTrail no envía notificaciones de Amazon SNS para una cuenta de miembro de una organización

CloudTrail no está distribuyendo eventos

Si CloudTrail no entrega los archivos de CloudTrail registro al bucket de Amazon S3

Compruebe si hay algún problema con el bucket de S3.

- Desde la CloudTrail consola, consulta la página de detalles de la ruta. Si hay algún problema con el depósito de S3, la página de detalles incluye una advertencia de que se ha producido un error en la entrega al depósito de S3.
- Desde AWS CLI, ejecuta el get-trail-statuscomando. Si se produce un error, el resultado del comando incluye el `LatestDeliveryError` campo, que muestra cualquier error de Amazon S3 que se CloudTrail haya producido al intentar entregar los archivos de registro al depósito designado. Este error se produce solo cuando hay un problema con el bucket de S3 de destino y no se produce cuando se agota el tiempo de espera. Para resolver el problema, corrija la política del depósito para CloudTrail poder escribir en el depósito o cree uno nuevo y, a continuación, llame `update-trail` para especificar el nuevo depósito. Para obtener información sobre la política de cubos de la organización, consulte Crear o actualizar un depósito de Amazon S3 para almacenar los archivos de registro de un registro de la organización.

Si no CloudTrail está entregando CloudWatch registros a Logs

Compruebe si hay algún problema con la configuración de la política de roles de CloudWatch Logs.

- Desde la CloudTrail consola, consulta la página de detalles de la ruta. Si hay algún problema con CloudWatch los registros, la página de detalles incluye una advertencia que indica que se ha producido un error en la entrega de CloudWatch los registros.

- Desde AWS CLI, ejecuta el get-trail-statuscomando. Si se produce un error, el resultado del comando incluye el `LatestCloudWatchLogsDeliveryError` campo, que muestra cualquier error de CloudWatch registro que se CloudTrail haya producido al intentar entregar los CloudWatch registros a Logs. Para resolver el problema, corrija la política de roles de CloudWatch Logs. Para obtener información sobre la política CloudWatch de roles de Logs, consulteDocumento de política de roles CloudTrail para usar CloudWatch registros para monitorear.

Si no ves la actividad de una cuenta de miembro en el registro de una organización

Si no ves la actividad de una cuenta de miembro en el registro de una organización, comprueba lo siguiente:

- Comprueba la región de origen de la ruta para comprobar si es una región que se ha suscrito

  Aunque la mayoría Regiones de AWS están habilitadas de forma predeterminada para ti Cuenta de AWS, debes habilitar manualmente determinadas regiones (también denominadas regiones de suscripción). Para obtener información sobre qué regiones están habilitadas de forma predeterminada, consulte Consideraciones antes de habilitar o deshabilitar las regiones en la Guía de AWS Account Management referencia. Para ver la lista de regiones CloudTrail compatibles, consulteCloudTrail regiones compatibles.

  Si el registro de la organización es multirregional y la región de origen es una región opcional, las cuentas de los miembros no enviarán la actividad al registro de la organización a menos que opten por hacerlo en el Región de AWS lugar en el que se creó el registro multirregional. Por ejemplo, si creas una ruta multirregional y eliges la región de Europa (España) como región de origen de la ruta, solo las cuentas de los miembros que hayan habilitado la región de Europa (España) en su cuenta enviarán la actividad de su cuenta a la ruta de la organización. Para resolver el problema, habilita la región de suscripción en cada cuenta de miembro de tu organización. Para obtener información sobre cómo habilitar una región de suscripción voluntaria, consulte Habilitar o deshabilitar una región de su organización en la Guía de AWS Account Management referencia.
- Compruebe si la política de la organización basada en los recursos entra en conflicto con la política de funciones vinculadas al servicio CloudTrail

  CloudTrail usa el rol vinculado al servicio denominado para respaldar los registros de la organización. `AWSServiceRoleForCloudTrail` Este rol vinculado al servicio permite realizar acciones sobre CloudTrail los recursos de la organización, por ejemplo: `organizations:DescribeOrganization` Si la política basada en los recursos de la organización deniega una acción que está permitida en la política de funciones vinculadas al

servicio, no CloudTrail podrá realizar la acción aunque esté permitida en la política de funciones vinculadas al servicio. Para resolver el problema, corrija la política basada en los recursos de la organización para que no deniegue las acciones que están permitidas en la política de funciones vinculadas al servicio.

CloudTrail no envía notificaciones de Amazon SNS para una cuenta de miembro de una organización

Si una cuenta de miembro con un registro de AWS Organizations la organización no envía notificaciones de Amazon SNS, podría haber un problema con la configuración de la política de temas de Amazon SNS. CloudTrail crea registros organizativos en las cuentas de los miembros incluso si se produce un error en la validación de un recurso; por ejemplo, el tema de SNS del registro de la organización no incluye todos los ID de las cuentas de los miembros. Si la política de temas de SNS es incorrecta, se produce un error de autorización.

Para comprobar si la política de temas de SNS de una ruta tiene un error de autorización:

- Desde la CloudTrail consola, consulta la página de detalles del sendero. Si se produce un error en la autorización, la página de detalles incluye una advertencia `SNS authorization failed` e indica que hay que corregir la política de temas de SNS.
- Desde AWS CLI, ejecute el get-trail-statuscomando. Si se produce un error de autorización, el resultado del comando incluye el `LastNotificationError` campo con un valor de`AuthorizationError`. Para resolver el problema, corrija la política de temas de Amazon SNS. Para obtener información sobre la política temática de Amazon SNS, consulte. Política temática de Amazon SNS para CloudTrail

Para obtener más información sobre los temas de SNS y suscribirse a ellos, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Visualizar eventos de CloudTrail Insights para registros de seguimiento

Después de habilitar CloudTrail Insights en un registro de seguimiento, puede ver hasta 90 días de eventos de Insights mediante la consola de CloudTrail o la AWS CLI. En esta sección se describe cómo ver, buscar y descargar un archivo de eventos de Insights. A fin de obtener más información sobre el uso de la API `LookupEvents` para recuperar información de los eventos de CloudTrail,

consulte la Referencia de la API de AWS CloudTrail. Para obtener más información sobre CloudTrail Insights, consulte Registro de eventos de Insights en esta guía.

Para obtener más información acerca de cómo crear y administrar una traza, consulte Creación de un registro de seguimiento y Obtención y visualización de archivos de registros de CloudTrail.

> **Note**
>
> Para registrar los eventos de Insights sobre el volumen de llamadas de la API, el registro de seguimiento debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el registro de seguimiento debe registrar los eventos de administración de `read` o `write`.

Temas

- Visualizar eventos de CloudTrail Insights para registros de seguimiento en la consola de CloudTrail
- Visualización de eventos de CloudTrail Insights para senderos con el AWS CLI

Visualizar eventos de CloudTrail Insights para registros de seguimiento en la consola de CloudTrail

Después de habilitar eventos de CloudTrail Insights en una traza, cuando CloudTrail detecta una actividad de tasa de error o API, CloudTrail genera eventos de Insights y los muestra en las páginas Dashboard (Panel) e Insights en la AWS Management Console. Puede ver los eventos de Insights en la consola y solucionar los problemas de la actividad inusual. En la consola se muestran los 90 días más recientes de los eventos de Insights. También puede descargar los eventos de Insights mediante la consola de AWS CloudTrail. Puede buscar eventos mediante programación con los SDK de AWS o AWS Command Line Interface. Para obtener más información sobre los eventos de CloudTrail Insights, consulte Registro de eventos de Insights en esta guía.

> **Note**
>
> Para registrar los eventos de Insights sobre el volumen de llamadas de la API, el registro de seguimiento debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el registro de seguimiento debe registrar los eventos de administración de `read` o `write`.

Una vez registrados los eventos de Insights, estos se muestran en la página Insights durante 90 días. No se pueden eliminar manualmente eventos de la página Insights . Como debe crear un registro de seguimiento para poder habilitar CloudTrail Insights, puede ver los eventos de Insights registrados en su registro de seguimiento siempre y cuando los almacene en el bucket de S3 establecidos en la configuración del registro de seguimiento.

Monitoree sus registros de seguimiento y reciba notificaciones cuando se produzcan eventos de Insights específicos con Amazon CloudWatch Logs. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Para ver eventos de Insights

Los eventos de CloudTrail Insights deben habilitarse en su registro de seguimiento para ver los eventos de Insights en la consola. Espere hasta 36 horas para que CloudTrail pueda enviar los primeros eventos de Insights, si se detecta actividad inusual.

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/home/.
2. En el panel de navegación, elija Dashboard (Panel) para ver los cinco eventos de Insights más recientes o Insights a fin de ver todos los eventos de Insights registrados en su cuenta en los últimos 90 días.

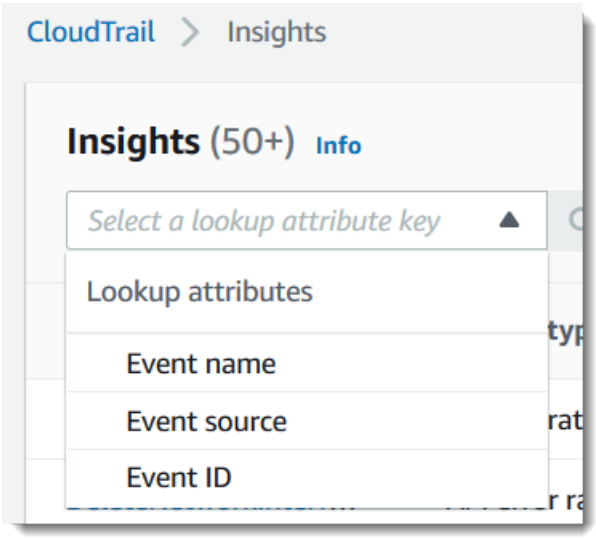
   En la página Insights puede filtrar los eventos de Insights por criterios como el origen de la API de eventos, el nombre del evento y el ID del evento, y limitar los eventos mostrados a los que se producen dentro de un intervalo de tiempo específico. Para obtener más información sobre el filtrado de eventos de Insights, consulte Filtrado de eventos de Insights.

Contenido

- Filtrado de eventos de Insights
- Visualice los detalles de eventos de Insights
- Aplicar zoom al gráfico, desplazarlo y descargarlo
- Cambiar la configuración del intervalo de tiempo del gráfico
- Descarga de eventos de Insights

Filtrado de eventos de Insights

La visualización predeterminada de eventos en Insights muestra los eventos en orden cronológico inverso. Los eventos de Insights más recientes, ordenados por hora de inicio del evento, se encuentran en la parte superior. En la lista siguiente se describen los atributos disponibles. Se pueden filtrar los tres primeros atributos: Event name (Nombre del evento), Event source (Origen del evento) y Event ID (ID de evento).



Nombre de evento

El nombre del evento, normalmente la API de AWS en la que se registraron niveles inusuales de actividad.

Tipo de información

El tipo de evento de Insights de CloudTrail, que es la tasa de llamadas a la API o la tasa de errores de la API. El tipo de información sobre la tasa de llamadas a la API analiza las llamadas a la API de administración de solo escritura que se agregan por minuto en comparación con un volumen de llamadas a la API de referencia. El tipo de información sobre la tasa de errores de la API analiza las llamadas a la API de administración que generan códigos de error. El error se muestra si la llamada a la API no se hace correctamente.

Origen del evento

El servicio de AWS para el que se ha realizado la solicitud, como `iam.amazonaws.com` o `s3.amazonaws.com`. Puede desplazarse por una lista de orígenes de eventos después de elegir el filtro Event source.

ID de evento

El ID del evento de Insights. Los ID de evento no se muestran en la tabla de la página de Insights, pero son un atributo por el que puede filtrar los eventos de Insights. Los ID de evento de los eventos de administración que se analizan para generar eventos de Insights son diferentes de los ID de evento de los eventos de Insights.

Hora de inicio del evento

Hora de inicio del evento de Insights, medido como el primer minuto en el que se registró actividad inusual. Este atributo se muestra en la tabla Insights, pero no puede filtrar la hora de inicio del evento en la consola.

Promedio de referencia

El patrón normal de actividad de tasa de error o de llamadas a API. El promedio de referencia se calcula a lo largo de los siete días anteriores al inicio de un evento de Insights. Aunque el valor de referencia de la duración (el periodo que analiza CloudTrail para la actividad normal en las API) es de aproximadamente siete días, CloudTrail redondea la duración de referencia a un día entero, por lo que la duración de referencia exacta puede variar.

Promedio de Insight

El número promedio de llamadas a una API, o el número promedio de un error específico que se devolvió en las llamadas a una API, que desencadenó el evento Insights. El promedio de CloudTrail Insights del evento de inicio es la tasa de ocurrencias que desencadenó el evento de Insights. Por lo general, este es el primer minuto de actividad inusual. El promedio de Insights del evento de finalización es la tasa de ocurrencias durante la actividad inusual, entre el evento de Insights de inicio y el evento de Insights de finalización.

Cambio de tasa

La diferencia entre el valor de Promedio de referencia y Promedio de Insight, medido en porcentaje. Por ejemplo, si el promedio de referencia de un error `AccessDenied` que se produce es 1,0, y el promedio de Insight es 3,0, el cambio de tasa es del 300 %. Un cambio de tasa para un promedio de Insight que supera un promedio de referencia muestra una flecha hacia arriba junto al valor. Si el evento Insights se registró porque la actividad está por debajo del promedio de referencia, Cambio de tasa muestra una flecha hacia abajo junto al porcentaje.

Si no hay eventos registrados para el atributo o el tiempo elegidos, la lista de resultados estará vacía. Solo puede aplicar un filtro de atributo además del intervalo de tiempo. Si elige un atributo diferente, se mantiene el filtro de intervalo de tiempo especificado.

Los siguientes pasos describen cómo filtrar por atributo.

Para filtrar por atributo

1. Para filtrar los resultados por atributo, elija un atributo de búsqueda en el menú desplegable y, a continuación, escriba o elija un valor en el cuadro Enter a lookup value (Ingresar un valor de búsqueda).
2. Para eliminar un filtro de atributo, elija la X situada a la derecha del cuadro de filtro de atributo.

Los siguientes pasos describen cómo filtrar por una fecha y una hora de inicio y finalización.

Para filtrar por una fecha y hora de inicio y finalización

1. Para reducir el intervalo de tiempo de los eventos que desea ver, seleccione un intervalo de tiempo en la barra de intervalo de tiempo en la parte superior de la tabla. Los intervalos de tiempo preestablecidos incluyen 30 minutos, 1 hora, 3 horas o 12 horas. Para especificar un intervalo de tiempo personalizado, elija Custom (Personalizado).
2. Elija una de las siguientes pestañas:
   - Absolute (Absoluto): permite elegir una hora específica. Continúe con el paso siguiente.
   - Relative to selected event (Relativo al evento seleccionado): seleccionada de forma predeterminada. Permite elegir un periodo de tiempo relativo a la hora de inicio de un evento de Insights. Continúe con el paso 4.
3. Para establecer un rango de tiempo Absolute (Absoluto), haga lo siguiente.
   a. En la pestaña Absolute (Absoluto), elija el día en el que desea que comience el intervalo de tiempo. Ingrese una hora de inicio en el día seleccionado. Para ingresar una fecha de forma manual, escriba la fecha con el formato `yyyy/mm/dd`. Las horas de inicio y finalización siguen el formato de 24 horas y los valores deben tener el formato `hh:mm:ss`. Por ejemplo, para que la hora de inicio sea a las 6:30 p. m., ingrese **`18:30:00`**.
   b. Elija una fecha de finalización para el intervalo en el calendario o especifique una fecha y hora de finalización debajo del calendario. Seleccione Aplicar.
4. Para establecer un intervalo de tiempo Relative to selected event (Relativo al evento seleccionado), haga lo siguiente.

a. Elija un periodo de tiempo predefinido relativo a la hora de inicio de los eventos de Insights. Los valores predefinidos se encuentran disponibles en minutos, horas, días o semanas. El periodo de tiempo relativo máximo es de 12 semanas.

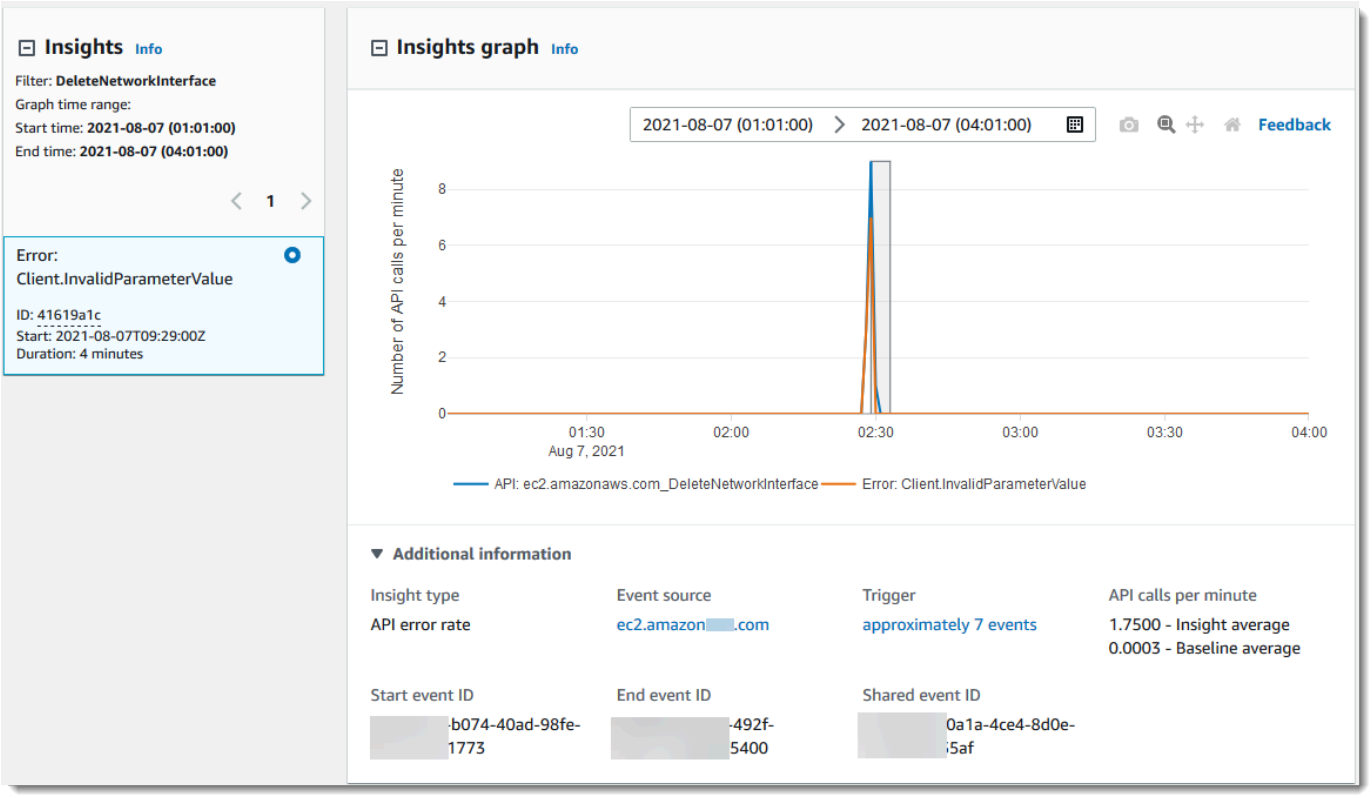
b. Si es necesario, personalice el valor predefinido en los cuadros situados debajo de los ajustes predefinidos. Elija Clear (Borrar) para restablecer los cambios si es necesario. Cuando haya establecido la hora relativa que desea, elija Apply (Aplicar).

5. En To (Hasta), elija el día y especifique la hora a la que desea que termine el intervalo de tiempo. Seleccione Aplicar.

6. Para eliminar un filtro de intervalo de tiempo, elija el icono de calendario situado a la derecha del cuadro Time range (Intervalo de tiempo) y, a continuación, elija Remove (Eliminar).

Visualice los detalles de eventos de Insights

1. Elija un evento de Insights de la lista de resultados para mostrar sus detalles. La página de detalles de un evento de Insights muestra un gráfico de la línea de tiempo de la actividad inusual.



2. Coloque el cursor sobre las bandas resaltadas para mostrar la hora de inicio y duración de cada evento de Insights en el gráfico.

La siguiente información se muestra en el área Información adicional del gráfico:

- Insight type (Tipo de información). Puede ser la tasa de llamadas a la API o la tasa de error de la API.
- Desencadenador. Este es un enlace a la pestaña Cloudtrail events (Eventos de Cloudtrail), que presenta los eventos de administración que se analizaron para determinar que se produjo una actividad inusual.
- Llamadas a la API por minuto
  - Baseline average (Promedio de referencia): la tasa típica de ocurrencias por minuto a esta API en la que se registró el evento Insights, medido en aproximadamente los siete días anteriores, en una región específica de su cuenta.
  - Insights average (Promedio de Insights): la tasa de ocurrencias por minuto a esta API que desencadenaron el evento de Insights. El promedio de CloudTrail Insights del evento de inicio es la tasa de llamadas o errores por minuto a la API que desencadenó el evento de Insights. Por lo general, este es el primer minuto de actividad inusual. El promedio de Insights del evento final es el porcentaje de llamadas o errores por minuto a la API durante la actividad inusual, entre el evento de Insights inicial y el evento de Insights final.
- Fuente del evento. El punto de conexión de servicio de AWS en el que se llevó a cabo el número inusual de llamadas a la API. En la imagen anterior, el origen es `ec2.amazonaws.com`, que es el punto de conexión de servicio de Amazon EC2.
- Event IDs (Id. de evento)
  - Start event ID (ID de evento de inicio): el ID del evento de Insights que registró al principio de una actividad inusual.
  - End event ID (ID de evento de finalización): ID del evento Insights que se registró al final de una actividad inusual.
  - Shared event ID (ID de evento compartido): en los eventos de Insights, el ID de evento compartido es un GUID generado por CloudTrail Insights para identificar de forma exclusiva un par de eventos de Insights inicial y final. Shared event ID (ID de evento compartido) es igual en los eventos de inicio y finalización de Insights, y ayuda a relacionar ambos eventos para identificar de forma inequívoca la actividad inusual.

3. Elija la pestaña Attributions (Atribuciones) para ver información sobre las identidades de usuario, los agentes de usuario y sobre eventos de Insight de la tasa de llamadas a la API, códigos

de error correlacionados con la actividad inusual y de referencia. Se muestra un máximo de cinco identidades de usuario, cinco agentes de usuario y cinco códigos de error en las tablas de la pestaña Attributions (Atribuciones), ordenado por un promedio del recuento de la actividad, en orden descendente de mayor a menor. Para obtener más información sobre la pestaña Attributions (Atribuciones), consulte Pestaña Atributions (Atribuciones) y Elemento `insightDetails` CloudTrail Insights en esta guía.

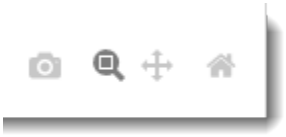
4. En la pestaña CloudTrail events (Eventos de CloudTrail), vea los eventos relacionados que CloudTrail analizó para determinar que se produjo una actividad inusual. De forma predeterminada, ya se aplica un filtro para el nombre del evento de Insights, que también es el nombre de la API relacionada. La pestaña CloudTrail events (Eventos de CloudTrail) muestra los eventos de administración de CloudTrail relacionados con la API en cuestión que se produjeron entre la hora de inicio (menos un minuto) y finalización (más un minuto) del evento de Insights.

   A medida que selecciona otros eventos de Insights en el gráfico, cambian los eventos que se muestran en la tabla CloudTrail events (Eventos de CloudTrail). Estos eventos le ayudan a realizar un análisis más detallado para determinar la causa probable de un evento de Insights y las razones de la actividad inusual de la API.

   Para mostrar todos los eventos de CloudTrail registrados durante la duración del evento Insights y no solo los de la API relacionada, desactive el filtro.
5. Elija la pestaña Insights event record (Registro de eventos de Insights) para ver los eventos de inicio y finalización de Insights en formato JSON.
6. Al elegir el enlace Event source (Origen de eventos), se lo redirige a la página Insights filtrada por ese origen de eventos.

Aplicar zoom al gráfico, desplazarlo y descargarlo

Puede acercar o alejar, desplazar y restablecer los ejes del gráfico en la página de detalles del evento de Insights mediante la barra de herramientas situada en la esquina superior derecha.



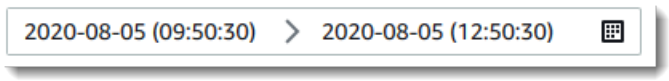
De izquierda a derecha, los botones de la barra de herramientas de gráficos hacen lo siguiente:

- Download plot as a PNG (Descargar gráfico como PNG): descarga la imagen del gráfico mostrada en la página de detalles y la guarda en formato PNG.

- Zoom: arrastre para seleccionar el área del gráfico que desea ampliar y ver con mayor detalle.
- Pan (Desplazamiento panorámico): desplace el gráfico para ver fechas u horas adyacentes.
- Reset axes (Restablecer ejes): revierta los ejes del gráfico a los originales borrando los ajustes de zoom y desplazamiento panorámico.

Cambiar la configuración del intervalo de tiempo del gráfico

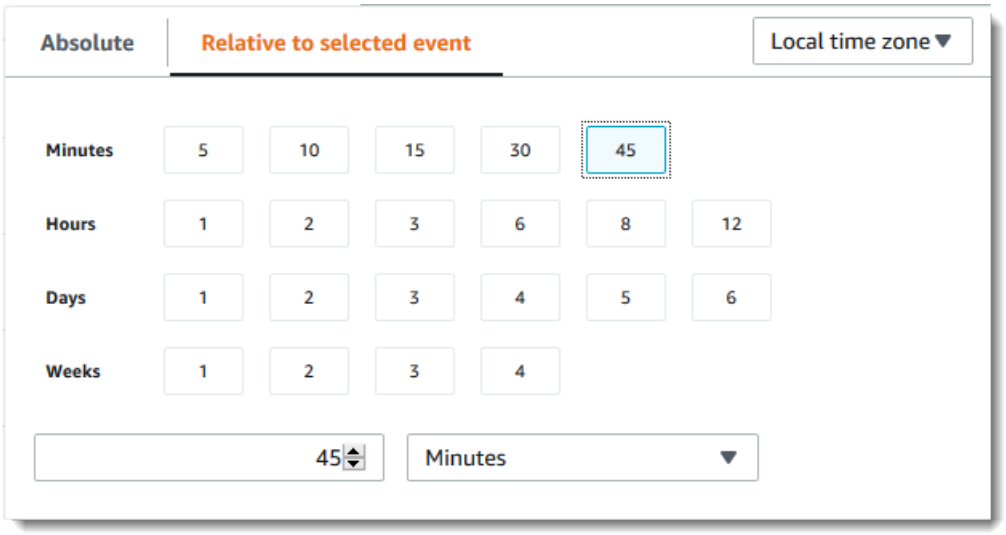
Puede cambiar el intervalo de tiempo (la duración seleccionada de los eventos que se muestran en el eje x) que se muestra en el gráfico al elegir una configuración en la esquina superior derecha del gráfico.



El intervalo de tiempo predeterminado que se muestra en el gráfico depende de la duración del evento de Insights seleccionado.

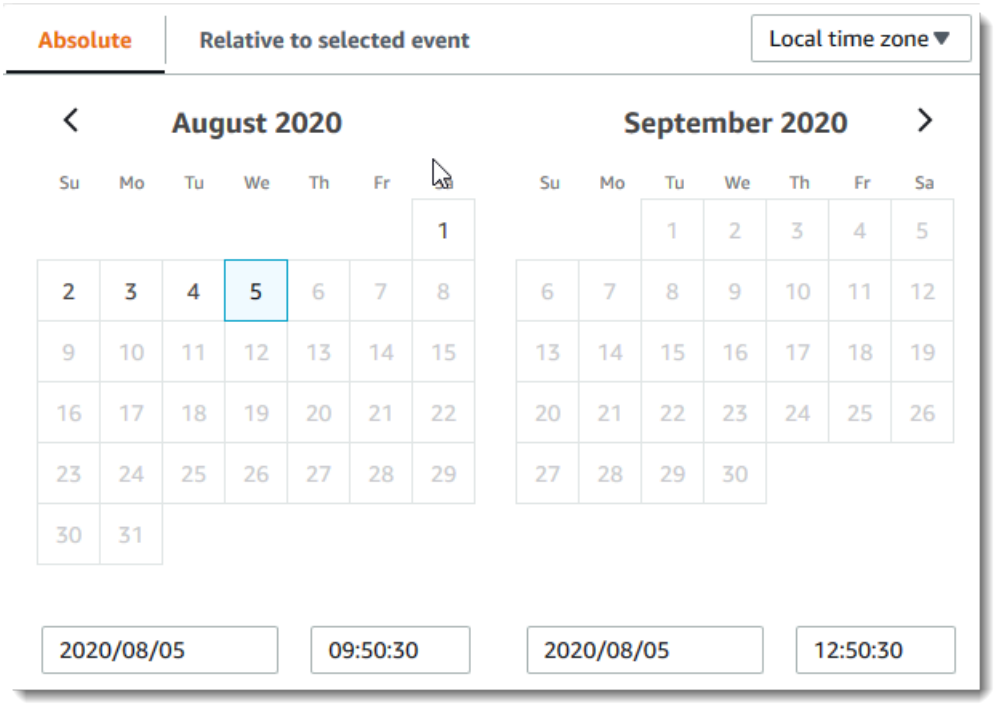
Duración del evento de Insights	Periodo de tiempo predeterminado
Menos de 4 horas	3h (tres horas)
Entre 4 y 12 horas	12h(12 horas)
Entre 12 y 24 horas	1d (un día)
Entre 24 y 72 horas	3d (tres días)
Más de 72 horas	1w (una semana)

Puede elegir ajustes predefinidos de cinco minutos, 30 minutos, una hora, tres horas, 12 horas o Custom (Personalizado). En la siguiente imagen se muestran los periodos de tiempo Relative to selected event (Relativo al evento seleccionado) que puede elegir en la configuración Custom (Personalizado). Los periodos de tiempo relativos son periodos de tiempo aproximados cercanos al inicio y al final del evento de Insights seleccionado que se muestra en una página de detalles del evento de Insights.



Para personalizar un ajuste predefinido seleccionado, especifique un número y una unidad de tiempo en los cuadros situados debajo de los ajustes predefinidos.

Para especificar una fecha y un intervalo de tiempo exactos, seleccione la pestaña Absolute (Absoluto). Si establece un intervalo de fecha y hora absolutos, se requieren las horas de inicio y finalización. Para obtener información sobre cómo establecer la hora, consulte the section called "Filtrado de eventos de Insights" en este tema.



Descarga de eventos de Insights

Puede descargar el historial de eventos de Insights registrados como un archivo en formato JSON o CSV. Utilice filtros e intervalos de tiempo para reducir el tamaño del archivo que descargue.

> **Note**
>
> Los archivos de historial de eventos de CloudTrail son archivos de datos que contienen información (como nombres de recursos) que pueden configurar los usuarios. Algunos de estos datos podrían ser interpretados como comandos en los programas que se utilizan para leer y analizar esta información (inyección CSV). Por ejemplo, cuando se exportan eventos de CloudTrail a CSV y se importan a un programa de hoja de cálculo, este programa podría advertirle sobre problemas de seguridad. Como práctica recomendada de seguridad, deshabilite los enlaces o las macros de los archivos del historial de eventos descargados.

1. Especifique el filtro y el intervalo de tiempo de los eventos que desee descargar. Por ejemplo, puede especificar el nombre del evento, `StartInstances`, y un intervalo de tiempo de los tres últimos días de actividad.
2. Elija Download events (Descargar eventos) y, a continuación, elija Download CSV (Descargar CSV) o Download JSON (Descargar JSON). Se le pedirá que elija una ubicación para guardar el archivo.

   > **Note**
   >
   > La descarga podría tardar un tiempo en terminar. Antes de iniciar el proceso de descarga, y para obtener resultados más rápidos, utilice un filtro más específico o un intervalo de tiempo más breve para limitar los resultados.

3. Cuando haya finalizado la descarga, abra el archivo para ver los eventos que ha especificado.
4. Para cancelar la descarga, elija Cancel download (Cancelar descarga). Si cancela una descarga antes de que termine, es posible que un archivo CSV o JSON de la computadora local solo contenga parte de sus eventos.

Visualización de eventos de CloudTrail Insights para senderos con el AWS CLI

Puede buscar los eventos de CloudTrail Insights de los últimos 90 días ejecutando el aws cloudtrail lookup-events comando. El comando `lookup-events` tiene las siguientes opciones:

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

Para obtener información general sobre el uso del AWS Command Line Interface, consulte la Guía del AWS Command Line Interface usuario.

Contenido

- Requisitos previos
- Obtener ayuda de la línea de comandos
- Búsqueda de eventos de Insights
- Especificación del número de eventos de Insights que se devuelven
- Búsqueda de eventos de Insights por intervalo de tiempo
- Búsqueda de eventos de Insights por atributo
  - Ejemplos de búsqueda de atributos
- Especificar la siguiente página de resultados
- Obtener datos de entrada JSON de un archivo
- Campos de resultados de búsqueda

Requisitos previos

- Para ejecutar AWS CLI comandos, debe instalar el AWS CLI. Para obtener más información, consulte Instalación de la interfaz de línea de AWS comandos.
- Asegúrese de que su AWS CLI versión sea posterior a la 1.6.6. Para comprobar la versión de la CLI, ejecute aws --version en la línea de comandos.
- Para configurar la cuenta, la región y el formato de salida predeterminado de una AWS CLI sesión, utilice el aws configure comando. Para obtener más información, consulte Configuración de la interfaz de línea de comandos de AWS.
- Para registrar los eventos de Insights sobre el volumen de llamadas de la API, el registro de seguimiento debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el registro de seguimiento debe registrar los eventos de administración de `read` o `write`.

> **Note**
>
> Los CloudTrail AWS CLI comandos distinguen mayúsculas de minúsculas.

Obtener ayuda de la línea de comandos

Para ver la ayuda de la línea de comandos de `lookup-events`, escriba el siguiente comando.

```
aws cloudtrail lookup-events help
```

Búsqueda de eventos de Insights

Para ver los diez últimos eventos de Insights, escriba el siguiente comando.

```
aws cloudtrail lookup-events --event-category insight
```

Un evento devuelto es similar al siguiente ejemplo,

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
```

```
            "eventVersion": "1.07",
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
```

```
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "userAgent",
                  "insight": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "errorCode",
                  "insight": [
                    {
                      "value": "null",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "null",
                      "average": 0.0000882145
                    }
                  ]
                }
              ]
            }
          },
            "eventCategory": "Insight"
        },
        {
            "eventVersion": "1.07",
```

```
            "eventTime": "2019-10-15T21:14:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "End",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
```

```
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      }
  ]
}
```

Para obtener una explicación de los campos relacionados con la búsqueda en el resultado, consulte Campos de resultados de búsqueda sobre este tema. Para obtener una explicación de los campos del evento de Insights, consulte CloudTrail contenido del registro.

Especificación del número de eventos de Insights que se devuelven

Para especificar el número de eventos que se devuelven, escriba el siguiente comando:

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

El valor predeterminado de *<entero>*, si no se especifica, es 10. Los valores posibles comprenden del 1 al 50. El ejemplo siguiente devuelve un solo resultado.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

Búsqueda de eventos de Insights por intervalo de tiempo

Se pueden buscar eventos de Insights de los últimos 90 días. Para especificar un intervalo de tiempo, escriba el siguiente comando.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>* especifica, en UTC, que solo se devuelvan los eventos de Insights que se producen en el tiempo especificado o con posterioridad. Si la fecha de inicio especificada es posterior a la fecha de finalización especificada, se devuelve un error.

`--end-time` *<timestamp>* especifica, en UTC, que solo se devuelvan los eventos de Insights que se producen en el tiempo especificado o con anterioridad. Si la fecha de finalización especificada es anterior a la fecha de inicio especificada, se devuelve un error.

La fecha de inicio predeterminada es la primera fecha posible en que los datos están disponibles en los últimos 90 días. La fecha de finalización predeterminada es la fecha del evento que se produjo más cercana a la fecha actual.

Todas las marcas temporales se muestran en UTC.

Búsqueda de eventos de Insights por atributo

Para filtrar por un atributo, escriba el siguiente comando.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Solo puede especificar un atributo de pares de clave-valor para cada comando lookup-events. Los siguientes son valores válidos de eventos de Insights para `AttributeKey`. Los nombres de los valores distinguen entre mayúsculas y minúsculas.

- `EventId`
- `EventName`
- `EventSource`

La longitud máxima para el `AttributeValue` es de 2000 caracteres. Los siguientes caracteres ('_', '', , '\\n') cuentan como dos caracteres dentro del límite de 2000 caracteres.

Ejemplos de búsqueda de atributos

El siguiente comando de ejemplo devuelve los eventos de Insights en los que el valor de `EventName` es `PutRule`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

El siguiente comando de ejemplo devuelve los eventos de Insights en los que el valor de `EventId` es `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

El siguiente comando de ejemplo devuelve los eventos de Insights en los que el valor de `EventSource` es `iam.amazonaws.com`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

Especificar la siguiente página de resultados

Para obtener la siguiente página de resultados de un comando `lookup-events`, escriba el siguiente comando.

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

En este comando, el valor de *<token>* se obtiene del primer campo del resultado del comando anterior.

Cuando utiliza `--next-token` en un comando, debe utilizar los mismos parámetros que en el comando anterior. Suponga, por ejemplo, que ejecuta el siguiente comando.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Para obtener la siguiente página de resultados, el siguiente comando sería similar a este.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

Obtener datos de entrada JSON de un archivo

AWS CLI Para algunos AWS servicios, `--generate-cli-skeleton` tiene dos parámetros: uno`--cli-input-json`, uno puede usarlo para generar una plantilla JSON, que puede modificar y usar como entrada para el `--cli-input-json` parámetro. En esta sección se describe cómo utilizar estos parámetros con `aws cloudtrail lookup-events`. Para obtener más información, consulte el tema sobre cómo generar parámetros JSON CLI Skeleton y CLI Input.

Para buscar eventos de Insights al obtener los datos de entrada JSON de un archivo

1. Cree una plantilla de entrada para usarla con `lookup-events` redirigiendo el resultado de `--generate-cli-skeleton` a un archivo, como En el ejemplo siguiente.

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   El archivo de plantilla generado (en este caso, LookupEvents .txt) tiene el siguiente aspecto.

   ```
   {
   ```

```
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Utilice un editor de texto para modificar los datos JSON según sea necesario. Los datos de entrada JSON solo deben contener los valores que se especifican.

> **Important**
>
> Todos los valores vacíos o null deben eliminarse de la plantilla antes de utilizarla.

El ejemplo siguiente especifica un intervalo de tiempo y un número máximo de resultados que se devuelven.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Para utilizar el archivo editado como entrada, use la sintaxis `--cli-input-json file://<nombreArchivo>`, como en el ejemplo siguiente.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> Puede utilizar otros argumentos en la misma línea de comandos como `--cli-input-json`.

Campos de resultados de búsqueda

Eventos

Una lista de eventos de búsqueda en función del atributo de búsqueda y el intervalo de tiempo especificados. La lista de eventos se ordena por tiempo, con el último evento en primer lugar. Cada entrada contiene información sobre la solicitud de búsqueda e incluye una cadena que representa el CloudTrail evento que se recuperó.

Las siguientes entradas describen los campos de cada evento de búsqueda.

CloudTrailEvent

Una cadena JSON que contiene una representación de objeto del evento devuelto. Para obtener información sobre cada uno de los elementos devueltos, consulte la información sobre el contenido del cuerpo del registro.

EventId

Una cadena que contiene el GUID del evento devuelto.

EventName

Una cadena que contiene el nombre del evento devuelto.

EventSource

El AWS servicio al que se realizó la solicitud.

EventTime

La fecha y la hora, en formato de tiempo UNIX, del evento.

Recursos

Una lista de los recursos a los que hace referencia el evento devuelto. Cada entrada de recurso especifica un tipo de recurso y un nombre de recurso.

ResourceName

Una cadena que contiene el nombre del recurso al que hace referencia el evento.

ResourceType

Una cadena que contiene el tipo de recurso al que hace referencia el evento. Cuando el tipo de recurso no se puede determinar, se devuelve null.

Nombre de usuario

Una cadena que contiene el nombre de usuario de la cuenta del evento devuelto.

NextToken

Una cadena para obtener la siguiente página de resultados de un comando `lookup-events` anterior. Para utilizar el token, los parámetros deben ser los mismos que los del comando original. Si no aparece ninguna entrada `NextToken` en la salida, no hay más resultados que devolver.

Para obtener más información sobre los eventos de CloudTrail Insights, consulte Registro de eventos de Insights esta guía.

Copiar los eventos del sendero al CloudTrail lago

Puede copiar los eventos de senderos existentes a un banco de datos de eventos de CloudTrail Lake para crear una point-in-time instantánea de los eventos registrados en el sendero. Copiar eventos de registro de seguimiento no interfiere con la capacidad del registro de seguimiento para registrar eventos y no modifica el registro de seguimiento de ninguna manera.

Puede copiar los eventos de los senderos a un banco de datos de eventos existente configurado para CloudTrail eventos, o puede crear un nuevo banco de datos de CloudTrail eventos y elegir la opción Copiar los eventos de los senderos como parte de la creación del banco de datos de eventos. Para obtener más información acerca de cómo copiar eventos de registros de seguimiento en un almacén de datos de eventos existente, consulte Copie los eventos de seguimiento a un almacén de datos de eventos existente mediante la consola CloudTrail . Para obtener más información acerca de la creación de un nuevo almacén de datos de eventos, consulte Cree un banco de datos de CloudTrail eventos para eventos.

Al copiar los eventos de los senderos a un banco de datos de eventos de CloudTrail Lake, puede realizar consultas sobre los eventos copiados. CloudTrail Las consultas de Lake ofrecen una visión más profunda y personalizable de los eventos que las simples búsquedas de claves y valores en el historial de eventos o en curso. `LookupEvents` Para obtener más información sobre CloudTrail Lake, consulte. Trabajando con AWS CloudTrail Lake

Si va a copiar los eventos de registro de seguimiento en el almacén de datos de eventos de una organización, debe utilizar la cuenta de administración de la organización. No puede copiar los eventos de registro de seguimiento con la cuenta del administrador delegado de una organización.

CloudTrail Los almacenes de datos de eventos de Lake incurren en cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener información sobre CloudTrail los precios y la administración de los costos de Lake, consulte AWS CloudTrail Precios yGestión de los costos CloudTrail del lago.

Cuando copias los eventos de los senderos a un banco de datos de eventos de CloudTrail Lake, incurres en cargos en función de la cantidad de datos sin comprimir que ingiera el almacén de datos de eventos.

Al copiar los eventos de los senderos en CloudTrail Lake, se CloudTrail descomprimen los registros almacenados en formato gzip (comprimido) y, a continuación, se copian los eventos contenidos en los registros en el almacén de datos de eventos. El tamaño de los datos sin comprimir podría ser mayor que el tamaño real del almacenamiento de S3. Para obtener una estimación general del tamaño de los datos sin comprimir, puede multiplicar por 10 el tamaño de los registros del bucket de S3.

Puede reducir los costos especificando un intervalo de tiempo más reducido para los eventos copiados. Si planea usar solo el almacén de datos de eventos para consultar los eventos copiados, puede desactivar la ingesta de eventos para evitar generar cargos por eventos futuros. Para obtener más información, consulte Precios de AWS CloudTrail y Gestión de los costos CloudTrail del lago.

Escenarios

En la siguiente tabla, se describen algunos escenarios habituales para copiar eventos de registros de seguimiento y cómo seguir cada uno de ellos mediante la consola.

Escenario	¿Cómo puedo lograr esto en la consola?
Analiza y consulta los eventos históricos de los senderos de CloudTrail Lake sin ingerir nuevos eventos	Cree un nuevo almacén de datos de eventos y seleccione la opción Copiar eventos de registros de seguimiento como parte de la creación del almacén de datos de eventos. Al crear el almacén de datos de eventos, desmarque Incorporar eventos (paso 15 del procedimiento) para garantizar que el almacén de datos de eventos contenga solo los eventos históricos del registro de seguimiento y no los eventos futuros.

Escenario	¿Cómo puedo lograr esto en la consola?
Sustituya su sendero actual por un almacén de datos de eventos de CloudTrail Lake	Cree un almacén de datos de eventos con los mismos selectore s de eventos que el registro de seguimiento para asegurarse de que el almacén de datos de eventos tenga la misma cobertura que el registro de seguimiento. Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de fecha para los eventos copiados que sea anterior a la creación del almacén de datos de eventos. Después de crear el almacén de datos de eventos, puede desactivar el registro del registro de seguimiento para evitar cargos adicionales.

Temas

- Consideraciones para copiar eventos de registros de seguimiento
- Permisos necesarios para copiar eventos de registro de seguimiento
- Copie los eventos de seguimiento a un almacén de datos de eventos existente mediante la consola CloudTrail

Consideraciones para copiar eventos de registros de seguimiento

Tenga en cuenta los siguientes factores al copiar eventos de registro de seguimiento.

- Al copiar los eventos de las rutas, CloudTrail utiliza la operación de la `GetObject`API de S3 para recuperar los eventos de las rutas del depósito de S3 de origen. Hay algunas clases de almacenamiento archivado de S3, como S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts y S3 Intelligent-Tiering Deep Archive, a las que no puede acceder con `GetObject`. Para copiar los eventos de registros de seguimiento almacenados en estas clases de almacenamiento archivado, primero debe restaurar una copia mediante la operación `RestoreObject` de S3. Para obtener información sobre la restauración de objetos archivados, consulte Restauración de objetos archivados en la Guía del usuario de Amazon S3.

- Al copiar los eventos de seguimiento a un banco de datos de eventos, CloudTrail copia todos los eventos de seguimiento, independientemente de la configuración de los tipos de eventos del banco de datos de eventos de destino, de los selectores de eventos avanzados o Región de AWS.
- Antes de copiar los eventos del registro de seguimiento a un almacén de datos de eventos existente, asegúrese de que la opción de precios y el periodo de retención del almacén de datos de eventos estén configurados adecuadamente para su caso de uso.
  - Opción de precios: la opción de precios determina el costo de la incorporación y el almacenamiento de los eventos. Para obtener más información sobre las opciones de precios, consulte Precios de AWS CloudTrail y Opciones de precios del almacén de datos de eventos.
  - Período de retención: el período de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos del evento. CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Para determinar el período de retención adecuado, calcula la suma del evento más antiguo que deseas copiar en días y el número de días que deseas conservar los eventos en el almacén de datos del evento (período de retención = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.
- Si está copiando eventos de registros de seguimiento en un almacén de datos de eventos para investigarlos y no desea incorporar ningún evento futuro, puede detener la incorporación en el almacén de datos de eventos. Al crear el almacén de datos de eventos, desmarque la opción Incorporar eventos (paso 15 del procedimiento) para garantizar que el almacén de datos de eventos contenga solo los eventos históricos del registro de seguimiento y no los eventos futuros.
- Antes de copiar los eventos de registro de seguimiento, desactive cualquier lista de control de acceso (ACL) adjunta al bucket de S3 de origen y actualice la política de buckets de S3 para el almacén de datos de eventos de destino. Para obtener más información sobre la actualización de la política de buckets de S3, consulte Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento. Para obtener más información sobre la desactivación de las ACL, consulte Control de la propiedad de los objetos y desactivación de las ACL del bucket.
- CloudTrail solo copia los eventos de seguimiento de los archivos de registro comprimidos con Gzip que se encuentran en el depósito S3 de origen. CloudTrail no copia los eventos de seguimiento de archivos de registro sin comprimir ni de archivos de registro que se comprimieron con un formato que no sea Gzip.

- Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de tiempo para los eventos copiados que sea anterior a la creación del almacén de datos de eventos.
- De forma predeterminada, CloudTrail solo copia CloudTrail los eventos contenidos en el prefijo del bucket de S3 y los `CloudTrail` prefijos incluidos en el prefijo, y no comprueba los `CloudTrail` prefijos de otros servicios. AWS Si desea copiar los CloudTrail eventos incluidos en otro prefijo, debe elegir el prefijo al copiar los eventos de seguimiento.
- Para copiar los eventos de registro de seguimiento en el almacén de datos de eventos de una organización, debe utilizar la cuenta de administración de la organización. No puede usar la cuenta del administrador delegado para copiar eventos de registros de seguimiento en el almacén de datos de eventos de una organización.

Permisos necesarios para copiar eventos de registro de seguimiento

Antes de copiar los eventos de seguimiento, asegúrese de tener todos los permisos necesarios para su función de IAM. Solo necesita actualizar los permisos del rol de IAM si elige un rol de IAM existente para copiar los eventos de registro de seguimiento. Si decide crear un nuevo rol de IAM, CloudTrail proporciona todos los permisos necesarios para el rol.

Si el depósito de S3 de origen utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS CloudTrail permita descifrar los datos del depósito. Si el bucket de S3 de origen usa varias claves KMS, debe actualizar la política de cada clave CloudTrail para poder descifrar los datos del bucket.

Temas

- Permisos de IAM para copiar eventos de registro de seguimiento
- Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento
- Política de claves KMS para descifrar datos en el bucket de S3 de origen

Permisos de IAM para copiar eventos de registro de seguimiento

Al copiar eventos de registro de seguimiento, tiene la opción de crear un nuevo rol de IAM o utilizar uno existente. Al elegir una nueva función de IAM, CloudTrail crea una función de IAM con los permisos necesarios y no es necesario que realice ninguna otra acción por su parte.

Si elige un rol existente, asegúrese de que las políticas del rol de IAM permitan CloudTrail copiar los eventos de seguimiento del bucket de S3 de origen. Esta sección proporciona ejemplos de las políticas de confianza y de permisos necesarias para el rol de IAM.

En el siguiente ejemplo, se proporciona la política de permisos, que permite CloudTrail copiar los eventos de seguimiento del depósito de S3 de origen. Sustituya *myBucketNamemyAccountID*, *region*, *prefijo* e *eventDataStoreId* por los valores adecuados para su configuración. El *myAccountID* es el identificador de AWS cuenta utilizado para CloudTrail Lake, que puede no coincidir con el identificador de cuenta del bucket de S3. AWS

Sustituya *key-region*, *keyAccountID* y *keyID* por los valores de la clave de KMS utilizada para cifrar el bucket de S3 de origen. Puede omitir la instrucción `AWSCloudTrailImportKeyAccess` si el bucket de S3 de origen no utiliza una clave de KMS para el cifrado.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

El siguiente ejemplo proporciona la política de confianza de IAM, que permite asumir una función de IAM CloudTrail para copiar los eventos de seguimiento del bucket de S3 de origen. Sustituya *eventDataStoremyAccountID, region e Id* por los valores adecuados para su configuración. El *myAccountID* es el identificador de AWS cuenta utilizado para CloudTrail Lake, que puede no coincidir con el identificador de AWS cuenta del bucket de S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento

De forma predeterminada, los buckets y los objetos de Amazon S3 son privados. Solo el propietario del recurso (la cuenta de AWS que creó el bucket) puede tener acceso al bucket y a los objetos que contiene. El propietario del recurso puede conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Antes de copiar los eventos de seguimiento, debe actualizar la política del bucket de S3 CloudTrail para permitir copiar los eventos de trail del bucket.

Puedes añadir la siguiente declaración a la política de cubos de S3 para conceder estos permisos. Sustituya *RoLearn* y por *myBucketName*los valores adecuados para su configuración.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

Política de claves KMS para descifrar datos en el bucket de S3 de origen

Si el depósito de S3 de origen utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS proporcione CloudTrail `kms:GenerateDataKey` los permisos necesarios para copiar los eventos de seguimiento de un depósito de S3 con el cifrado SSE-KMS activado. `kms:Decrypt` Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave. La actualización de la política de claves de KMS CloudTrail permite descifrar los datos

del bucket S3 de origen, realizar comprobaciones de validación para garantizar que los eventos cumplen con los CloudTrail estándares y copiar los eventos en el almacén de datos de eventos de CloudTrail Lake.

El siguiente ejemplo proporciona la política de claves de KMS, que CloudTrail permite descifrar los datos del bucket de S3 de origen. Sustituya *RoLearn myBucketName*, *eventDataStoremyAccountID, region e Id* por los valores adecuados para su configuración. El *myAccountID* es el identificador de AWS cuenta utilizado para CloudTrail Lake, que puede no coincidir con el identificador de cuenta del bucket de S3. AWS

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Copie los eventos de seguimiento a un almacén de datos de eventos existente mediante la consola CloudTrail

Utilice el siguiente procedimiento para copiar los eventos de registros de seguimiento en un almacén de datos de eventos existente. Para obtener información sobre cómo crear un nuevo almacén de datos de eventos, consulte Cree un banco de datos de CloudTrail eventos para eventos.

> **Note**
>
> Antes de copiar los eventos del registro de seguimiento a un almacén de datos de eventos existente, asegúrese de que la opción de precios y el periodo de retención del almacén de datos de eventos estén configurados adecuadamente para su caso de uso.
>
> - Opción de precios: la opción de precios determina el costo de la incorporación y el almacenamiento de los eventos. Para obtener más información sobre las opciones de precios, consulte Precios de AWS CloudTrail y Opciones de precios del almacén de datos de eventos.
> - Período de retención: el período de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos del evento. CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Para determinar el período de retención adecuado, calcula la suma del evento más antiguo que deseas copiar en días y el número de días que deseas conservar los eventos en el almacén de datos del evento (período de retención = *`oldest-event-in-days`*+ *`number-days-to-retain`*). Por ejemplo, si el evento más antiguo que va a copiar tiene 45 días y desea conservar los eventos en el almacén de datos de eventos durante otros 45 días, debe establecer el periodo de retención en 90 días.

Para copiar eventos de registros de seguimiento en un almacén de datos de eventos

1. Inicie sesión AWS Management Console y abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
2. Selecciona Trails en el panel de navegación izquierdo de la CloudTrail consola.
3. En la página Trails (Registros de seguimiento), elija el registro de seguimiento y, a continuación, Copy events to Lake (Copiar eventos en Lake). Si el depósito S3 de origen de la ruta utiliza una clave de KMS para el cifrado de datos, asegúrese de que la política de claves de KMS CloudTrail permita descifrar los datos del depósito. Si el depósito de S3 de origen utiliza varias claves KMS, debe actualizar la política de cada clave CloudTrail para poder descifrar los datos del depósito. Para obtener más información sobre la actualización de la política de claves KMS, consulte Política de claves KMS para descifrar datos en el bucket de S3 de origen.
4. (Opcional) De forma predeterminada, CloudTrail solo copia CloudTrail los eventos contenidos en el `CloudTrail` prefijo del bucket de S3 y los prefijos incluidos en el `CloudTrail` prefijo, y no comprueba los prefijos de otros servicios. AWS Si desea copiar CloudTrail los eventos incluidos

en otro prefijo, elija Introducir el URI de S3 y, a continuación, elija Examinar S3 para buscar el prefijo.

La política de buckets de S3 debe permitir el CloudTrail acceso a la copia de eventos de seguimiento. Para obtener más información sobre la actualización de la política de buckets de S3, consulte Política de buckets de Amazon S3 para copiar eventos de registro de seguimiento.

5. En Especificar un rango de tiempo de eventos, elija el rango de tiempo para copiar los eventos. CloudTrail comprueba el prefijo y el nombre del archivo de registro para comprobar que el nombre contiene una fecha entre la fecha de inicio y la de finalización elegidas antes de intentar copiar los eventos de la ruta. Puede elegir un intervalo relativo o un intervalo absoluto. Para evitar la duplicación de eventos entre el registro de seguimiento de origen y el almacén de datos de eventos de destino, elija un intervalo de tiempo que sea anterior a la creación del almacén de datos de eventos.

   > **Note**
   >
   > CloudTrail solo copia los eventos de seguimiento que están `eventTime` dentro del período de retención del almacén de datos de eventos. Por ejemplo, si el período de retención de un almacén de datos de eventos es de 90 días, no CloudTrail copiará ningún evento de ruta que tenga una `eventTime` antigüedad superior a 90 días.

   - Si eliges Rango relativo, puedes elegir copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un rango personalizado. CloudTrail copia los eventos registrados en el período de tiempo elegido.
   - Si elige Rango absoluto, puede elegir una fecha de inicio y finalización específica. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y finalización elegidas.
6. Para Delivery location (Lugar de entrega), elija el almacén de datos de eventos de destino en la lista desplegable.
7. Para Permissions (Permisos), elija una de las siguientes opciones de rol de IAM. Si elige un rol de IAM existente, verifique que la política de roles de IAM proporcione los permisos necesarios. Para obtener más información acerca de la actualización de los permisos de rol de IAM, consulte Permisos de IAM para copiar eventos de registro de seguimiento.

   - Elija Create a new role (recommended) (Crear un nuevo rol [recomendado]) para crear un nuevo rol de IAM. En Enter IAM role name (Ingresar nombre del rol de IAM), escriba un

nombre único para el rol. CloudTrail crea automáticamente los permisos necesarios para este nuevo rol.

- Elija Usar un ARN de rol de IAM personalizado para usar un rol de IAM personalizado que no aparezca en la lista. En Enter IAM role ARN (Ingresar ARN del rol de IAM), escriba el ARN de IAM.
- Elija un rol de IAM existente de la lista desplegable.

8. Elija Copy events (Copiar eventos).
9. Se le solicitará que confirme la copia. Cuando esté listo para confirmar, elija Copy trail events to Lake (Copiar eventos de registro de seguimiento en Lake) y, a continuación, Copy events (Copiar eventos).
10. En la página Copy details (Detalles de la copia), puede observar el estado de la copia y revisar cualquier error. Cuando se completa la copia de un evento de registro de seguimiento, el campo Copy status (Estado de la copia) se establece en Completed (Completa), si no hubo errores, o Failed (Error), si hubo errores.

> **Note**
>
> Los detalles que aparecen en la página de detalles de la copia del evento no aparecen en tiempo real. Los valores reales de detalles, como los prefijos copiados, pueden ser superiores a los que se muestran en la página. CloudTrail actualiza los detalles de forma incremental a lo largo del texto del evento.

11. Si Copy status (Estado de la copia) está establecido en Failed (Error), corrija los errores que aparecen en Copy failures (Errores de la copia) y, a continuación, elija Retry copy (Volver a copiar). Al volver a intentar una copia, la CloudTrail reanuda en la ubicación en la que se produjo el error.

Para obtener más información sobre cómo ver los detalles de la copia de un evento de registro de seguimiento, consulte Detalles de la copia del evento.

Obtención y visualización de archivos de registros de CloudTrail

Después de haber creado y configurado un seguimiento para capturar los archivos de registro que desee, tendrá que ser capaz de encontrar los archivos de registro y de interpretar la información que contienen.

CloudTrail envía los archivos de registros al bucket de Amazon S3 que indique al crear el registro de seguimiento. En general, CloudTrail envía registros en un plazo de 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el Acuerdo de nivel de servicios de AWS CloudTrail. Normalmente, los eventos de información se envían al bucket tras 30 minutos de actividad inusual. Después de habilitar los eventos de información primera vez, los primeros eventos aparecen al cabo de 36 horas, si se detecta actividad inusual.

> **Note**
>
> Si configura mal su registro de seguimiento (por ejemplo, si no se puede acceder al bucket de S3), CloudTrail intentará volver a entregar los archivos de registro a su bucket de S3 durante 30 días, y estos eventos de intento de entrega estarán sujetos a los cargos estándar de CloudTrail. Para evitar que se le cobre por un registro de seguimiento mal configurado, debe eliminarlo.

Temas

- Búsqueda de los archivos de CloudTrail registro
- Descarga de los archivos de registros de CloudTrail

Búsqueda de los archivos de CloudTrail registro

CloudTrail publica los archivos de registro en su bucket de S3 en un archivo gzip. En el bucket de S3, el archivo de registro tiene un nombre con formato que incluye los siguientes elementos:

- El nombre del bucket que especificaste al crear el sendero (que se encuentra en la página Trails de la CloudTrail consola)
- El prefijo (opcional) que haya especificado al crear el registro de seguimiento
- La cadena "AWSLogs»
- El número de cuenta
- La cadena «CloudTrail»
- Un identificador de región como, por ejemplo, us-west-1
- El año en que se publicó el archivo de registro con el formato `YYYY`
- El mes en que se publicó el archivo de registro con el formato `MM`

- El día en que se publicó el archivo de registro con el formato DD
- Cadena alfanumérica que desambigua el archivo de otros que abarcan el mismo periodo de tiempo

El ejemplo siguiente muestra un nombre de objeto del archivo de registro completo:

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> En el caso de los registros de la organización, el nombre del objeto del archivo de registro del bucket de S3 incluye el ID de la unidad organizativa en la ruta, de la siguiente manera:
>
> ```
> bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

Para recuperar un archivo de registros, puede utilizar la consola de Amazon S3, la interfaz de línea de comandos (CLI) de Amazon S3 o la API.

Para encontrar los archivos de registros con la consola de Amazon S3

1. Abra la consola de Amazon S3.
2. Elija el bucket especificado.
3. Recorra la jerarquía de objetos hasta que encuentre el archivo de registro que desee.

   Todos los archivos de registro tienen la extensión .gz.

Verá una jerarquía de objetos similar a la del siguiente ejemplo, pero con otro nombre de bucket, ID de cuenta, región y fecha.

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
```

```
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

Un archivo de registro para la jerarquía de objetos anterior se parecerá a lo siguiente:

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> Aunque es poco frecuente, puede recibir archivos de registro que contengan uno o más eventos duplicados. En la mayoría de los casos, los eventos duplicados tendrán el mismo `eventID`. Para obtener más información acerca del campo `eventID`, consulte CloudTrail contenido del registro.

Descarga de los archivos de registros de CloudTrail

Los archivos de registro están en formato JSON. Si tiene un complemento de visor de JSON instalado, puede ver los archivos directamente en el navegador. Haga doble clic en el nombre de archivo de registro en el bucket para abrir una nueva ventana o pestaña del navegador. El código JSON se muestra en formato legible.

Por ejemplo, si utiliza Mozilla Firefox, también puede descargar el complemento JSONView. Con JSONView puede hacer doble clic en el archivo .gz comprimido en su bucket para abrir el archivo de registro en formato JSON.

Los archivos de registros de CloudTrail son objetos de Amazon S3. Para recuperar los archivos de registros, puede utilizar la consola de Amazon S3, la AWS Command Line Interface (CLI) o la API de Amazon S3.

Para obtener más información, consulte Trabajar con objetos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

En el procedimiento siguiente se describe cómo descargar un archivo de registro con la AWS Management Console.

Para descargar y leer un archivo de registro

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el bucket y el archivo de registro que desea descargar.
3. Elija Descargar o Descargar como y siga las instrucciones para guardar el archivo. Se guarda en formato comprimido.

   > **Note**
   >
   > Algunos navegadores, como Chrome, extraen automáticamente el archivo de registro automáticamente. Si lo hace así su navegador, vaya al paso 5.

4. Utilice un producto como 7-Zip para extraer el archivo de registro.
5. Abra el archivo de registro en un editor de texto como Notepad++.

Para obtener más información sobre los campos de eventos que pueden aparecer en una entrada de archivo de registro, consulte Referencia de eventos de registro de CloudTrail.

AWS colabora con terceros especialistas en el registro y análisis para proporcionar soluciones que utilizan la información de CloudTrail. Para obtener más información, consulte Red de socios de AWS: socios de AWS CloudTrail.

> **Note**
>
> También puede utilizar la característica Event history para buscar eventos con el fin de crear, actualizar y eliminar la actividad de la API durante los últimos 90 días.
> Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Configuración de notificaciones de Amazon SNS para CloudTrail

Puede recibir una notificación cada vez que CloudTrail publique nuevos archivos de registros en su bucket de Amazon S3. Puede administrar las notificaciones mediante Amazon Simple Notification Service (Amazon SNS)

Las notificaciones son opcionales. Si desea recibir notificaciones, configure CloudTrail para que envíe información actualizada sobre un tema de Amazon SNS cada vez que se envíe un archivo

de registros nuevo. Para recibir estas notificaciones, puede utilizar Amazon SNS para suscribirse al tema Como suscriptor puede obtener las actualizaciones enviadas a una cola de Amazon Simple Queue Service (Amazon SQS), lo que le permite gestionar estas notificaciones mediante programación.

Temas

- Configuración de CloudTrail para el envío de notificaciones

Configuración de CloudTrail para el envío de notificaciones

Puede configurar un registro de seguimiento para utilizar un tema de Amazon SNS. Puede utilizar la consola de CloudTrail o el comando de la CLI aws cloudtrail create-trail para crear el tema. CloudTrail crea el tema de Amazon SNS automáticamente y adjunta una política adecuada, de forma que CloudTrail tenga permiso para publicar en ese tema.

Los nombres de tema de SNS creados deben cumplir los siguientes requisitos:

- Deben tener entre 1 y 256 caracteres.
- Deben contener letras ASCII en mayúsculas y minúsculas, números, guiones bajos o guiones.

Cuando configure notificaciones para un registro de seguimiento aplicable a todas las regiones, las notificaciones de todas las regiones se envían al tema de Amazon SNS que haya especificado. Si tiene uno o varios registros de seguimiento específicos de una región, será preciso que cree un tema para cada región y que se suscriba a cada uno por individual.

Para recibir notificaciones, suscríbase al tema o los temas de Amazon SNS que utiliza CloudTrail. Esto se hace con la consola de Amazon SNS o los comandos de la CLI de Amazon SNS. Para obtener más información, consulte Suscribirse a un tema en la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> CloudTrail envía una notificación cuando los archivos de registros se escriben en el bucket de Amazon S3. Las cuentas activas pueden generar un gran número de notificaciones. Si se suscribe mediante correo electrónico o SMS, puede recibir un gran volumen de mensajes. Se recomienda que se suscriba con Amazon Simple Queue Service (Amazon SQS), puesto que le permite gestionar las notificaciones mediante programación. Para obtener más

información, consulte Suscribirse a una cola de un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Queue Service.

La notificación de Amazon SNS consta de un objeto JSON que incluye un campo `Message`. El campo `Message` muestra la ruta completa al archivo de registro, tal y como aparece En el ejemplo siguiente:

```
{
    "s3Bucket": "your-bucket-name","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Si se envían múltiples archivos de registros al bucket de Amazon S3 es posible que las notificaciones contengan varios registros, tal como se muestra en el siguiente ejemplo:

```
{
    "s3Bucket": "your-bucket-name",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

Si decide recibir notificaciones por correo electrónico, el cuerpo del mensaje incluirá el contenido del campo `Message`. Para obtener una descripción completa de la estructura JSON, consulte Envío de mensajes Amazon SNS a las colas de Amazon SQS en la Guía para desarrolladores de Amazon Simple Notification Service. Solo el campo `Message` muestra información de CloudTrail. Los demás campos contienen información del servicio de Amazon SNS.

Si crea un registro de seguimiento con la API de CloudTrail, podrá especificar un tema de Amazon SNS existente al que quiera que CloudTrail envíe notificaciones con las operaciones `CreateTrail`

o `UpdateTrail`. Debe asegurarse de que el tema exista y que tenga los permisos necesarios para que CloudTrail pueda enviarle notificaciones. Consulte Política temática de Amazon SNS para CloudTrail.

Recursos adicionales

Para obtener más información sobre los temas de Amazon SNS y de la suscripción a ellos, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Consejos para la administración de registros de seguimiento

- A partir del 12 de abril de 2019, los registros de seguimiento solo se pueden ver en las Regiones de AWS en las que se registren eventos. Si crea un registro de seguimiento que registra eventos en todas las Regiones de AWS, aparecerá en la consola en todas las Regiones de AWS de la partición de AWS en la que trabaja. Si crea un registro de seguimiento que solo registra los eventos en una Región de AWS, solo podrá verlo y administrarlo en esa Región de AWS.
- Para editar un registro de seguimiento de la lista, elija el nombre del registro.
- Configure al menos un registro de seguimiento que se aplique a todas las regiones, de forma que reciba archivos de registro de todas las regiones de la partición de AWS en la que trabaja.
- Para registrar eventos de una región concreta y enviar los archivos de registro a un bucket de S3 en la misma región, puede actualizar el registro de seguimiento para aplicarlo a una única región. Esto resulta útil si desea conservar los archivos de registro separados. Por ejemplo, es posible que desee que los usuarios administren sus propios registros en regiones específicas o que desee separar las alarmas de Registros de CloudWatch por región.
- Para registrar eventos de varias cuentas de AWS en un solo registro de seguimiento, considere la posibilidad de crear una organización en AWS Organizations y, a continuación, crear un registro de seguimiento de organización.
- La creación de varios registros de seguimiento generará costos adicionales. Para obtener más información sobre los precios, consulte AWS CloudTrail Precios.

Gestión de los costes de los CloudTrail senderos

Como práctica recomendada, recomendamos utilizar AWS servicios y herramientas que puedan ayudarle a gestionar CloudTrail los costes. También puede configurar y gestionar las CloudTrail rutas de forma que capturen los datos que necesita sin dejar de ser rentable. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail los precios.

Herramientas para ayudar a administrar los costos

AWS Los presupuestos, una función de AWS Billing and Cost Management, te permiten establecer presupuestos personalizados que te avisan cuando los costes o el uso superan (o se prevé que superen) el importe presupuestado.

Al crear varios registros, la mejor práctica recomendada es crear un presupuesto CloudTrail mediante AWS presupuestos, que puede ayudarte a llevar un registro de tus CloudTrail gastos. Los presupuestos basados en los costes ayudan a dar a conocer cuánto te podrían facturar por el uso que hagas CloudTrail . Las alertas de presupuesto le notifican el momento en que su factura alcanza el límite que ha definido. Cuando reciba una alerta de presupuesto, puede realizar cambios antes de que finalice el ciclo de facturación para administrar los costos.

Después de crear un presupuesto, puedes usarlo AWS Cost Explorer para ver cómo influyen tus CloudTrail costos en tu factura general AWS . En AWS Cost Explorer, después de añadirlo CloudTrail al filtro de servicios, puede comparar sus CloudTrail gastos históricos con los de sus gastos actuales month-to-date (MTD), tanto por región como por cuenta. Esta función le ayuda a supervisar y detectar los costes inesperados de sus CloudTrail gastos mensuales. Las funciones adicionales de Cost Explorer le permiten comparar los CloudTrail gastos con los gastos mensuales en un nivel de recurso específico, lo que proporciona información sobre lo que podría estar provocando aumentos o disminuciones de los costos en su factura.

> **Note**
>
> Si bien puede aplicar etiquetas a los CloudTrail senderos, actualmente AWS Billing no se pueden usar las etiquetas aplicadas a los senderos para asignar los costos. Cost Explorer puede mostrar los costos de los almacenes de datos de eventos de CloudTrail Lake y del CloudTrail servicio en su conjunto.

Para empezar a usar AWS Presupuestos, abra y AWS Billing and Cost Management, a continuación, seleccione Presupuestos en la barra de navegación izquierda. Te recomendamos configurar las alertas de presupuesto al crear un presupuesto para hacer un seguimiento de CloudTrail los gastos. Para obtener más información sobre cómo usar AWS los presupuestos, consulte Administrar sus costos con presupuestos y Mejores prácticas para AWS los presupuestos.

Configuración de registros de seguimiento

CloudTrail ofrece flexibilidad a la hora de configurar las rutas en su cuenta. Algunas decisiones que tomas durante el proceso de configuración requieren que comprendas los impactos en tu CloudTrail factura. Los siguientes son ejemplos de cómo las configuraciones de los senderos pueden influir en su CloudTrail factura.

Creación de varios registros de seguimiento

La primera entrega de cada evento de administración de una cuenta es gratuita. Si crea más senderos que ofrezcan los mismos eventos de gestión a otros destinos, las entregas posteriores generarán CloudTrail costes. Puede hacerlo para permitir que diferentes grupos de usuarios (tales como desarrolladores, personal de seguridad y auditores de TI) reciban sus propias copias de los archivos de registro. En el caso de los eventos de datos, todas las entregas conllevan CloudTrail costes, incluida la primera.

A medida que crea más registros de seguimiento, es especialmente importante estar familiarizado con los registros y comprender los tipos y los volúmenes de eventos generados por los recursos de su cuenta. Esto le ayuda a prever el volumen de eventos que están asociados a una cuenta y a planificar los costos de registro de seguimiento. Por ejemplo, el uso del cifrado AWS KMS gestionado del lado del servidor (SSE-KMS) en los buckets de S3 puede provocar una gran cantidad de eventos de administración. AWS KMS CloudTrail Los volúmenes de mayor tamaño de eventos en varios registros de seguimiento también pueden repercutir en los costos.

Para ayudar a limitar el número de eventos que se registran en su ruta, puede filtrar AWS KMS los eventos de la API de datos de Amazon RDS seleccionando Excluir eventos o Excluir AWS KMS eventos de la API de datos de Amazon RDS en las páginas Crear ruta o Actualizar ruta. Cuando se utilizan selectores de eventos básicos, solo se pueden filtrar los eventos de administración. Sin embargo, puede utilizar selectores de eventos avanzados para filtrar eventos de administración y de datos. Puede utilizar selectores de eventos avanzados para incluir o excluir eventos de datos en función de los campos `resources.type`, `eventName`, `resources.ARN` y `readOnly`, lo que le permite registrar solo los eventos de datos que le interesen. Para obtener más información sobre la configuración de estos campos, consulte AdvancedFieldSelector. Para obtener más información acerca de la creación y actualización de un registro de seguimiento, consulte Creación de un registro de seguimiento o Actualización de un registro de seguimiento en esta guía.

AWS Organizations

Cuando configuras una ruta de Organizations con CloudTrail, CloudTrail replica la ruta en cada cuenta de miembro de tu organización. Se crea el nuevo registro de seguimiento, además de los registros de seguimiento existentes en las cuentas miembro. Asegúrese de que la configuración del registro de seguimiento de organización coincida con la forma en que desea que los registros de seguimiento se configuren en todas las cuentas de una organización, ya que la configuración del registro de seguimiento de organización se propaga a todas las cuentas.

Dado que Organizations crea un registro de seguimiento en cada cuenta miembro, una cuenta miembro individual que crea un registro de seguimiento adicional para recopilar los mismos eventos de administración que el registro de seguimiento de Organizations recopila una segunda copia de los eventos. La segunda copia se cobra en la cuenta. Del mismo modo, si una cuenta tiene un registro de seguimiento de varias regiones y crea un segundo registro de seguimiento en una única región para recopilar los mismos eventos de administración que el registro de seguimiento de varias regiones, el registro de seguimiento de una única región envía una segunda copia de los eventos. Se aplican cargos a la segunda copia.

Véase también

- AWS CloudTrail Precios
- Gestione sus costes con AWS Budgets
- Introducción al Explorador de costos
- Prepararse a fin de crear un registro de seguimiento para la organización

Requisitos de nomenclatura

En esta sección se proporciona información sobre los requisitos de nomenclatura de los recursos de CloudTrail, los buckets de Amazon S3 y las claves de KMS.

Temas

- Requisitos de nomenclatura para recursos de CloudTrail
- Requisitos de nomenclatura para buckets de Amazon S3
- Requisitos de nomenclatura para el alias de AWS KMS

Requisitos de nomenclatura para recursos de CloudTrail

Los nombres de los recursos de CloudTrail deben cumplir los siguientes requisitos:

- Deben contener solo letras ASCII (a-z, A-Z), números (0-9), puntos (.), guiones bajos (_) y guiones (-).
- Deben empezar por una letra o un número y terminar con una letra o un número.
- Deben tener entre 3 y 128 caracteres.
- No deben tener puntos, guiones bajo o guiones adyacentes. Nombres como mi-_espaciodenombres y mi-\-espaciodenombres no son válidos.
- No deben tener el formado de una dirección IP (por ejemplo, `192.168.5.4`).

Requisitos de nomenclatura para buckets de Amazon S3

El bucket de Amazon S3 que utiliza a fin de almacenar archivos de registros de CloudTrail debe tener un nombre que cumpla los requisitos de nomenclatura para las regiones que no siguen el EE. UU. Estándar. Amazon S3 define un nombre de bucket como una serie de una o varias etiquetas, separadas por puntos. Para obtener una lista completa de las reglas de nomenclatura, consulte Reglas de nomenclatura de buckets en la Guía del usuario de Amazon Simple Storage Service.

A continuación se muestran algunas de las normas:

- El nombre del bucket puede tener entre 3 y 63 caracteres y puede contener únicamente caracteres en minúsculas, números, puntos y guiones.
- Cada etiqueta en el nombre del bucket debe empezar por un carácter en minúsculas o un número.
- El nombre del bucket no puede contener guiones bajos, terminar en guion, puntos suspensivos ni utilizar guiones junto con puntos.
- El nombre del bucket no puede tener el formato de una dirección IP (198.51.100.24).

> **Warning**
>
> Dado que S3 permite que el bucket se pueda utilizar como una dirección URL con acceso público, el nombre del bucket que elija deberá ser único de forma global. Si hay otra cuenta que ya haya creado un bucket con el nombre que eligió, deberá utilizar otro nombre. Para

obtener más información, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon Simple Storage Service.

Requisitos de nomenclatura para el alias de AWS KMS

Al crear una AWS KMS key, puede elegir un alias para identificarla. Por ejemplo, puede elegir el alias "KMS-CloudTrail-us-west-2" para cifrar los registros de un registro de seguimiento específico.

El alias debe cumplir los siguientes requisitos:

- Entre 1 y 256 caracteres inclusive
- Contener caracteres alfanuméricos (A-Z, a-z, 0-9), guiones (-), barras oblicuas (/) y guiones bajos (_)
- No puede empezar con aws

Para obtener más información, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service.

Controlar los permisos de usuario para los registros de seguimiento de CloudTrail

AWS CloudTrail se integra con AWS Identity and Access Management (IAM) para ayudarle a controlar el acceso a CloudTrail y otros recursos de AWS que requiere CloudTrail. Algunos ejemplos de estos recursos son los buckets de Amazon S3 y los temas de Amazon Simple Notification Service (Amazon SNS). Puede utilizar IAM para controlar qué usuarios de AWS pueden crear, configurar o eliminar registros de seguimiento de CloudTrail, comenzar y detener el registro y tener acceso a los buckets que contienen información de registro. Para obtener más información, consulte Administración de identidades y accesos para AWS CloudTrail.

Los siguientes temas le ayudan a comprender los permisos, las políticas y la seguridad de CloudTrail:

- Otorgar permisos de CloudTrail administración
- Reglas de nomenclatura de buckets de Amazon S3
- Política de bucket de Amazon S3 para CloudTrail

- Un ejemplo de política de bucket para el registro de seguimiento de una organización en Crear un registro para una organización con AWS Command Line Interface.
- Política temática de Amazon SNS para CloudTrail
- Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS)
- Permisos necesarios para copiar eventos de registro de seguimiento
- Permisos necesarios para designar un administrador delegado
- Política de claves de KMS predeterminada creada en la consola de CloudTrail
- Otorgar permiso para ver AWS Config información en la consola CloudTrail
- Compartir archivos de registro de CloudTrail entre cuentas de AWS
- Permisos necesarios para crear un registro de seguimiento de organización
- Utilizar un rol de IAM previamente existente para agregar la supervisión de un registro de seguimiento de la organización a Registros de Amazon CloudWatch

Uso de AWS CloudTrail con los puntos de enlace de la VPC de la interfaz

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus recursos de AWS, puede establecer una conexión entre su VPC y AWS CloudTrail. Puede utilizar esta conexión para habilitar que CloudTrail se comunique con sus recursos en su VPC sin pasar por la red pública de Internet.

Amazon VPC es un servicio de AWS que puede utilizar para lanzar recursos de AWS en una red virtual que defina. Con una VPC, puede controlar la configuración de la red, como el rango de direcciones IP, las subredes, las tablas de ruteo y las gateways de red. Con puntos de enlace de la VPC, el enrutamiento entre la VPC y los servicios de AWS se controla mediante la red de AWS y puede utilizar políticas de IAM para controlar el acceso a los recursos de servicio.

Para conectar su VPC CloudTrail, debe definir un punto final de VPC de interfaz para. CloudTrail Un punto de conexión de interfaz es una interfaz de red elástica con una dirección IP privada que actúa como punto de entrada para el tráfico dirigido a un servicio de AWS compatible. El punto final proporciona una conectividad fiable y escalable CloudTrail sin necesidad de una puerta de enlace a Internet, una instancia de traducción de direcciones de red (NAT) ni una conexión VPN. Para obtener más información, consulte Qué es Amazon VPC en la Guía del usuario de Amazon VPC.

Los puntos de conexión de VPC de tipo interfaz utilizan AWS PrivateLink, una tecnología de AWS que permite la comunicación privada entre los servicios de AWS mediante una interfaz de red elástica con direcciones IP privadas. Para obtener más información, consulte AWS PrivateLink.

Los siguientes pasos son para usuarios de Amazon VPC. Para obtener más información, consulte Introducción a Amazon VPC en la Guía del usuario de Amazon VPC.

Disponibilidad

CloudTrail actualmente admite puntos finales de VPC en las siguientes regiones: AWS

- US East (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (Centro)
- Oeste de Canadá (Calgary
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milán)

- Europa (París)
- Europa (España)
- Europa (Estocolmo)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Estados Unidos-Oeste)

Cree un punto final de VPC para CloudTrail

Para empezar a usarlo CloudTrail con su VPC, cree un punto de enlace de VPC de interfaz para. CloudTrail Para obtener más información, consulte Acceso a un servicio de Servicio de AWS a través de un punto de conexión de VPC de tipo interfaz en la Guía de usuario de Amazon VPC.

No necesita cambiar la configuración de. CloudTrail CloudTrail llama a otros Servicios de AWS mediante puntos de conexión públicos o puntos de conexión de VPC de interfaz privada, según se utilicen.

Subredes compartidas

Un punto de enlace de CloudTrail VPC, como cualquier otro punto de enlace de VPC, solo lo puede crear una cuenta de propietario en la subred compartida. Sin embargo, una cuenta de participante puede usar puntos de enlace de CloudTrail VPC en subredes que se comparten con la cuenta de participante. Para obtener más información sobre el uso compartido de Amazon VPC, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Cuenta de AWS cierre y senderos

AWS CloudTrail monitorea y registra continuamente los eventos relacionados con la actividad de la cuenta generados por cualquier usuario, rol o Servicio de AWS para un Cuenta de AWS. Los usuarios pueden crear un CloudTrail registro para recibir una copia de estos eventos en un bucket de S3 que sea de su propiedad.

CloudTrail es un servicio de seguridad fundamental, por lo que las rutas creadas por los usuarios siguen existiendo y publicando eventos incluso después de que Cuenta de AWS se cierre una ruta, a menos que un usuario elimine explícitamente las rutas Cuenta de AWS antes de cerrarlas. Este comportamiento también se aplica a los registros de seguimiento organizativos que crea la cuenta de administración o el administrador delegado, y a los registros de seguimiento organizativos de varias regiones que luego se crean en las cuentas de los miembros de la organización. Esto garantiza que, si un usuario vuelve a abrir una cuenta cerrada, dicho usuario tenga un registro ininterrumpido de la actividad de la cuenta. También ofrece a los usuarios visibilidad de cualquier actividad final de la cuenta, incluida la eliminación y cancelación de los recursos y servicios restantes de la cuenta.

Los usuarios tienen la opción de eliminar las rutas antes de cerrarlas Cuenta de AWS o ponerse en contacto con ellas AWS Supportpara solicitar que se eliminen después de cerrarlas Cuenta de AWS .

Para obtener más información sobre cómo cerrar una Cuenta de AWS, consulte Cerrar una Cuenta de AWS.

> **Note**
>
> Si la validación de los archivos de CloudTrail registro está habilitada, los usuarios seguirán recibiendo archivos de resumen cada hora en los que se indica si se creó algún CloudTrail registro o no.
> CloudTrail Los almacenes de datos de eventos de CloudTrail Lake, los canales de Lake para integraciones, los canales CloudTrail vinculados a servicios y los recursos creados para las rutas (por ejemplo, los grupos de CloudWatch registros de Amazon Logs y los depósitos de Amazon S3 existentes en la cuenta cerrada) siguen un AWS comportamiento estándar para el cierre de la cuenta y se eliminan permanentemente tras el período posterior al cierre (normalmente 90 días).

Trabajar con archivos de registros de CloudTrail

Puede realizar tareas más avanzadas con sus archivos de CloudTrail.

- Cree varios registros de seguimiento por región.
- Para monitorear los archivos de registros de CloudTrail, envíelos a CloudWatch Logs.
- Comparta archivos de registros entre cuentas.
- Utilice la biblioteca de procesamiento de CloudTrail de AWS para escribir aplicaciones de procesamiento de registros en Java.
- Valide los archivos de registros para verificar que no hayan cambiado después de que CloudTrail los ha enviado.

Cuando se produce un evento en su cuenta, CloudTrail evalúa si coincide con la configuración de sus registros de seguimiento. Solo se envían al bucket de Amazon S3 y al grupo de registros de Amazon CloudWatch Logs los eventos que coinciden con la configuración del registro de seguimiento.

Puede configurar varios registros de seguimiento de forma distinta, de modo que procesen y registren únicamente los eventos que especifique. Por ejemplo, un registro de seguimiento puede registrar eventos de datos de solo lectura y de administración, con el fin de que todos los eventos de solo lectura se envíen a un bucket de S3. Otro registro de seguimiento puede registrar únicamente eventos de datos de solo escritura y de administración, con el fin de que todos los eventos de solo escritura se envíen a un bucket de S3 independiente.

También puede configurar sus registros de seguimiento con un registro para que envíe todos los eventos de administración a un bucket de S3 y otro que registre y envíe todos los eventos de datos a otro bucket de S3.

Puede configurar sus registros de seguimiento para que registren lo siguiente:

- Datos de eventos: estos eventos proporcionan visibilidad de las operaciones realizadas en un recurso o dentro de él. Se denominan también operaciones del plano de datos.
- Eventos de administración: proporcionan visibilidad de las operaciones de administración que se realizan en los recursos de su cuenta de AWS. Se denominan también operaciones del plano de control. Los eventos de administración también pueden incluir eventos no generados por la API que se producen en su cuenta. Por ejemplo, cuando un usuario inicia sesión en su cuenta,

CloudTrail registra el evento `ConsoleLogin`. Para obtener más información, consulte Eventos no generados por la API capturados por CloudTrail.

> **Note**
>
> No todos los servicios de AWS admiten eventos de CloudTrail. Para obtener más información acerca de los servicios compatibles, consulte CloudTrail servicios e integraciones compatibles. Para obtener información detallada sobre las API que se registran para un determinado servicio, consulte la documentación del servicio en CloudTrail servicios e integraciones compatibles.

- Eventos de Insights: capturan la actividad inusual que se detecta en la cuenta. Si ha habilitado eventos de Insights y CloudTrail detecta actividad inusual, los eventos de Insights se registran en el bucket de S3 de destino para su registro de seguimiento, pero en una carpeta diferente. También puede ver el tipo de evento de Insights y el periodo de tiempo del incidente si consulta los eventos de Insights en la consola de CloudTrail. A diferencia de otros tipos de eventos capturados en un registro de seguimiento de CloudTrail, los eventos de Insights solo se registran cuando CloudTrail detecta cambios en el uso de la API de su cuenta que difieren considerablemente de los patrones de uso típicos de la cuenta.

  Los eventos de Insights solo se generan para las API de administración. Para obtener más información, consulte Registro de eventos de Insights.

> **Note**
>
> En general, CloudTrail envía registros en un plazo de 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el Acuerdo de nivel de servicios de AWS CloudTrail.
> Si configura mal su registro de seguimiento (por ejemplo, si no se puede acceder al bucket de S3), CloudTrail intentará volver a entregar los archivos de registro a su bucket de S3 durante 30 días, y estos eventos de intento de entrega estarán sujetos a los cargos estándar de CloudTrail. Para evitar que se le cobre por un registro de seguimiento mal configurado, debe eliminarlo.

Temas

- Crear varios registros de seguimiento

- Registro de eventos de administración
- Registro de eventos de datos
- Registro de eventos de Insights
- Recepción de archivos de registro de CloudTrail de varias regiones
- Administración de la consistencia de los datos en CloudTrail
- Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs
- Recepción de archivos de CloudTrail registro de varias cuentas
- Compartir archivos de registro de CloudTrail entre cuentas de AWS
- Validar la integridad de los archivos de registros de CloudTrail
- Uso de la biblioteca de procesamiento de CloudTrail

Crear varios registros de seguimiento

Puede utilizar los archivos de registros de CloudTrail para solucionar problemas de funcionamiento o seguridad en su cuenta de AWS. Puede crear registros de seguimiento para diferentes usuarios, que pueden crear y administrar sus propios registros de seguimiento. Puede configurar registros de seguimiento para enviar archivos de registro a buckets de S3 diferentes o buckets de S3 compartidos.

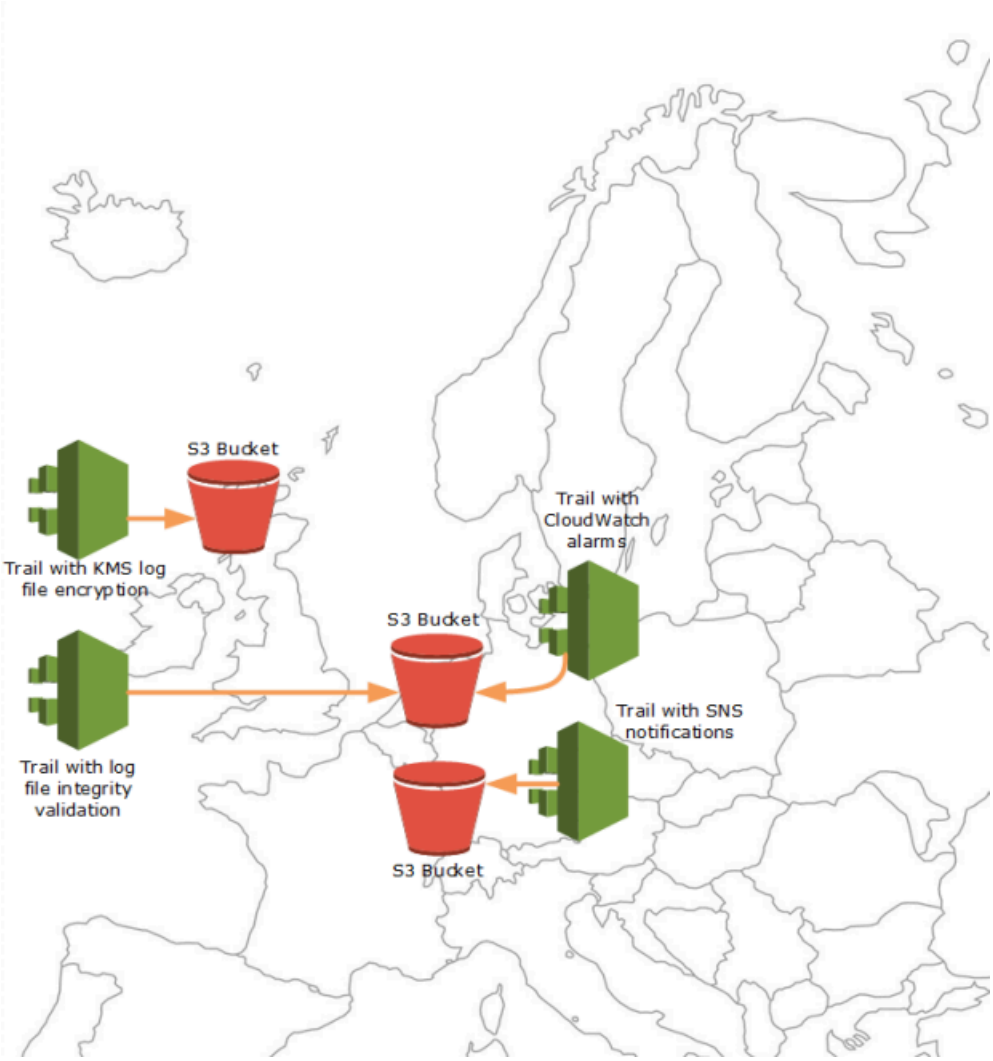
> **Note**
>
> La creación de varios registros de seguimiento generará costos adicionales. Para obtener más información, consulte Precios de AWS CloudTrail.

Por ejemplo, es posible que tenga los siguientes usuarios:

- Un administrador de seguridad crea un registro de seguimiento en la región de Europa (Irlanda) y configura el cifrado de los archivos de registros de KMS. El registro de seguimiento envía los archivos de registros a un bucket de S3 en la región de Europa (Irlanda).
- Un auditor de TI crea un registro de seguimiento en la región de Europa (Irlanda) y configura la validación de la integridad de los archivos de registros para garantizar que estos no han cambiado desde que CloudTrail los entregó. El registro de seguimiento se encuentra configurado para enviar archivos de registros a un bucket de S3 en la región de Europa (Fráncfort)

- Un desarrollador crea un registro de seguimiento en la región de Europa (Fráncfort) y configura alarmas de CloudWatch para recibir notificaciones de la actividad específica de la API. El registro de seguimiento comparte el mismo bucket de S3 que ha configurado el registro de seguimiento para la integridad de los archivos de registro.
- Otro desarrollador crea un registro de seguimiento en la región de Europa (Fráncfort) y configura SNS. Los archivos de registros se entregan en un bucket de S3 diferente en la región de Europa (Fráncfort).

La imagen siguiente ilustra este ejemplo.



> **Note**
>
> Puede crear un máximo de cinco registros de seguimiento por cada Región de AWS. Un registro de seguimiento que registra la actividad de todas las regiones cuenta como un registro de seguimiento por región.

Puede utilizar los permisos de nivel de recursos para administrar la capacidad de un usuario para realizar operaciones específicas en CloudTrail.

Por ejemplo, puede conceder a un usuario permiso para ver la actividad del registro de seguimiento, pero impedir que inicie o detenga dicho registro. Puede conceder a otro usuario permiso completo para crear y eliminar registros de seguimiento. De este modo, dispondrá de control exhaustivo de los registros de seguimiento y el acceso de los usuarios.

Para obtener más información sobre los permisos de nivel de recursos, consulte Ejemplos: creación y aplicación de políticas para acciones en registros de seguimiento específicos.

Para obtener más información sobre varios registros de seguimiento, consulte los siguientes recursos:

- ¿Cómo se CloudTrail comporta a nivel regional y global?
- Preguntas frecuentes sobre CloudTrail

Registro de eventos de administración

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos registran eventos de administración y no incluyen datos ni eventos de Insights.

Se aplican cargos adicionales por los eventos de datos o de Insights. Para más información, consulte Precios de AWS CloudTrail.

Contenido

- Eventos de administración
  - Registro de eventos de administración con la AWS Management Console
- Eventos de lectura y escritura
- Registro de eventos con la AWS Command Line Interface

- Ejemplos: Registro de eventos de administración para los registros de seguimiento
  - Ejemplos: registro de eventos de administración para senderos mediante selectores de eventos avanzados
  - Ejemplos: registrar los eventos de administración de los senderos mediante selectores de eventos básicos
- Ejemplos: Registros de eventos de administración para los almacenes de datos de eventos
- Registro de eventos con los SDK de AWS
- Envío de eventos a Amazon CloudWatch Logs

Eventos de administración

Los eventos de administración proporcionan visibilidad de las operaciones de administración que se realizan en los recursos de una cuenta de AWS. Se denominan también operaciones del plano de control. Algunos ejemplos de eventos de administración son los siguientes:

- Configuración de la seguridad (por ejemplo, operaciones de la API `AttachRolePolicy` de IAM)
- Registro de dispositivos (por ejemplo, operaciones de la API `CreateDefaultVpc` de Amazon EC2)
- Configuración de reglas para el enrutamiento de datos (por ejemplo, operaciones de la API `CreateSubnet` de Amazon EC2)
- Configuración del registro (por ejemplo, operaciones de la API `CreateTrail` de AWS CloudTrail)

Los eventos de administración también pueden incluir eventos no generados por la API que se producen en su cuenta. Por ejemplo, cuando un usuario inicia sesión en tu cuenta, CloudTrail registra el `ConsoleLogin` evento. Para obtener más información, consulte Eventos no generados por la API capturados por CloudTrail.

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos están configurados para registrar eventos de administración.

> **Note**
>
> La función de historial de CloudTrail eventos solo admite eventos de administración. No puede excluir a AWS KMS ni a eventos de la API de datos de Amazon RDS del Historial de eventos; la configuración que se aplica a un registro de seguimiento o almacén de datos de

eventos no se aplica al Historial de eventos. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Registro de eventos de administración con la AWS Management Console

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. Para actualizar una ruta, abre la página Rutas de la CloudTrail consola y elige el nombre de la ruta.

   Para actualizar un banco de datos de eventos, abra la página de almacenes de datos de eventos de la CloudTrail consola y elija el nombre del banco de datos de eventos.
3. En Management events (Eventos de administración), elija Edit (Editar).

   - Seleccione si desea que el registro de seguimiento o el almacén de datos de eventos registren eventos de Lectura, Escritura, o ambos.
   - Seleccione Excluir eventos de AWS KMS para filtrar eventos de AWS Key Management Service (AWS KMS) fuera del registro de seguimiento o del almacén de datos de eventos. La configuración predeterminada es incluir a todos los eventos de AWS KMS.

     La opción para registrar o excluir eventos de AWS KMS solo se encuentra disponible si registra eventos de administración en su registro de seguimiento o almacén de datos de eventos. Si elige no registrar eventos de administración, no se registran eventos de AWS KMS y no podrá cambiar la configuración del registro de eventos de AWS KMS.

     En general, las acciones de AWS KMS como `Encrypt`, `Decrypt` y `GenerateDataKey` generan un gran volumen (más del 99 %) de eventos. Estas acciones se registran ahora como eventos de lectura. Las acciones relevantes y de bajo volumen de AWS KMS, como `Disable`, `Delete`, y `ScheduleKey` (que normalmente representan menos del 0,5 % del volumen de eventos de AWS KMS) se registran como eventos Write (Escritura).

     Para excluir eventos de gran volumen como `Encrypt`, `Decrypt` y `GenerateDataKey`, y seguir registrando eventos relevantes como `Disable`, `Delete` y `ScheduleKey`, elija registrar eventos de administración Write (Escritura) y desmarque la casilla de verificación Exclude AWS KMS events (Excluir eventos de KMS).
   - Seleccione Excluir eventos de la API de datos de Amazon RDS para quitar del registro de seguimiento o del almacén de datos de eventos los eventos de la API de datos de Amazon

Relational Database Service. La configuración predeterminada es incluir a todos los eventos de la API de datos de Amazon RDS. A fin de obtener más información sobre los eventos de API de datos de Amazon RDS, consulte Registro de llamadas a la API de datos con AWS CloudTrail en la Guía del usuario de Amazon RDS para Aurora.

4. Cuando haya terminado, seleccione Guardar cambios.

Eventos de lectura y escritura

Cuando configure su registro de seguimiento o almacén de datos de eventos para registrar eventos de administración, puede indicar si desea que se registren eventos de solo lectura, de solo escritura, o ambos.

- Lectura

  Los eventos de solo lectura incluyen los roles de API que leen sus recursos, pero no realizan cambios. Por ejemplo, los eventos de solo lectura incluyen las operaciones de la API de Amazon EC2 `DescribeSecurityGroups` y `DescribeSubnets`. Estas operaciones devuelven únicamente información sobre sus recursos de Amazon EC2 y no cambian las configuraciones.

- Escritura

  Los eventos de solo escritura incluyen funciones de API que modifican (o podrían modificar) sus recursos. Por ejemplo, las operaciones de la API de Amazon EC2 `RunInstances` y `TerminateInstances` modifican sus instancias.

Ejemplo: Registro de eventos de lectura y escritura en registros de seguimiento individuales

El ejemplo siguiente muestra cómo puede configurar registros de seguimiento para dividir la actividad de registro de una cuenta en diferentes buckets de S3: un bucket recibe los eventos de solo lectura y un segundo bucket, aquellos de solo escritura.

1. Usted crea un registro de seguimiento y elige un bucket de S3 llamado `read-only-bucket` para recibir los archivos de registro. A continuación, actualiza el registro de seguimiento para indicar que desea registrar los eventos de administración de Read (Lectura).
2. Usted crea un segundo registro de seguimiento y elige un bucket de S3 denominado `write-only-bucket` para recibir los archivos de registro. A continuación, actualiza el registro de seguimiento para indicar que desea registrar los eventos de administración de escritura.

3. En su cuenta se generan las operaciones de la API `DescribeInstances` y `TerminateInstances` de Amazon EC2.
4. La operación de API `DescribeInstances` es un evento de solo lectura y coincide con la configuración del primer registro de seguimiento. El registro de seguimiento registra y envía el evento al `read-only-bucket`.
5. La operación de API `TerminateInstances` es un evento de solo escritura y coincide con la configuración del segundo registro de seguimiento. El registro de seguimiento registra y envía el evento al `write-only-bucket`.

Registro de eventos con la AWS Command Line Interface

Puede configurar sus registros de seguimiento o los almacenes de datos de eventos para que registren los eventos de administración con la AWS CLI.

Temas

- Ejemplos: Registro de eventos de administración para los registros de seguimiento
- Ejemplos: Registros de eventos de administración para los almacenes de datos de eventos

Ejemplos: Registro de eventos de administración para los registros de seguimiento

Para saber si su registro de seguimiento está registrando los eventos de administración, ejecute el comando `get-event-selectors`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

El ejemplo siguiente devuelve la configuración predeterminada de un registro de seguimiento. De forma predeterminada, los registros de seguimiento registran todos los eventos de administración, registran los eventos de todos los orígenes de eventos y no registran los eventos de datos.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

Puede utilizar selectores de eventos básicos o avanzados para registrar los eventos de administración. No puede aplicar selectores de eventos ni selectores de eventos avanzados a un registro de seguimiento. Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes. En las siguientes secciones se proporcionan ejemplos de cómo registrar los eventos de administración mediante selectores de eventos avanzados y selectores de eventos básicos.

Temas

- Ejemplos: registro de eventos de administración para senderos mediante selectores de eventos avanzados
- Ejemplos: registrar los eventos de administración de los senderos mediante selectores de eventos básicos

Ejemplos: registro de eventos de administración para senderos mediante selectores de eventos avanzados

El siguiente ejemplo crea un selector de eventos avanzado para una ruta cuyo nombre *TrailName* incluye eventos de gestión de solo lectura y solo escritura (omitiendo el `readOnly` selector), pero excluye eventos (). AWS Key Management Service AWS KMS Como AWS KMS los eventos se consideran eventos de gestión y puede haber un gran volumen de ellos, pueden tener un impacto sustancial en su CloudTrail factura si tiene más de un registro que capture los eventos de administración.

Si elige no registrar eventos de administración, no se registran eventos de AWS KMS y no podrá cambiar la configuración del registro de eventos de AWS KMS.

Para comenzar de nuevo el registro de eventos de AWS KMS en un registro de seguimiento, quite el selector `eventSource` y ejecute de nuevo el comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
```

```
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

El ejemplo devuelve los selectores de eventos avanzados configurados para el registro de seguimiento.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para comenzar de nuevo el registro de eventos excluidos en un registro de seguimiento, quite el selector `eventSource`, como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
```

```
  }
]'
```

El siguiente ejemplo crea un selector de eventos avanzado para una ruta cuyo nombre *TrailName*incluye eventos de administración de solo lectura y solo escritura (omitiendo el `readOnly` selector), pero excluye los eventos de administración de Amazon RDS Data API. Para excluir los eventos de administración de la API de datos de Amazon RDS, especifique la fuente de eventos de la API de datos de Amazon RDS en el valor de cadena del `eventSource` campo:. `rdsdata.amazonaws.com`

Si decide no registrar los eventos de administración, los eventos de administración de la API de datos de Amazon RDS no se registran y no puede cambiar la configuración del registro de eventos de la API de datos de Amazon RDS.

Para volver a iniciar el registro de los eventos de administración de la API de datos de Amazon RDS en una ruta, quite el `eventSource` selector y vuelva a ejecutar el comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

El ejemplo devuelve los selectores de eventos avanzados configurados para el registro de seguimiento.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
```

```
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Para comenzar de nuevo el registro de eventos excluidos en un registro de seguimiento, quite el selector `eventSource`, como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Ejemplos: registrar los eventos de administración de los senderos mediante selectores de eventos básicos

Para configurar el registro de seguimiento para que registre los eventos de administración, ejecute el comando `put-event-selectors`. El ejemplo siguiente muestra cómo configurar su registro de seguimiento para que incluya todos los eventos de administración para dos objetos de S3. Puede especificar entre 1 y 5 selectores de eventos en los registros de seguimiento. Puede especificar entre 1 y 250 recursos de datos en los registros de seguimiento.

> **Note**
>
> El número máximo de recursos de datos de S3 es 250, independientemente del número de selectores de eventos.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
```

```
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

El ejemplo siguiente devuelve el selector de eventos configurado para el registro de seguimiento.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

Para excluir los eventos de AWS Key Management Service (AWS KMS) del registro de seguimiento, ejecute el comando `put-event-selectors` y añada el atributo `ExcludeManagementEventSources` con un valor de `kms.amazonaws.com`. En el siguiente ejemplo, se crea un selector de eventos para una ruta cuyo nombre incluye *TrailName*los eventos de gestión de solo lectura y solo de escritura, pero los excluye. AWS KMS Como AWS KMS puede generar un gran volumen de eventos, el usuario de este ejemplo podría querer limitar los eventos para administrar el costo de un registro de seguimiento.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

El ejemplo devuelve el selector de eventos configurado para el registro de seguimiento.

```
{
```

```
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

Para excluir los eventos de administración de la API de datos de Amazon RDS de los registros de una ruta, ejecute el `put-event-selectors` comando y añada el atributo `ExcludeManagementEventSources` con un valor de`rdsdata.amazonaws.com`. El siguiente ejemplo crea un selector de eventos para una ruta cuyo nombre *`TrailName`*incluye eventos de administración de solo lectura y solo escritura, pero excluye los eventos de administración de Amazon RDS Data API. Dado que la API de datos de Amazon RDS puede generar un gran volumen de eventos de administración, es posible que el usuario de este ejemplo desee limitar los eventos para administrar el costo de una ruta.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
}
```

Para volver a iniciar AWS KMS el registro de los eventos de administración de Amazon RDS Data API en una ruta, pase una cadena vacía como el valor de`ExcludeManagementEventSources`, tal y como se muestra en el siguiente comando.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Para registrar eventos de AWS KMS relevantes en un seguimiento como `Disable`, `Delete` y `ScheduleKey`, y excluir eventos de AWS KMS de gran volumen como `Encrypt`, `Decrypt` y `GenerateDataKey`, registre eventos de administración de solo escritura y mantenga la configuración predeterminada para registrar eventos de AWS KMS, como se muestra en el ejemplo siguiente.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Ejemplos: Registros de eventos de administración para los almacenes de datos de eventos

Para ver si el almacén de datos de eventos incluye eventos de administración, ejecute el comando get-event-data-store.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

A continuación, se muestra un ejemplo de respuesta. Las horas de creación y última actualización están en formato `timestamp`.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

Para crear un almacén de datos de eventos que incluya todos los eventos de administración, ejecute el comando create-event-data-store. No es necesario especificar ningún selector de eventos avanzado para incluir todos los eventos de administración.

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

Para crear un almacén de datos de eventos que excluya los eventos de AWS Key Management Service (AWS KMS), ejecute el comando `create-event-data-store` y especifique que `eventSource` no es igual que `kms.amazonaws.com`. En el ejemplo siguiente se crea un almacén de datos de eventos que incluye eventos de administración de solo lectura y de solo escritura, pero excluye los eventos de AWS KMS.

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
```

```
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Para crear un almacén de datos de eventos que excluya los eventos de administración de la API de datos de Amazon RDS, ejecute el `create-event-data-store` comando y especifique que `eventSource` no es igual. `rdsdata.amazonaws.com` En el ejemplo siguiente se crea un almacén de datos de eventos que incluye eventos de administración de solo lectura y de solo escritura, pero excluye los eventos de la API de datos de Amazon RDS.

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
```

```
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```


Registro de eventos con los SDK de AWS

Utilice la GetEventSelectorsoperación para comprobar si su ruta registra los eventos de administración de una ruta. Puede configurar sus senderos para registrar los eventos de administración con la PutEventSelectorsoperación. Para obtener más información, consulte la Referencia de la API de AWS CloudTrail.

Ejecute la GetEventDataStoreoperación para comprobar si su almacén de datos de eventos incluye eventos de gestión. Puede configurar sus almacenes de datos de eventos para incluir eventos de administración ejecutando las UpdateEventDataStoreoperaciones CreateEventDataStoreo. Para obtener más información, consulte Administrar CloudTrail Lake mediante la AWS CLI y la AWS CloudTrail API Reference.

Envío de eventos a Amazon CloudWatch Logs

En el caso de las rutas, CloudTrail admite el envío de datos y eventos de gestión a CloudWatch Logs. Cuando configuras tu ruta para enviar eventos a tu grupo de CloudWatch registros, CloudTrail envía solo los eventos que especifiques en tu ruta. Por ejemplo, si configuras tu ruta para registrar solo los eventos de administración, tu ruta solo entrega los eventos de administración a tu grupo de CloudWatch registros. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Registro de eventos de datos

De forma predeterminada, los registros y los almacenes de datos de eventos no registran eventos de datos. Se aplican cargos adicionales a los eventos de datos. Para obtener más información, consulte AWS CloudTrail Precios.

> **Note**
>
> Los eventos que registran tus rutas están disponibles en Amazon EventBridge. Por ejemplo, si decide registrar eventos de datos para objetos de S3, pero no eventos de administración, el registro de seguimiento procesará y registrará únicamente los eventos de datos relativos a los objetos de S3 indicados. Los eventos de datos de estos objetos de S3 están disponibles en Amazon EventBridge. Para obtener más información, consulta Eventos de los AWS servicios en la Guía del EventBridge usuario de Amazon.

Contenido

- Eventos de datos
  - Registrar eventos de datos con el AWS Management Console
  - Ejemplos: registrar eventos de datos para objetos de Amazon S3
  - Registrar los eventos de datos de los objetos de S3 en otras AWS cuentas
- Eventos de solo lectura y de solo escritura
- Registrar eventos de datos con AWS Command Line Interface
  - Registrar eventos de datos para senderos con el AWS CLI
    - Registrar eventos mediante selectores de eventos avanzados
    - Registre todos los eventos de Amazon S3 de un bucket de Amazon S3 mediante selectores de eventos avanzados

        - Registrar eventos de Amazon S3 en eventos de AWS Outposts mediante selectores de eventos avanzados
        - Registrar eventos mediante selectores de eventos básicos
    - Registrar los eventos de datos para los almacenes de datos de eventos con el AWS CLI
        - Incluir todos los eventos de Amazon S3 en un bucket
        - Incluir Amazon S3 en los eventos de AWS Outposts
- Registrar eventos de datos para la conformidad con AWS Config
- Registrar eventos de datos con los SDK AWS
- Envío de eventos a Amazon CloudWatch Logs

Eventos de datos

Los eventos de datos muestran información sobre las operaciones realizadas en un recurso o dentro de él. Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen.

Algunos ejemplos de eventos de datos son los siguientes:

- Actividad de la API en cuanto a objetos de Amazon S3 (por ejemplo, las operaciones `GetObject`, `DeleteObject` y `PutObject` de la API) en buckets y objetos en buckets.
- AWS Lambda actividad de ejecución de funciones (la `Invoke` API).
- CloudTrail `PutAuditEvents`actividad en un canal de CloudTrail Lake que se utiliza para registrar eventos del exterior AWS.
- Operaciones de la API `Publish` y `PublishBatch` de Amazon SNS sobre temas.

En la siguiente tabla, se muestran los tipos de eventos de datos disponibles para los registros de seguimiento y los almacenes de datos de eventos. En la columna Tipo de evento de datos (consola), se muestra la selección adecuada en la consola. La columna de valores resources.type muestra el `resources.type` valor que deberías especificar para incluir eventos de datos de ese tipo en tu almacén de datos de rutas o eventos mediante las AWS CLI API o. CloudTrail

En el caso de los registros de seguimiento, puede utilizar selectores de eventos básicos o avanzados para registrar eventos de datos para buckets de Amazon S3 y objetos de bucket, funciones de Lambda y tablas de DynamoDB (se muestran en las tres primeras filas de la tabla). Solo puede usar

selectores de eventos avanzados para registrar los tipos de eventos de datos que se muestran en las filas restantes.

En el caso de los almacenes de datos de eventos, puede utilizar selectores de eventos avanzados para que se incluyan eventos de datos únicamente.

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon DynamoDB	Actividad de la API a nivel de objeto de Amazon DynamoDB en las tablas (por ejemplo `PutItem`, `DeleteItem`, y las operaciones de la API). `UpdateItem` **Note** Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si	DynamoDB	`AWS::DynamoDB::Table`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir los eventos de streaming, añada un filtro en el campo `eventName`		
AWS Lambda	AWS Lambda actividad de ejecución de funciones (la `Invoke` API).	Lambda	`AWS::Lambda::Function`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon S3	Actividad de la API en cuanto a objetos de Amazon S3 (por ejemplo, las operaciones `GetObject` , `DeleteObject` y `PutObject` de la API) en buckets y objetos en buckets.	S3	`AWS::S3::Object`
AWS AppConfig	AWS AppConfig Actividad de la API para operaciones de configuración, como las llamadas a `StartConfiguration Session` y`GetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Intercambio de datos B2B	Actividad de la API de intercambio de datos entre empresas para operaciones de Transformer, como las llamadas a `GetTransformerJob` y `StartTransformerJob` .	Intercambio de datos entre empresas	`AWS::B2BI::Transformer`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon Bedrock	Actividad de la API de Amazon Bedrock en un alias de agente.	Alias de agente de Bedrock	`AWS::Bedrock::AgentAlias`
	Actividad de la API de Amazon Bedrock en una base de conocimientos.	Base de conocimientos de Bedrock	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront Actividad de la API en un KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Actividad de la API en un espacio de nombres.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Actividad de la API en un servicio.	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` actividad en un canal de CloudTrail Lake que se utiliza para registrar eventos externos AWS.	CloudTrail	`AWS::CloudTrail::Channel`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon CodeWhisperer	Actividad CodeWhisperer de la API de Amazon en una personalización.	CodeWhisperer personalización	`AWS::CodeWhisperer::Customization`
	Actividad CodeWhisperer de la API de Amazon en un perfil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Actividad de la API de Amazon Cognito en los grupos de identidades de Amazon Cognito.	Grupos de identidades de Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Actividad de la API de Amazon DynamoDB en los flujos.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	API directas de Amazon Elastic Block Store (EBS), como `PutSnapshotBlock`, `GetSnapshotBlock` y `ListChangedBlocks` en instantáneas de Amazon EBS.	API directas de Amazon EBS	`AWS::EC2::Snapshot`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon EMR	Actividad de la API de Amazon EMR en un espacio de trabajo de registros de escritura anticipada.	Espacio de trabajo de registro de escritura anticipada de EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Actividad de la API de Amazon FinSpace en entornos.	FinSpace	`AWS::FinSpace::Environment`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS Glue	AWS Glue Actividad de la API en tablas creadas por Lake Formation. **Note** AWS Glue Los eventos de datos para tablas actualmente solo se admiten en las siguientes regiones: • Este de EE. UU. (Norte de Virginia) • Este de EE. UU. (Ohio) • Oeste de EE. UU. (Oregón) • Europa (Irlanda)	Lake Formation	`AWS::Glue::Table`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	• Región de Asia-Pacífico (Tokio)		
Amazon GuardDuty	Actividad GuardDuty de la API de Amazon para un detector.	GuardDuty detector	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging Actividad de la API en los almacenes de datos.	Almacén de datos de imágenes médicas	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Actividad de la API en los certificados.	Certificado IoT	`AWS::IoT::Certificate`
	AWS IoT Actividad de la API en las cosas.	Cosa de IoT	`AWS::IoT::Thing`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS IoT Greengrass Version 2	Actividad de la API de Greengrass desde un dispositivo principal de Greengrass en una versión de componentes. **Note** Greengrass no registra los eventos de acceso denegado.	Versión del componente IoT Greengrass	`AWS::GreengrassV2::ComponentVersion`
	Actividad de la API de Greengrass desde un dispositivo principal de Greengrass en una implementación. **Note** Greengrass no registra los eventos de acceso denegado.	Despliegue de IoT Greengrass	`AWS::GreengrassV2::Deployment`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS IoT SiteWise	Actividad de SiteWise la API de IoT en los activos.	SiteWise Activo de IoT	`AWS::IoTSiteWise::Asset`
	Actividad SiteWise de la API de IoT en series temporales.	Series SiteWise temporales de IoT	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Actividad TwinMaker de la API de IoT en una entidad.	TwinMaker Entidad de IoT	`AWS::IoTTwinMaker::Entity`
	Actividad de TwinMaker la API de IoT en un espacio de trabajo.	TwinMaker Espacio de trabajo de IoT	`AWS::IoTTwinMaker::Workspace`
Clasificación de Amazon Kendra Intelligent	Actividad de la API de Amazon Kendra Intelligent Ranking en los planes de ejecución de nuevas puntuaciones.	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (para Apache Cassandra)	Actividad de la API de Amazon Keyspaces en una tabla.	Mesa Cassandra	`AWS::Cassandra::Table`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon Kinesis	Actividad de la API de Amazon Kinesis en transmisiones de video, como llamadas a `GetMedia` y `PutMedia`.	Kinesis Video Streams	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Actividad de la API de Amazon Managed Blockchain en una red.	Red de Managed Blockchain	`AWS::ManagedBlockchain::Network`
	Llamadas JSON-RPC de Amazon Managed Blockchain en nodos de Ethereum, como `eth_getBalance` o `eth_getBlockByNumber` .	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Gráfico de Amazon Neptune	Actividades de la API de datos, por ejemplo, consultas, algoritmos o búsquedas vectoriales, en un gráfico de Neptune.	Gráfico de Neptune	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Conector para la actividad de la API de Active Directory.	AWS Private CA Conector para Active Directory	`AWS::PCAConnectorAD::Connector`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
Amazon Q Business	Actividad de la API de Amazon Q Business en una aplicación.	Aplicación de Amazon Q Business	`AWS::QBusiness::Application`
	Actividad de la API de Amazon Q Business en un origen de datos.	Origen de datos de Amazon Q Business	`AWS::QBusiness::DataSource`
	Actividad de la API de Amazon Q Business en un índice.	Índice de Amazon Q Business	`AWS::QBusiness::Index`
	Actividad de la API de Amazon Q Business en una experiencia web.	Experiencia web de Amazon Q Business	`AWS::QBusiness::WebExperience`
Amazon RDS	Actividad de la API de Amazon RDS en un clúster de base de datos.	API de datos de RDS: clúster de base de datos	`AWS::RDS::DBCluster`
Amazon S3	Actividad de la API de Amazon S3 en los puntos de acceso.	Punto de acceso de S3	`AWS::S3::AccessPoint`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	Actividad de la API en los puntos de acceso de Amazon S3 Object Lambda, como las llamadas a `CompleteMultipartUpload` y `GetObject` .	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 en Outposts	Actividad de la API en cuanto a objetos de Amazon S3 en Outposts.	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Actividad de Amazon en los puntos finales.	SageMaker punto final	`AWS::SageMaker::Endpoint`
	Actividad SageMaker de la API de Amazon en tiendas destacadas.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
	Actividad de la SageMaker API de Amazon en componentes de prueba de experimentos.	SageMaker métricas (componente de prueba de experimentos)	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Operaciones de la API `Publish` de Amazon SNS en los puntos de conexión de la plataforma.	Punto de conexión de la plataforma de SNS	`AWS::SNS::PlatformEndpoint`
	Operaciones de la API `Publish` y `PublishBatch` de Amazon SNS sobre temas.	Tema de SNS	`AWS::SNS::Topic`
Amazon SQS	Actividad de la API de Amazon SQS en los mensajes.	SQS	`AWS::SQS::Queue`
AWS Supply Chain	AWS Supply Chain Actividad de la API en una instancia.	Cadena de suministro	`AWS::SCN::Instance`
Amazon SWF	Actividad de la API Amazon SWF en los dominios.	Dominio SWF	`AWS::SWF::Domain`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS Systems Manager	Actividad de la API de Systems Manager en los canales de control.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Actividad de la API de Systems Manager en los nodos gestionados.	Nodo gestionado por Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Actividad de la API `Query` de Amazon Timestream en las bases de datos.	Base de datos de Timestream	`AWS::Timestream::Database`
	Actividad de la API `Query` de Amazon Timestream en las tablas.	Tabla de Timestream	`AWS::Timestream::Table`
Amazon Verified Permissions	Actividad de la API de Amazon Verified Permissions en un almacén de políticas.	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`
Amazon WorkSpaces Thin Client	WorkSpaces Actividad de la API de Thin Client en un dispositivo.	Dispositivo de cliente ligero	`AWS::ThinClient::Device`
	WorkSpaces Actividad de la API de Thin Client en un entorno.	Entorno de cliente ligero	`AWS::ThinClient::Environment`

AWS servicio	Descripción	Tipo de evento de datos (consola)	resources.type value
AWS X-Ray	Actividad de la API X-Ray en las trazas.	Rastro de rayos X	`AWS::XRay::Trace`

El registro de los eventos de datos está deshabilitado de forma predeterminada cuando crea un registro de seguimiento o un almacén de datos de eventos. Para registrar CloudTrail los eventos de datos, debe añadir de forma explícita los recursos o tipos de recursos compatibles para los que desea recopilar la actividad. Para más información, consulte Creación de un registro de seguimiento y Cree un banco de datos de CloudTrail eventos para eventos.

En un registro de seguimiento o un almacén de datos de eventos de una sola región, puede registrar eventos de datos solo para los recursos a los que puede acceder en esa región. Aunque los buckets de S3 son globales, AWS Lambda las funciones y las tablas de DynamoDB son regionales.

Se aplican cargos adicionales para registrar eventos de datos. Para CloudTrail conocer los precios, consulte Precios.AWS CloudTrail

Registrar eventos de datos con el AWS Management Console

En los siguientes procedimientos, se describe cómo actualizar un almacén de datos de eventos existente o un registro de seguimiento de eventos para registrar los eventos de datos mediante la AWS Management Console. Para obtener información acerca de cómo crear un almacén de datos de eventos para registrar eventos de datos, consulte Cree un banco de datos de CloudTrail eventos para eventos. Para obtener más información sobre cómo crear un registro de seguimiento para registrar eventos de datos, consulte Creación de un registro de seguimiento en la consola.

En el caso de los registros de seguimiento, los pasos para registrar los eventos de datos varían en función de si se utilizan selectores de eventos avanzados o selectores de eventos básicos. Puede registrar eventos de datos para todos los tipos de eventos de datos mediante selectores de eventos avanzados, pero solo puede registrar eventos de datos para buckets de Amazon S3 y objetos de bucket, AWS Lambda funciones y tablas de Amazon DynamoDB utilizando selectores de eventos básicos.

Actualización de un almacén de datos de eventos existente para registrar los eventos de datos en el AWS Management Console

Utilice los siguientes procedimientos para actualizar un almacén de datos de eventos existente para registrar los eventos de datos.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. En el panel de navegación, en Lago, elija Almacenes de datos de eventos.
3. En la página Almacenes de datos de eventos, seleccione el almacén de datos de eventos que desee actualizar.

> **Note**
>
> Solo puede habilitar los eventos de datos en los almacenes de datos de eventos que contienen CloudTrail eventos. No puede habilitar los eventos de datos en CloudTrail los almacenes de datos de eventos para elementos de AWS Config configuración, eventos de CloudTrail Insights o no AWS eventos.

4. En la página de detalles, en Eventos de datos, seleccione Editar.
5. Si aún no registra eventos de datos, elija la casilla Data events (Eventos de datos).
6. En Data event type (Tipo de evento de datos), elija el tipo de recurso en el que desea registrar los eventos de datos.
7. Elija una plantilla de selección de registros. CloudTrail incluye plantillas predefinidas que registran todos los eventos de datos del tipo de recurso. Para crear una plantilla de selector de registros personalizada, elija Custom (Personalizado).

> **Note**
>
> Si elige una plantilla predefinida para los depósitos de S3, podrá registrar los eventos de datos de todos los depósitos que se encuentren actualmente en su AWS cuenta y de los que cree una vez que haya terminado de crear el banco de datos de eventos. También permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
> Si el almacén de datos de eventos solo se aplica a una región, seleccionar una plantilla predefinida que registra todos los buckets de S3 permite el registro de eventos de

datos de todos los buckets en la misma región que el almacén de datos de eventos, así como de cualquier otro bucket que cree posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de su AWS cuenta.
Si va a crear un banco de datos de eventos para todas las regiones, al elegir una plantilla predefinida para las funciones de Lambda se habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en su AWS cuenta y para cualquier función de Lambda que pueda crear en cualquier región una vez que haya terminado de crear el banco de datos de eventos. Si va a crear un banco de datos de eventos para una sola región, esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear el banco de datos de seguimiento o evento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
El registro de eventos de datos para todas las funciones también permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

8. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo opcional para un selector de eventos avanzado, como “Registrar eventos de datos para solo dos buckets de S3”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
9. En Advanced event selectors (Selectores de eventos avanzados), cree una expresión para los recursos específicos en los que desea registrar eventos de datos. Puede omitir este paso si utiliza una plantilla de registro predefinida.

   a. Elija uno de los siguientes campos.

   - **`readOnly`**- se `readOnly` puede configurar para que sea igual a un valor de `true` o`false`. Los eventos de datos de solo lectura son eventos que no cambian el estado de un recurso, como eventos `Get*` o `Describe*`. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`. Para registrar eventos `read` y `write`, no agregue un selector de `readOnly`.
   - **`eventName`**: `eventName` puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de datos registrado CloudTrail, como `PutBucketGetItem`, o`GetSnapshotBlock`.

- **`resources.ARN`**- Puede usar cualquier operador con`resources.ARN`, pero si usa valores iguales o no iguales, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo que especificó en la plantilla como valor de. `resources.type`

  En la siguiente tabla, se muestra el formato de ARN de cada `resources.type`.

  > **Note**
  >
  > No puede usar el `resources.ARN` campo para filtrar los tipos de recursos que no tienen ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*

resources.type	resources.ARN
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*

resources.type	resources.ARN
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*

resources.type	resources.ARN
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	El ARN debe estar en uno de los siguientes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*

resources.type	resources.ARN
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir los eventos de streaming, añade un filtro en el `eventName` campo.

[2] Para registrar todos los eventos de datos de todos los objetos en un bucket de S3 específico, utilice el operador `StartsWith` e incluya solo el ARN del bucket como valor coincidente. La barra diagonal final es intencional; no la excluya.

[3] Para registrar eventos en todos los objetos de un punto de acceso de S3, se recomienda que utilice solo el ARN del punto de acceso. No incluya la ruta de acceso del objeto y utilice los operadores `StartsWith` o `NotStartsWith`.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte Acciones, recursos y claves de condición en la Guía del usuario de AWS Identity and Access Management .

b. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones. Por ejemplo, para excluir los eventos de datos de dos cubos de S3 de los eventos de datos que se registran en el almacén de datos de eventos, puede establecer el campo en Resources.ARN, configurar el operador para no comienza por y, a continuación, pegar el ARN de un bucket de S3 o buscar los cubos de S3 para los que no desea registrar eventos.

   Para agregar el segundo bucket de S3, seleccione + Condición y, a continuación, repita la instrucción anterior, pegue el ARN o busque un bucket diferente.

   > **Note**
   >
   > Puede tener un máximo de 500 valores para todos los selectores de un almacén de datos de eventos. Esto incluye matrices de varios valores para un selector como `eventName`. Si tiene valores únicos para todos los selectores, puede agregar un máximo de 500 condiciones a un selector.
   > Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un banco de datos de eventos. Puede registrar todas las funciones con una plantilla de selector predefinida, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear el banco de datos de eventos en la consola y, a continuación, usarlo AWS CLI para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Registrar eventos de datos con AWS Command Line Interface.

c. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos. Por ejemplo, no especifique un ARN en un selector para que sea igual a un valor y luego especifique que el ARN no sea igual al mismo valor en otro selector.

10. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos). Repita desde el paso 6 hasta este paso a fin de configurar selectores de eventos avanzados para el tipo de evento de datos.

11. Una vez que haya revisado y verificado las elecciones, seleccione Guardar cambios.

Actualización de un registro existente para registrar eventos de datos con selectores de eventos avanzados en AWS Management Console

En el AWS Management Console, si su ruta utiliza selectores de eventos avanzados, puede elegir entre plantillas predefinidas que registran todos los eventos de datos en un recurso seleccionado. Después de elegir una plantilla de selector de registros, puede personalizar la plantilla con el fin de incluir solo los eventos de datos que más desee ver. Para obtener más información y sugerencias sobre la utilización de selectores de eventos avanzados, consulte Registrar eventos mediante selectores de eventos avanzados en este tema.

1. En las páginas del panel de control o de rutas de la CloudTrail consola, elige la ruta que quieres actualizar.
2. En la página de detalles, en Eventos de datos, seleccione Editar.
3. Si aún no registra eventos de datos, elija la casilla Data events (Eventos de datos).
4. En Data event type (Tipo de evento de datos), elija el tipo de recurso en el que desea registrar los eventos de datos.
5. Elige una plantilla de selección de registros. CloudTrail incluye plantillas predefinidas que registran todos los eventos de datos del tipo de recurso. Para crear una plantilla de selector de registros personalizada, elija Custom (Personalizado).

> **Note**
>
> Si eliges una plantilla predefinida para los depósitos de S3, podrás registrar los eventos de datos de todos los depósitos que hay actualmente en tu AWS cuenta y de los que crees una vez que hayas terminado de crear el registro. También permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
> Si el registro de seguimiento solo aplica a una región, elegir una plantilla predefinida que registra todos los buckets de S3 permite el registro de eventos de datos de todos los buckets en la misma región que el registro de seguimiento, así como de cualquier otro bucket que cree posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de su AWS cuenta.
> Si va a crear un registro para todas las regiones, al elegir una plantilla predefinida para las funciones de Lambda se habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en su AWS cuenta y para cualquier función

de Lambda que pueda crear en cualquier región una vez que haya terminado de crear el registro. Si va a crear una ruta para una sola región (en el caso de las rutas, solo puede hacerlo mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región en su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
El registro de eventos de datos para todas las funciones también permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

6. (Opcional) En Nombre del selector, escriba un nombre para identificar el selector. El nombre del selector es un nombre descriptivo opcional para un selector de eventos avanzado, como “Registrar eventos de datos para solo dos buckets de S3”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
7. En Advanced event selectors (Selectores de eventos avanzados), cree una expresión para los recursos específicos en los que desea registrar eventos de datos. Puede omitir este paso si utiliza una plantilla de registro predefinida.

   a. Elija uno de los siguientes campos.

   - **`readOnly`**- se `readOnly` puede configurar para que sea igual a un valor de `true` o`false`. Los eventos de datos de solo lectura son eventos que no cambian el estado de un recurso, como eventos `Get*` o `Describe*`. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`. Para registrar eventos `read` y `write`, no agregue un selector de `readOnly`.
   - **`eventName`**: `eventName` puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de datos registrado CloudTrail, como `PutBucketGetItem`, o`GetSnapshotBlock`.
   - **`resources.ARN`**- Puede usar cualquier operador con`resources.ARN`, pero si usa valores iguales o no iguales, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo que especificó en la plantilla como valor de. `resources.type`

     En la siguiente tabla, se muestra el formato de ARN de cada `resources.type`.

> **Note**
>
> No puede usar el `resources.ARN` campo para filtrar los tipos de recursos que no tienen ARN.

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`
`AWS::Bedrock::AgentAlias`	`arn:partition :bedrock: region:account_ID :agent-alias/ agent_ID/alias_ID`
`AWS::Bedrock::KnowledgeBase`	`arn:partition :bedrock: region:account_ID :knowledge-base/knowledge_base_ID`

resources.type	resources.ARN
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*

resources.type	resources.ARN
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*

resources.type	resources.ARN
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*

resources.type	resources.ARN
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	El ARN debe estar en uno de los siguientes formatos: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
`AWS::ThinClient::Environment`	`arn:partition :thinclient: region:account_ID :environment/ environment_ID`
`AWS::Timestream::Database`	`arn:partition :timestream: region:account_ID :database/ database_name`
`AWS::Timestream::Table`	`arn:partition :timestream: region:account_ID :database/ database_name /table/table_name`
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Para las tablas con flujos habilitados, el campo `resources` del evento de datos contiene `AWS::DynamoDB::Stream` y `AWS::DynamoDB::Table`. Si especifica `AWS::DynamoDB::Table` como `resources.type`, registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir los eventos de streaming, añade un filtro en el `eventName` campo.

[2] Para registrar todos los eventos de datos de todos los objetos en un bucket de S3 específico, utilice el operador `StartsWith` e incluya solo el ARN del bucket como valor coincidente. La barra diagonal final es intencional; no la excluya.

[3] Para registrar eventos en todos los objetos de un punto de acceso de S3, se recomienda que utilice solo el ARN del punto de acceso. No incluya la ruta de acceso del objeto y utilice los operadores `StartsWith` o `NotStartsWith`.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte Acciones, recursos y claves de condición en la Guía del usuario de AWS Identity and Access Management .

b. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones. Por ejemplo, para excluir los eventos de datos de dos cubos de S3 de los eventos de datos que se registran en su ruta, puede establecer el campo en Resources.ARN, configurar el operador para no comienza por y, a continuación, pegar el ARN de un bucket de S3 o buscar los cubos de S3 para los que no desea registrar eventos.

   Para agregar el segundo bucket de S3, seleccione + Condición y, a continuación, repita la instrucción anterior, pegue el ARN o busque un bucket diferente.

   > **Note**
   >
   > Puede tener un máximo de 500 valores para todos los selectores de un registro de seguimiento. Esto incluye matrices de varios valores para un selector como `eventName`. Si tiene valores únicos para todos los selectores, puede agregar un máximo de 500 condiciones a un selector.
   > Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Puede registrar todas las funciones con una plantilla de selector predefinida, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear la ruta en la consola y, a continuación, utilizarla AWS CLI para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Registrar eventos de datos con AWS Command Line Interface.

c. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos. Por ejemplo, no especifique un ARN en un selector para que sea igual a un valor y luego especifique que el ARN no sea igual al mismo valor en otro selector.

8. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos). Repita desde el paso 4 hasta este paso a fin de configurar selectores de eventos avanzados para el tipo de evento de datos.
9. Una vez que haya revisado y verificado las elecciones, seleccione Guardar cambios.

Actualice un registro existente para registrar los eventos de datos con los selectores de eventos básicos de AWS Management Console

Utilice los siguientes procedimientos para actualizar un registro de seguimiento existente para registrar los eventos de datos con selectores de eventos básicos.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. Abre la página Rutas de la CloudTrail consola y elige el nombre de la ruta.

> **Note**
>
> Aunque puede editar un registro de seguimiento existente para registrar eventos de datos, como práctica recomendada, considere la posibilidad de crear un registro de seguimiento independiente específicamente para registrar eventos de datos.

3. En Data events (Eventos de datos), elija Edit (Editar).
4. Para buckets de Amazon S3:
   a. En Data event source (Fuente de evento de datos), elija S3.
   b. Puede registrar All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) o bien, especificar buckets o funciones individuales. De forma predeterminada, los eventos de datos se registran para todos los buckets de S3 actuales y futuros.

> **Note**
>
> Si mantiene la opción predeterminada Todos los depósitos de S3 actuales y futuros, se permite registrar los eventos de datos de todos los depósitos que se encuentren actualmente en su AWS cuenta y de todos los depósitos que cree una vez que haya terminado de crear la ruta. También permite registrar la actividad de eventos de datos realizada por cualquier usuario o rol de tu AWS cuenta, incluso si esa actividad se realiza en un bucket que pertenece a otra cuenta. AWS
> Si va a crear una ruta para una sola región (se hace mediante la AWS CLI), al seleccionar la opción Seleccione todos los depósitos de S3 de su cuenta, se registrarán los eventos de datos de todos los grupos de la misma región que su ruta y de todos los grupos que cree posteriormente en esa región. No registrará

los eventos de datos de los buckets de Amazon S3 en otras regiones de su AWS cuenta.

c. Si conserva la opción predeterminada, All current and future S3 buckets (Todos los buckets de S3 actuales y futuros), elija registrar eventos de Read (Lectura), Write (Escritura) o ambos.

d. Para seleccionar buckets individuales, desmarque las casillas de verificación Read (Lectura) y Write (Escritura) en All current and future S3 buckets (Todos los buckets de S3 actuales y futuros). En Individual bucket selection (Selección de bucket individual), busque un bucket en el que registrar los eventos de datos. Para buscar buckets específicos, escriba un prefijo de bucket para el bucket que desee. En esta ventana puede seleccionar varios buckets. Elija Add bucket (Agregar bucket) para registrar eventos de datos en más buckets. Elija registrar eventos de Read (Lectura), como `GetObject`, Write (Escritura), como `PutObject`, o de ambos.

   Esta configuración tiene prioridad sobre la configuración individual de cada bucket. Por ejemplo, si establece la configuración para que se registren los eventos de tipo Read de todos los buckets de S3 y posteriormente decide agregar un determinado bucket en el registro de eventos de datos, la opción Read ya aparecerá seleccionada en el bucket que agregue. Esta selección no se puede anular. Solo se puede configurar la opción Write.

   Para eliminar un bucket del registro, elija X.

5. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos).

6. Para funciones Lambda:

   a. En Data event source (Fuente de evento de datos), elija Lambda.

   b. En Lambda function (Función Lambda), elija All regions (Todas las regiones) para registrar todas las funciones Lambda, o Input function as ARN (Función de entrada como ARN) a fin de registrar eventos de datos en una función específica.

      Para registrar eventos de datos de todas las funciones Lambda de su cuenta de AWS , seleccione Log all current and future functions (Registrar todas las funciones actuales y futuras). Esta configuración tiene prioridad sobre la configuración individual de cada función. Se registran todas las funciones aunque no se muestren.

> **Note**
>
> Si va a crear un registro de seguimiento para todas las regiones, esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en la cuenta de AWS , así como de cualquier función Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear una ruta para una sola región (mediante la AWS CLI), esta selección habilita el registro de eventos de datos para todas las funciones que se encuentran actualmente en esa región de su AWS cuenta y para cualquier función de Lambda que pueda crear en esa región una vez que haya terminado de crear la ruta. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.
> El registro de los eventos de datos para todas las funciones también permite registrar la actividad de los eventos de datos realizada por cualquier usuario o función de su AWS cuenta, incluso si esa actividad se realiza en una función que pertenece a otra AWS cuenta.

c. Si elige Input function as ARN (Función de entrada como ARN), ingrese el ARN de una función Lambda.

> **Note**
>
> Si tiene más de 15 000 funciones Lambda en su cuenta, no podrá ver ni seleccionar todas las funciones de la CloudTrail consola al crear un registro. Sí que puede seleccionar la opción para registrar todas las funciones, aunque estas no se muestren. Si desea registrar eventos de datos para funciones específicas, puede añadir manualmente una función si conoce su ARN. También puede terminar de crear la ruta en la consola y, a continuación, utilizar el put-event-selectors comando AWS CLI and the para configurar el registro de eventos de datos para funciones Lambda específicas. Para obtener más información, consulte Administrar senderos con el AWS CLI.

7. Para agregar otro tipo de datos en el que registrar eventos de datos, elija Add data event type (Agregar tipo de evento de datos).
8. Para tablas de DynamoDB:

   a. En Data event source (Fuente de evento de datos), elija DynamoDB.

b. En DynamoDB table selection (Selección de tabla de DynamoDB), elija Browse (Examinar) para seleccionar una tabla o pegue el ARN de una tabla de DynamoDB a la que tenga acceso. El ARN de la tabla de DynamoDB utiliza el siguiente formato:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Para agregar otra tabla, elija Add row (Agregar fila) y busque una tabla o pegue el ARN de una tabla a la que tenga acceso.

9. Elija Guardar cambios.

Ejemplos: registrar eventos de datos para objetos de Amazon S3

Registrar eventos de datos de todos los objetos de S3 de un bucket de S3

En el ejemplo siguiente, se ilustra cómo funciona el registro cuando se configura para todos los eventos de datos de un bucket de S3 llamado *bucket-1*. En este ejemplo, el CloudTrail usuario especificó un prefijo vacío y la opción de registrar los eventos de lectura y escritura de datos.

1. Un usuario carga un objeto en `bucket-1`.
2. La operación de API `PutObject` es una API de nivel de objetos de Amazon S3. Se registra como un evento de datos en CloudTrail. Como el CloudTrail usuario especificó un depósito de S3 con un prefijo vacío, se registran los eventos que se producen en cualquier objeto de ese depósito. El registro de seguimiento o almacén de datos de eventos procesa y registra el evento.
3. Otro usuario carga un objeto en `bucket-2`.
4. La operación de API `PutObject` tuvo lugar en un objeto de un bucket de S3 que no estaba especificado en el registro de seguimiento o el almacén de datos de eventos. El registro de seguimiento o el almacén de datos de eventos no registra el evento.

Registrar eventos de datos para objetos de S3 concretos

En el ejemplo siguiente, se muestra cómo funciona el registro cuando se configura un registro de seguimiento o un almacén de datos de eventos para registrar eventos de objetos de S3 específicos. En este ejemplo, el CloudTrail usuario especificó un bucket de S3 denominado ***bucket-3***, con el prefijo ***my-images*** y la opción de registrar únicamente los eventos de Write data.

1. Un usuario elimina un objeto que comienza con el prefijo `my-images` del bucket; por ejemplo `arn:aws:s3:::bucket-3/my-images/example.jpg`.

2. La operación de API `DeleteObject` es una API de nivel de objetos de Amazon S3. Se graba como un evento de escritura de datos en. CloudTrail El evento tuvo lugar en un objeto que coincide con el bucket de S3 y el prefijo especificados en el registro de seguimiento o almacén de datos de eventos. El registro de seguimiento o almacén de datos de eventos procesa y registra el evento.
3. Otro usuario elimina un objeto con un prefijo diferente del bucket de S3; por ejemplo `arn:aws:s3:::bucket-3/my-videos/example.avi`.
4. El evento tuvo lugar en un objeto que no coincide con el prefijo especificado en el registro de seguimiento o almacén de datos de eventos. El registro de seguimiento o el almacén de datos de eventos no registra el evento.
5. Un usuario llama a la operación de API `GetObject` para el objeto `arn:aws:s3:::bucket-3/my-images/example.jpg`.
6. El evento tuvo lugar en un bucket y un prefijo especificados en el registro de seguimiento o almacén de datos de eventos, pero `GetObject` es una API de nivel de objetos de Amazon S3 de tipo lectura. Se registra como un evento de lectura de datos en CloudTrail, y el almacén de datos de seguimiento o evento no está configurado para registrar eventos de lectura. El registro de seguimiento o el almacén de datos de eventos no registra el evento.

> **Note**
>
> En el caso de los registros de seguimiento, si registra eventos de datos para determinados buckets de Amazon S3, recomendamos que no utilice un bucket de Amazon S3 para el que registre eventos de datos si desea recibir los archivos de registros que especificó en la sección de eventos de datos del registro de seguimiento. Si se utiliza el mismo bucket de Amazon S3, el seguimiento registra un evento de datos cada vez que los archivos de registros se envían al bucket de Amazon S3. Los archivos de registro contienen el total de eventos enviados a intervalos y, por tanto, no hay una relación 1:1 entre el evento y el archivo de registro; el evento se registra en el siguiente archivo de registro. Por ejemplo, cuando CloudTrail entrega registros, el `PutObject` evento se produce en el bucket de S3. Si el bucket de S3 también está indicado en la sección de eventos de datos, el registro de seguimiento procesa y registra el evento `PutObject` como evento de datos. Esta acción es otro evento `PutObject` y el registro de seguimiento procesa y registra el evento una vez más. Para obtener más información, consulte Cómo CloudTrail funciona.
> Para evitar el registro de eventos de datos para el bucket de Amazon S3 donde recibe los archivos de registro si configura un registro para registrar todos los eventos de datos de

Amazon S3 de su AWS cuenta, considere la posibilidad de configurar la entrega de archivos de registro a un bucket de Amazon S3 que pertenezca a otra AWS cuenta. Para obtener más información, consulte Recepción de archivos de CloudTrail registro de varias cuentas.

Registrar los eventos de datos de los objetos de S3 en otras AWS cuentas

Al configurar su ruta para registrar eventos de datos, también puede especificar objetos de S3 que pertenezcan a otras AWS cuentas. Cuando se produce un evento en un objeto específico, CloudTrail evalúa si el evento coincide con alguna de las rutas de cada cuenta. Si el evento coincide con la configuración de un registro de seguimiento, este procesa y registra el evento para dicha cuenta. Por lo general, tanto los intermediarios de la API como los propietarios de recursos pueden recibir eventos.

Si tiene un objeto de S3 y lo indica en su registro de seguimiento, su registro de seguimiento registra eventos que se produzcan en el objeto de su cuenta. Dado que posee el objeto, su registro de seguimiento también registra los eventos cuando otras cuentas llaman al objeto.

Si especifica un objeto de S3 en su registro de seguimiento y otra cuenta posee el objeto, su registro de seguimiento únicamente registra los eventos que se produzcan en dicho objeto en su cuenta. Su registro de seguimiento no registra los eventos que se producen en otras cuentas.

Ejemplo: Registrar eventos de datos para un objeto de Amazon S3 para dos cuentas de AWS

El siguiente ejemplo muestra cómo se configuran dos AWS cuentas CloudTrail para registrar eventos para el mismo objeto de S3.

1. En su cuenta, usted desea que su registro de seguimiento registre eventos de datos para todos los objetos en el bucket de S3 denominado `owner-bucket`. Configura el registro de seguimiento indicando el bucket de S3 con un prefijo de objeto vacío.
2. Bob tiene una cuenta independiente a la que se ha permitido el acceso al bucket de S3. Bob también quiere registrar los eventos de datos para todos los objetos en el mismo bucket de S3. Para su registro de seguimiento, configura su registro de seguimiento e indica el mismo bucket de S3 con un prefijo de objeto vacío.
3. Bob carga un objeto al bucket de S3 con la operación de API `PutObject`.
4. Este evento se produjo en su cuenta y coincide con la configuración de su registro de seguimiento. El registro de seguimiento de Bob procesa y registra el evento.

5. Dado que posee el bucket de S3 y el evento coincide con la configuración de su registro de seguimiento, su registro de seguimiento también procesa y registra el mismo evento. Como ahora hay dos copias del evento (una registrada en la ruta de Bob y otra registrada en la suya), se CloudTrail cobran dos copias del evento de datos.
6. Usted carga un objeto en el bucket de S3.
7. Este evento se produce en su cuenta y coincide con la configuración de su registro de seguimiento. Su registro de seguimiento procesa y registra el evento.
8. Como el evento no se produjo en la cuenta de Bob y él no es el propietario del depósito S3, la ruta de Bob no registra el evento. CloudTrail cobra solo por una copia de este evento de datos.

Ejemplo: registrar los eventos de datos de todos los depósitos, incluido un depósito de S3 utilizado por dos cuentas AWS

El siguiente ejemplo muestra el comportamiento de registro cuando la opción Seleccionar todos los buckets de S3 de tu cuenta está habilitada para las rutas que recopilan eventos de datos en una AWS cuenta.

1. En su cuenta, desea que su registro de seguimiento registre eventos de datos para todos los buckets de S3. Puede configurar el registro de seguimiento al elegir eventos de Read (Lectura), eventos de Write (Escritura), o ambos para All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) en Data events (Eventos de datos).
2. Bob tiene una cuenta independiente a la que se le ha concedido acceso a un bucket de S3 en su cuenta. Desea registrar eventos de datos para el bucket al que tiene acceso. Configura su registro de seguimiento para obtener eventos de datos para todos los buckets de S3.
3. Bob carga un objeto al bucket de S3 con la operación de API `PutObject`.
4. Este evento se produjo en su cuenta y coincide con la configuración de su registro de seguimiento. El registro de seguimiento de Bob procesa y registra el evento.
5. Dado que posee el bucket de S3 y el evento coincide con la configuración de su registro de seguimiento, su registro de seguimiento también procesa y registra el evento. Como ahora hay dos copias del evento (una registrada en la ruta de Bob y otra registrada en la tuya), CloudTrail cobra a cada cuenta una copia del evento de datos.
6. Usted carga un objeto en el bucket de S3.
7. Este evento se produce en su cuenta y coincide con la configuración de su registro de seguimiento. Su registro de seguimiento procesa y registra el evento.

8. Como el evento no se produjo en la cuenta de Bob y él no es el propietario del depósito S3, la ruta de Bob no registra el evento. CloudTrail solo cobra una copia de este evento de datos en tu cuenta.
9. Un tercer usuario, Mary, tiene acceso al bucket de S3 y ejecuta una operación `GetObject` en el bucket. Tiene un registro de seguimiento configurado para registrar eventos de datos en todos los buckets de S3 de su cuenta. Como es la persona que llama a la API, CloudTrail registra un evento de datos en su registro. Aunque Bob tiene acceso al bucket, no es el propietario del recurso, por lo que no se registra ningún evento en su registro de seguimiento esta vez. Como propietario del recurso, recibes un evento en tu registro sobre la `GetObject` operación a la que Mary convocó. CloudTrailcobra a tu cuenta y a la de Mary por cada copia del evento de datos: una en Mary's Trail y otra en la tuya.

Eventos de solo lectura y de solo escritura

Cuando configure su registro de seguimiento o almacén de datos de eventos para registrar eventos de datos y administración, puede indicar si desea que se registren eventos de solo lectura, de solo escritura, o ambos.

- Lectura

  Los eventos de Read (Lectura) incluyen operaciones de la API que leen sus recursos, pero no realizan cambios. Por ejemplo, los eventos de solo lectura incluyen las operaciones de la API de Amazon EC2 `DescribeSecurityGroups` y `DescribeSubnets`. Estas operaciones devuelven únicamente información sobre sus recursos de Amazon EC2 y no cambian las configuraciones.

- Escritura

  Los eventos de Write (Escritura) incluyen operaciones de la API que modifican (o podrían modificar) sus recursos. Por ejemplo, las operaciones de la API de Amazon EC2 `RunInstances` y `TerminateInstances` modifican sus instancias.

Ejemplo: Registro de eventos de lectura y escritura en registros de seguimiento individuales

El ejemplo siguiente muestra cómo puede configurar registros de seguimiento para dividir la actividad de registro de una cuenta en diferentes buckets de S3: un bucket recibe los eventos de solo lectura y un segundo bucket, aquellos de solo escritura.

1. Usted crea un registro de seguimiento y elige un bucket de S3 llamado `read-only-bucket` para recibir los archivos de registro. A continuación, actualiza el registro de seguimiento para indicar que desea registrar los eventos de administración y los eventos de datos de Read (Lectura).
2. Usted crea un segundo registro de seguimiento y elige un bucket de S3 denominado `write-only-bucket` para recibir los archivos de registro. A continuación, actualiza el registro de seguimiento para indicar que desea registrar los eventos de administración y los eventos de datos de Write (Escritura).
3. En su cuenta se generan las operaciones de la API `DescribeInstances` y `TerminateInstances` de Amazon EC2.
4. La operación de API `DescribeInstances` es un evento de solo lectura y coincide con la configuración del primer registro de seguimiento. El registro de seguimiento registra y envía el evento al `read-only-bucket`.
5. La operación de API `TerminateInstances` es un evento de solo escritura y coincide con la configuración del segundo registro de seguimiento. El registro de seguimiento registra y envía el evento al `write-only-bucket`.

Registrar eventos de datos con AWS Command Line Interface

Puede configurar sus registros de seguimiento o los almacenes de datos de eventos para que registren los eventos de datos con la AWS CLI.

Temas

- Registrar eventos de datos para senderos con el AWS CLI
- Registrar los eventos de datos para los almacenes de datos de eventos con el AWS CLI

Registrar eventos de datos para senderos con el AWS CLI

Puede configurar sus registros de seguimiento para que registren los eventos de administración y los de datos con la AWS CLI. Para consultar si su registro de seguimiento está registrando los eventos de administración y de datos, ejecute el comando `get-event-selectors`.

Note

- Tenga en cuenta que, si su cuenta está registrando más de una copia de eventos de administración, generará cargos. Siempre hay un cargo por registrar eventos de datos. Para más información, consulte Precios de AWS CloudTrail.
- Puede utilizar selectores de eventos avanzados o selectores de eventos básicos, pero no ambos. Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes.
- Si su registro de seguimiento utiliza selectores de eventos básicos, solo puede registrar los siguientes tipos de recursos:
  - `AWS::DynamoDB::Table`
  - `AWS::Lambda::Function`
  - `AWS::S3::Object`

  Para registrar tipos de recursos adicionales, necesitará utilizar selectores de eventos avanzados. Para convertir un registro de seguimiento en selectores de eventos avanzados, ejecute el comando get-event-selectors para confirmar los selectores de eventos actuales y, a continuación, configure los selectores de eventos avanzados para que coincidan con la cobertura de los selectores de eventos anteriores. Luego, agregue selectores para cualquier tipo de recurso para el que desee registrar eventos de datos.
- Puede utilizar selectores de eventos avanzados para filtrar en función del valor de los campos `eventName`, `resources.ARN` y `readOnly`, así podrá registrar solo los eventos de datos que le interesen. Para obtener más información sobre la configuración de estos campos, consulte AdvancedFieldSelector.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

El comando devuelve la configuración predeterminada de un registro de seguimiento.

Temas

- Registrar eventos mediante selectores de eventos avanzados
- Registre todos los eventos de Amazon S3 de un bucket de Amazon S3 mediante selectores de eventos avanzados

- Registrar eventos de Amazon S3 en eventos de AWS Outposts mediante selectores de eventos avanzados
- Registrar eventos mediante selectores de eventos básicos

Registrar eventos mediante selectores de eventos avanzados

> **Note**
>
> Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes. Antes de configurar los selectores de eventos avanzados, ejecute el comando get-event-selectors para confirmar los selectores de eventos actuales y, a continuación, configure los selectores de eventos avanzados para que coincidan con la cobertura de los selectores de eventos anteriores. Luego, agregue selectores para cualquier evento de datos adicional que desee registrar.

En el siguiente ejemplo, se crean selectores de eventos avanzados personalizados para una ruta cuyo nombre *TrailName*incluye eventos de administración de lectura y escritura (omitiendo el `readOnly` selector) y eventos de `DeleteObject` datos para todas las combinaciones de bucket `PutObject` y prefijo de Amazon S3, excepto para un bucket con nombre `sample_bucket_name` y eventos de datos para una función denominada. AWS Lambda `MyLambdaFunction` Dado que se trata de selectores de eventos avanzados personalizados, cada conjunto de selectores tiene un nombre descriptivo. Tenga en cuenta que una barra diagonal final forma parte del valor de ARN para los buckets de S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
```

```
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

El ejemplo devuelve los selectores de eventos avanzados configurados para el registro de seguimiento.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
```

```
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Registre todos los eventos de Amazon S3 de un bucket de Amazon S3 mediante selectores de eventos avanzados

> **Note**
>
> Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes.

El ejemplo siguiente muestra cómo configurar su registro de seguimiento para que incluya eventos de datos para todos los objetos de Amazon S3 en un bucket de S3 específico. El valor de los eventos de S3 para el campo `resources.type` es `AWS::S3::Object`. Debido a que los valores de ARN

para los objetos de S3 y los buckets de S3 son ligeramente diferentes, debe agregar el operador `StartsWith` para `resources.ARN` a fin de capturar todos los eventos.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                }
```

```
            ]
        }
    ]
}
```

Registrar eventos de Amazon S3 en eventos de AWS Outposts mediante selectores de eventos avanzados

> **Note**
>
> Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes.

En el siguiente ejemplo se muestra cómo configurar su registro de seguimiento para que incluya todos los eventos de datos de todos los objetos de Amazon S3 on Outposts.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
```

```
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

Registrar eventos mediante selectores de eventos básicos

A continuación, se muestra un resultado de ejemplo del comando get-event-selectors que muestra los selectores de eventos básicos. De forma predeterminada, cuando crea una ruta con el AWS CLI, una ruta registra todos los eventos de administración. De forma predeterminada, los registros de seguimiento no registran eventos de datos.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

Para configurar el registro de seguimiento para que registre los eventos de administración y de datos, ejecute el comando `put-event-selectors`.

En el ejemplo siguiente, se muestra cómo utilizar selectores de eventos básicos a fin de configurar su registro de seguimiento de manera que incluya todos los eventos de administración y de datos para los objetos de S3 en dos prefijos de bucket de S3. Puede especificar entre 1 y 5 selectores de eventos en los registros de seguimiento. Puede especificar entre 1 y 250 recursos de datos en los registros de seguimiento.

> **Note**
>
> El número máximo de recursos de datos de S3 es 250, si elige limitar los eventos de datos mediante selectores de eventos básicos.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

El comando devuelve los selectores de eventos configurados para el registro de seguimiento.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

Registrar los eventos de datos para los almacenes de datos de eventos con el AWS CLI

Puede configurar sus almacenes de datos de eventos para que incluyan los eventos de datos con la AWS CLI. Utilice el comando `create-event-data-store` para crear un nuevo almacén de datos de eventos para registrar los eventos de datos. Utilice el comando `update-event-data-store` para actualizar los selectores de eventos avanzados de un almacén de datos de eventos existente.

Para ver si el almacén de datos de eventos incluye eventos de datos, ejecute el comando [get-event-data-store](#).

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

El comando devuelve la configuración del almacén de datos de eventos.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

Temas

- Incluir todos los eventos de Amazon S3 en un bucket

- Incluir Amazon S3 en los eventos de AWS Outposts

Incluir todos los eventos de Amazon S3 en un bucket

En el ejemplo siguiente, se muestra cómo crear un almacén de datos de eventos para que incluya todos los eventos de datos de todos los objetos de Amazon S3 en un bucket de S3 específico. El valor de los eventos de S3 para el campo `resources.type` es `AWS::S3::Object`. Debido a que los valores de ARN para los objetos de S3 y los buckets de S3 son ligeramente diferentes, debe agregar el operador `StartsWith` para `resources.ARN` a fin de capturar todos los eventos.

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
```

```
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

Incluir Amazon S3 en los eventos de AWS Outposts

En el ejemplo siguiente, se muestra cómo crear un almacén de datos de eventos que incluya todos los eventos de datos de todos los objetos de Amazon S3 en Outposts.

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```


Registrar eventos de datos para la conformidad con AWS Config

Si utiliza paquetes de AWS Config conformidad para ayudar a su empresa a cumplir con los estándares formalizados, como los exigidos por el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) o el Instituto Nacional de Estándares y Tecnología (NIST), los paquetes de conformidad para los marcos de cumplimiento generalmente requieren que registre los eventos de datos para los buckets de Amazon S3, como mínimo. Los paquetes de cumplimiento para los marcos de conformidad incluyen una regla administrada denominada `cloudtrail-s3-`

`dataevents-enabled` que comprueba el registro de eventos de datos de S3 en su cuenta. Varios paquetes de cumplimiento que no están asociados con marcos de conformidad también requieren el registro de eventos de datos de S3. A continuación, se muestran ejemplos de paquetes de cumplimiento que incluyen esta regla.

- Mejores prácticas operativas para el pilar de seguridad de AWS Well-Architected Framework
- Prácticas operativas recomendadas para la FDA Título 21 CFR Parte 11
- Prácticas operativas recomendadas para FFIEC
- Prácticas operativas recomendadas para FedRAMP (moderadas)
- Prácticas operativas recomendadas para la seguridad de HIPAA
- Prácticas operativas recomendadas para K-ISMS
- Prácticas operativas recomendadas para el registro

Para obtener una lista completa de los paquetes de conformidad de muestra disponibles en AWS Config, consulte las plantillas de ejemplo de paquetes de conformidad en la Guía para desarrolladores.AWS Config

Registrar eventos de datos con los SDK AWS

Ejecute la GetEventSelectorsoperación para comprobar si su ruta está registrando eventos de datos. Si ejecuta la PutEventSelectorsoperación, puede configurar sus senderos para que registren eventos de datos. Para obtener más información, consulte la Referencia de la API de AWS CloudTrail.

Ejecute la GetEventDataStoreoperación para comprobar si el almacén de datos de eventos está registrando eventos de datos. Puede configurar sus almacenes de datos de eventos para incluir eventos de datos ejecutando las UpdateEventDataStoreoperaciones CreateEventDataStoreo y especificando selectores de eventos avanzados. Para obtener más información, consulte Administrar CloudTrail Lake mediante la AWS CLI y la AWS CloudTrail API Reference.

Envío de eventos a Amazon CloudWatch Logs

CloudTrail admite el envío de eventos de datos a CloudWatch Logs. Cuando configuras tu ruta para enviar eventos a tu grupo de CloudWatch registros, CloudTrail envía solo los eventos que especifiques en tu ruta. Por ejemplo, si configuras tu ruta para registrar solo los eventos de datos, la ruta solo entrega los eventos de datos a tu grupo de CloudWatch registros. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Registro de eventos de Insights

AWS CloudTrail Insights ayuda a los usuarios de AWS a identificar y responder a la actividad inusual asociada a las llamadas a la API y las tasas de error de la API mediante el análisis continuo de los eventos de administración de CloudTrail. CloudTrail Insights analiza sus patrones normales de volumen de llamadas a la API y tasas de error de API, también conocido como valor de referencia, y genera eventos de Insights cuando el volumen se encuentra fuera de los patrones normales. Los eventos de Insights en el volumen de llamadas de API se generan para las API de administración de `write` y los eventos de Insights en la tasa de errores de API se generan tanto para las API de administración `read` como `write`.

> **Note**
>
> Para registrar los eventos de Insights sobre el volumen de llamadas a la API, el registro de seguimiento o almacén de datos de eventos debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el registro de seguimiento o el almacén de datos de eventos debe registrar los eventos de administración de `read` o `write`.

CloudTrail Insights analiza los eventos de administración que se producen en una sola región, no de forma global. Los eventos de CloudTrail Insights se generan en la misma región en la que se generan sus eventos de administración correspondientes.

Se aplican cargos adicionales por los eventos de Insights. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para más información, consulte Precios de AWS CloudTrail.

Contenido

- Descripción de la entrega de eventos de Insights
- Registro de eventos de Insights con la AWS Management Console
  - Habilitar los eventos de CloudTrail Insights en un registro de seguimiento existente
  - Habilitar eventos de CloudTrail Insights en un almacén de datos de eventos existente
- Registro de eventos de Insights con la AWS Command Line Interface
  - Registrar eventos de Insights para un registro de seguimiento mediante la AWS CLI
  - Registrar eventos de Insights para un almacén de datos de eventos mediante la AWS CLI

- Registro de eventos con los SDK de AWS
- Información adicional para registros de seguimiento
  - Ver eventos de Insights para registros de seguimiento en la consola
    - Columna de filtrado
    - Pestaña Insights graph (Gráfico de Insights)
    - Pestaña Atributions (Atribuciones)
      - Promedio de referencia y media de Insights
    - Pestaña CloudTrail events (Eventos de CloudTrail)
    - Pestaña Insights event record (Registro de eventos de Insights)
  - Enviar eventos de registro de seguimiento a Registros de Amazon CloudWatch

Descripción de la entrega de eventos de Insights

A diferencia de otros tipos de eventos que captura CloudTrail, los eventos de Insights solo se registran cuando CloudTrail detecta cambios en el uso de la API de su cuenta que difieren considerablemente de los patrones de uso típicos de la cuenta.

El lugar donde CloudTrail entrega los eventos y el tiempo que tarda en recibirlos de Insights difieren entre los registros de seguimiento y los almacenes de datos eventos.

Entrega de eventos de Insights para registros de seguimientos

Si ha habilitado eventos de Insights en un registro de seguimientos y CloudTrail detecta actividad inusual, CloudTrail envía los eventos de Insights a la carpeta `/CloudTrail-Insight` al bucket de S3 de destino para su registro de seguimiento. Después de que habilite la información de CloudTrail por primera vez en un registro de seguimiento, CloudTrail puede tardar hasta 36 horas en entregar el primer evento de Insights, si se detecta una actividad inusual.

Si deshabilita el registro de eventos de Insights en un registro de seguimiento y luego vuelve a habilitar los eventos de Insights o detiene y reinicia el registro de un registro en un registro de seguimiento, puede tardar hasta 36 horas para que CloudTrail reinicie la entrega de eventos de Insights, si se detecta una actividad inusual.

Entrega de eventos de Insights para los almacenes de datos de eventos

Si ha activado los eventos de Insights en un almacén de datos de eventos de origen, CloudTrail entrega los eventos de Insights al almacén de datos de eventos de destino. Después de que habilite

CloudTrail Insights por primera vez en el almacén de datos de eventos de origen, CloudTrail puede tardar hasta 7 días en entregar el primer evento de Insights al almacén de datos de eventos, si se detecta una actividad inusual.

Si desactiva el registro de eventos de Insights en un almacén de datos de eventos de origen y, a continuación, vuelve a habilitar los eventos de Insights, o detiene y reinicia la incorporación de eventos en un almacén de datos de eventos de origen, CloudTrail puede tardar hasta 7 días en reiniciar la entrega de eventos de Insights, si se detecta una actividad inusual. Se aplican cargos adicionales por incorporar eventos de Insights en CloudTrail Lake. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para obtener información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Registro de eventos de Insights con la AWS Management Console

Puede habilitar los eventos de Insights en un registro de seguimiento o almacén de datos de eventos mediante la consola.

Temas

- Habilitar los eventos de CloudTrail Insights en un registro de seguimiento existente
- Habilitar eventos de CloudTrail Insights en un almacén de datos de eventos existente

Habilitar los eventos de CloudTrail Insights en un registro de seguimiento existente

Utilice el siguiente procedimiento para habilitar los eventos de CloudTrail Insights en un registro de seguimiento existente. De forma predeterminada, los eventos de Insights no se encuentran habilitados.

1. En el panel de navegación izquierdo de la consola de CloudTrail, abra la página Trails (Registros de seguimiento) y elija el nombre del registro de seguimiento.
2. En Insights events (Eventos de Insights) elija Edit (Editar).

   > **Note**
   >
   > Se aplican cargos adicionales por registrar eventos de Insights. Para conocer los precios de CloudTrail, consulte Precios de AWS CloudTrail.

3. En Event type (Tipo de evento), seleccione Insights events (Eventos de Insights).

4. En Inshgts events (Eventos de Insights), en Choose Insights types (Elija tipos de Insights), elija API call rate (Tasa de llamada a la API), API error rate (Tasa de errores de API), o ambos. El registro de seguimiento debe registrar los eventos de administración de escritura para registrar los eventos de Insights para calcular la tasa de llamadas a la API. El registro de seguimiento debe registrar los eventos de administración de lectura o escritura para registrar los eventos de Insights para la tasa de errores de la API.
5. Elija Guardar cambios para guardar los cambios.

CloudTrail puede tardar hasta 36 horas en enviar los primeros eventos de Insights, si se detecta actividad inusual.

Habilitar eventos de CloudTrail Insights en un almacén de datos de eventos existente

Utilice el siguiente procedimiento para habilitar los eventos de CloudTrail Insights en un almacén de datos de eventos existente. De forma predeterminada, los eventos de Insights no se encuentran habilitados.

Se aplican cargos adicionales por incorporar eventos de Insights en CloudTrail Lake. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para obtener información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

> **Note**
>
> Solo puede habilitar los eventos de datos de CloudTrail Insights en los almacenes de datos de eventos que contengan eventos de administración de CloudTrail. No puede habilitar los eventos de CloudTrail Insights en otros tipos de almacenes de datos de eventos.

1. En el panel de navegación izquierdo de la consola de CloudTrail y, en Lake, elija Almacenes de datos de eventos.
2. Elija el nombre del almacén de datos de eventos.
3. En Eventos de administración, elija Editar.
4. Seleccione Habilitar Insights.
5. Elija el almacén de datos de eventos de destino en el que CloudTrail entregará los eventos de Insights. El almacén de datos de eventos de destino recopilará los eventos de Insights en función de la actividad de los eventos de administración en este almacén de datos de eventos. Para obtener información acerca de cómo crear un almacén de datos de eventos de destino,

consulte Cómo crear un almacén de datos de eventos de destino que registre los eventos de Insights.

6. En Elegir tipos de Insights, elija Tasa de llamadas a la API, Tasa de errores de la API, o ambos. Su almacén de datos de eventos debe registrar eventos de administración de Escritura para registrar los eventos de Insights para la tasa de llamadas a la API. Su almacén de datos de eventos debe registrar eventos de administración de Lectura o Escritura para registrar los eventos de Insights para la tasa de errores de la API.
7. Elija Guardar cambios para guardar los cambios.

CloudTrail puede tardar hasta 7 días en enviar los primeros eventos de Insights, si se detecta actividad inusual.

Registro de eventos de Insights con la AWS Command Line Interface

Puede configurar sus registros de seguimiento y los almacenes de datos de eventos para que registren los eventos de Insights con la AWS CLI.

> **Note**
>
> Para registrar los eventos de Insights sobre el volumen de llamadas a la API, el registro de seguimiento o almacén de datos de eventos debe registrar los eventos de administración de `write`. Para registrar los eventos de Insights sobre la tasa de errores de la API, el registro de seguimiento o el almacén de datos de eventos debe registrar los eventos de administración de `read` o `write`.

Temas

- Registrar eventos de Insights para un registro de seguimiento mediante la AWS CLI
- Registrar eventos de Insights para un almacén de datos de eventos mediante la AWS CLI

Registrar eventos de Insights para un registro de seguimiento mediante la AWS CLI

Para conocer si su registro de seguimiento está registrando los eventos de Insights, ejecute el comando `get-insight-selectors`.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

El siguiente resultado muestra la configuración predeterminada de un registro de seguimiento. De forma predeterminada, los registros de seguimiento no registran eventos de Insights. El valor del atributo `InsightType` está vacío y no se especifican selectores de eventos de Insight, porque la recopilación de eventos de Insights no está habilitada.

Si no agrega selectores de Insights, el ocmando get-insight-selectors devuelve el siguiente mensaje de error: “Se ha producido un error (InsightNotEnabledException) al llamar a la operación GetInsightSelectors: el *nombre* de la traza no tiene Insights habilitado. Edite la configuración de la traza para habilitar Insights y, a continuación, vuelva a intentar la operación”.

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Para configurar el registro de seguimiento a fin de que registre los eventos de Insights, ejecute el comando `put-insight-selectors`. En el siguiente ejemplo se muestra cómo configurar el registro de seguimiento para incluir eventos de Insights. Los valores del selector de insights pueden ser `ApiCallRateInsight`, `ApiErrorRateInsight` o ambos.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

El siguiente resultado muestra el selector de eventos de Insights configurado para el registro de seguimiento.

```
{
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Registrar eventos de Insights para un almacén de datos de eventos mediante la AWS CLI

Para habilitar Insights en un almacén de datos de eventos, debe tener un almacén de datos de eventos de origen que registre los eventos de administración y un almacén de datos de eventos de destino que registre los eventos de Insights.

Para ver si los eventos de Insights están habilitados en un almacén de datos de eventos, ejecute el comando get-insight-selectors.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Para ver si un almacén de datos de eventos está configurado para recibir eventos de Insights o eventos de administración, ejecute el comando get-event-data-store.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

En el siguiente procedimiento, se muestra cómo crear los almacenes de datos de eventos de origen y destino y, a continuación, habilitar los eventos de Insights.

1. Ejecute el comando aws cloudtrail create-event-data-store para crear un almacén de datos de eventos de destino que recopile los eventos de Insights. El valor para `eventCategory` debe ser `Insight`. Sustituya los *`retention-period-days`* con la cantidad de días que desea retener los eventos en su almacén de datos de eventos.

   Si ha iniciado sesión con la cuenta de administración de una organización de AWS Organizations, incluya el parámetro `--organization-enabled` si desea dar acceso al administrador delegado al almacén de datos de eventos.

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   --advanced-event-selectors '[
       {
         "Name": "Select Insights events",
         "FieldSelectors": [
   ```

```
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

Utilizará el ARN (o el sufijo ID del ARN) de la respuesta como valor del parámetro `--insights-destination` en el paso 3.

2. Ejecute el comando aws cloudtrail create-event-data-store para crear un almacén de datos de eventos de origen que registre los eventos de administración. De forma predeterminada, los almacenes de datos de eventos registran eventos de administración. No es necesario que especifique ningún selector de eventos avanzado si desea registrar todos los eventos de administración. Sustituya los *`retention-period-days`* con la cantidad de días que desea

retener los eventos en su almacén de datos de eventos. Si va a crear un almacén de datos de eventos de la organización, incluya el parámetro `--organization-enabled`.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

A continuación, se muestra un ejemplo de respuesta.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Utilizará el ARN (o el sufijo ID del ARN) de la respuesta como valor del parámetro `--event-data-store` en el paso 3.

3. Ejecute el comando put-insight-selectors para habilitar los eventos de Insights. Los valores del selector de insights pueden ser `ApiCallRateInsight`, `ApiErrorRateInsight` o ambos. Para el parámetro `--event-data-store`, especifique el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos de origen que registra los eventos de administración y habilitará

Insights. Para el parámetro `--insights-destination`, especifique el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos de destino que registrará los eventos de Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

En el siguiente resultado, se muestra el selector de eventos de Insights configurado para el almacén de datos de eventos.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Después de que habilite CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en entregar el primer evento de Insights, si se detecta una actividad inusual.

CloudTrail Insights analiza los eventos de administración que se producen en una sola región, no de forma global. Los eventos de CloudTrail Insights se generan en la misma región en la que se generan sus eventos de administración correspondientes.

En el caso de un almacén de datos de eventos de una organización, CloudTrail analiza los eventos de administración de la cuenta de cada miembro en lugar de analizar la agregación de todos los eventos de administración de la organización.

Se aplican cargos adicionales por incorporar eventos de Insights en CloudTrail Lake. Se le cobrará por separado si habilita Insights para los registros de seguimiento y almacenes de datos de eventos. Para obtener información sobre los precios de CloudTrail, consulte Precios de AWS CloudTrail.

Registro de eventos con los SDK de AWS

Ejecute la operación GetInsightSelectors para saber si su registro de seguimiento o el almacén de datos de eventos habilita los eventos de Insights. Puede configurar los registros de seguimiento o almacenes de datos de eventos para habilitar eventos de Insights con la operación PutInsightSelectors. Para obtener más información, consulte la Referencia de la API de AWS CloudTrail.

Información adicional para registros de seguimiento

En esta sección, se proporciona información adicional específica de los registros de seguimiento. En esta sección, se describe cómo puede ver los eventos de sus registros de seguimiento suscritos desde la página Insights de la consola de CloudTrail y cómo puede enviar estos eventos de forma opcional a CloudWatch Logs para su supervisión.

Temas

- Ver eventos de Insights para registros de seguimiento en la consola
- Enviar eventos de registro de seguimiento a Registros de Amazon CloudWatch

Ver eventos de Insights para registros de seguimiento en la consola

Para los registros de seguimiento, también puede obtener acceso y ver los eventos Insights en la página de Insights de la consola de CloudTrail. Para obtener más información sobre cómo obtener acceso a los eventos de Insights y consultarlos en la consola y mediante la AWS CLI, consulte Visualizar eventos de CloudTrail Insights para registros de seguimiento en esta guía.

En la siguiente imagen, se muestra un ejemplo de eventos de Insights para un registro de seguimiento. Para abrir las páginas de detalles de un evento de Insights, elija un nombre de evento de Insights en las páginas Dashboard (Panel) o Insights.

Si deshabilita CloudTrail Insights en un registro de seguimiento o detiene el proceso de registro en este (lo que deshabilita CloudTrail Insights), es posible que tenga eventos de Insights almacenados en su bucket de S3 de destino, o que estos se muestren en la página Insights de la consola, desde el momento en que tenía habilitado Insights.

Columna de filtrado

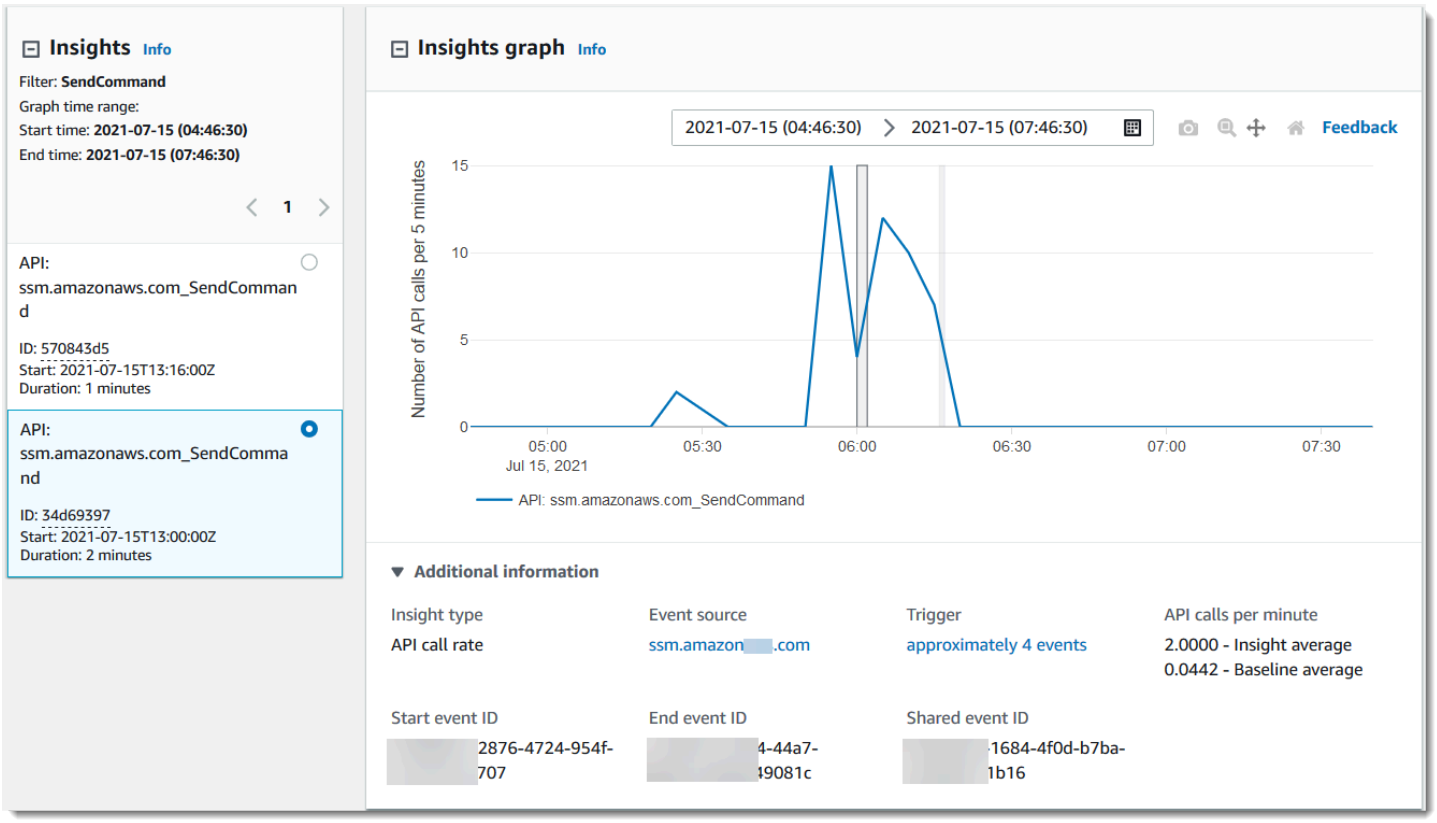
La columna de la izquierda muestra los eventos de Insights relacionados con la API en cuestión que tienen el mismo tipo de evento de Insights. La columna permite elegir el evento de Insights sobre el que desea obtener más información. Cuando elige un evento en esta columna, el evento se resalta en el gráfico de la pestaña Insights graph (Gráfico de Insights). De forma predeterminada, CloudTrail aplica un filtro que limita los eventos que se muestran en la pestaña CloudTrail events (Eventos de CloudTrail) a aquellos a los que la API específica que se llamó durante el periodo de actividad inusual que desencadenó el evento Insights. Para mostrar todos los eventos de CloudTrail que se llamaron durante el periodo de actividad inusual, incluidos los eventos no relacionados con el evento de Insights, desactive el filtro.

Pestaña Insights graph (Gráfico de Insights)

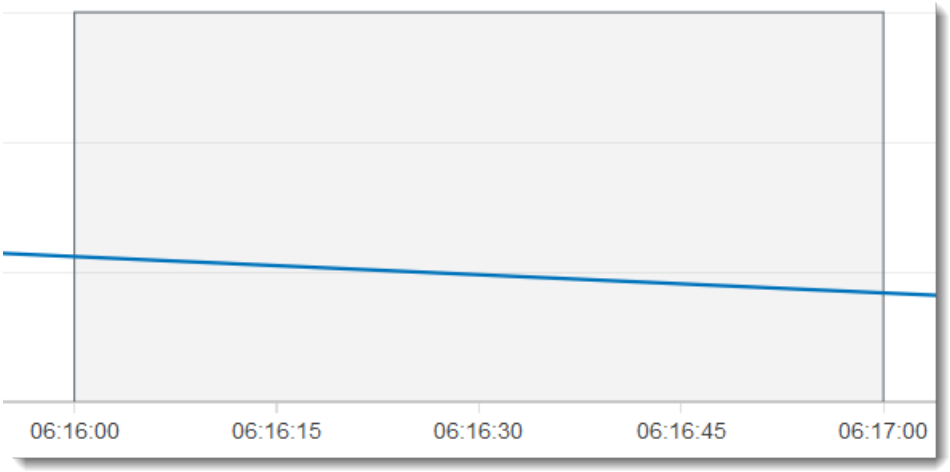
En la pestaña Insights graph (Gráfico de Insights), la página de detalles de un evento de Insights muestra un gráfico del volumen de llamadas a una API o tasa de error realizadas durante un periodo de tiempo previo y posterior al registro de uno o varios eventos de Insights. En el gráfico, los eventos de Insights se resaltan con barras verticales y el ancho de la barra muestra la hora de inicio y finalización del evento de Insights.

En este ejemplo, una banda de resaltado vertical muestra números inusuales de llamadas a la API AWS Systems Manager `SendCommand` en una cuenta. En el área resaltada, como el número de llamadas `SendCommand` superó el promedio del valor de referencia de 0,0442 llamadas por minuto de la cuenta, CloudTrail registró un evento de Insights cuando detectó la actividad inusual. El evento de Insights registró que hasta 15 llamadas de `SendCommand` se realizaron en un periodo de cinco minutos entre las 5:50 y las 5:55 a.m. Estas son aproximadamente dos llamadas más a la API por minuto que se preve para la cuenta. En este ejemplo, el intervalo de tiempo del gráfico es de tres horas: 4:30 a. m. PDT del 15 de julio de 2021 a las 7:30 a. m. PDT con fecha del 15 de julio de 2021. La hora de inicio de este evento es a las 6:00 a. m. PDT con fecha del 15 de julio de 2021 y dos minutos después de finalización. Un evento final de Insights, no destacado, muestra que la actividad inusual terminó alrededor de las 6:16 a. m.

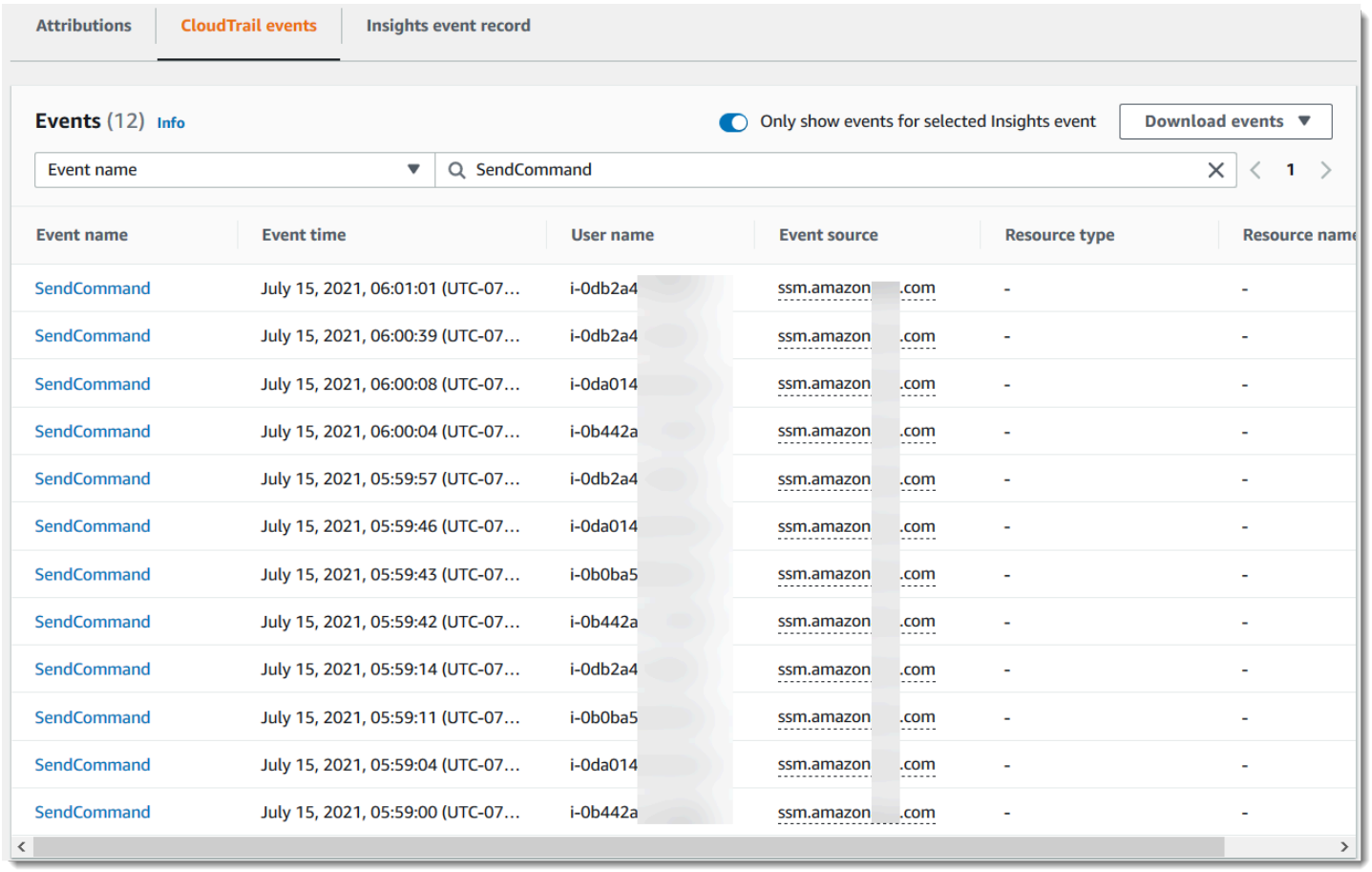
El valor de referencia se calcula a lo largo de los siete días anteriores al inicio de un evento de Insights. Aunque el valor de referencia de la duración (el periodo que analiza CloudTrail para la actividad normal en las API) es de aproximadamente siete días, CloudTrail redondea la duración de referencia a un día entero, por lo que la duración de referencia exacta puede variar.



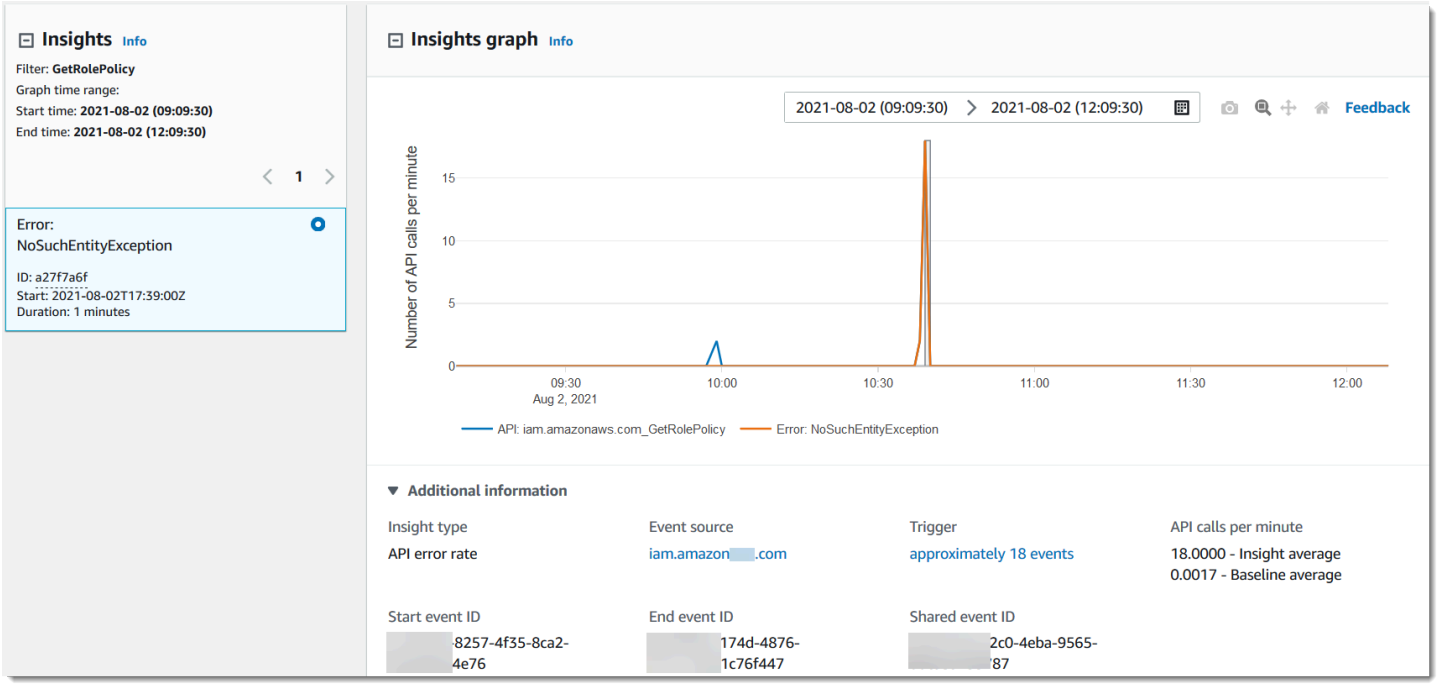
Puede utilizar el comando Zoom de la barra de herramientas para ampliar el evento Insights final, mostrando las horas de inicio y finalización. En este ejemplo, seleccione Zoom, luego arrastrando el cursor Zoom a una distancia muy corta sobre un borde del evento Insights resaltado amplía el evento Insights y muestra más detalles de la línea de tiempo.



Abra la pestaña CloudTrail events (Eventos de CloudTrail), vea los eventos de CloudTrail que se analizaron para determinar que se produjo una actividad inusual. En este ejemplo, CloudTrail analizó 12 eventos, cuatro de los cuales desencadenaron el evento Insights.

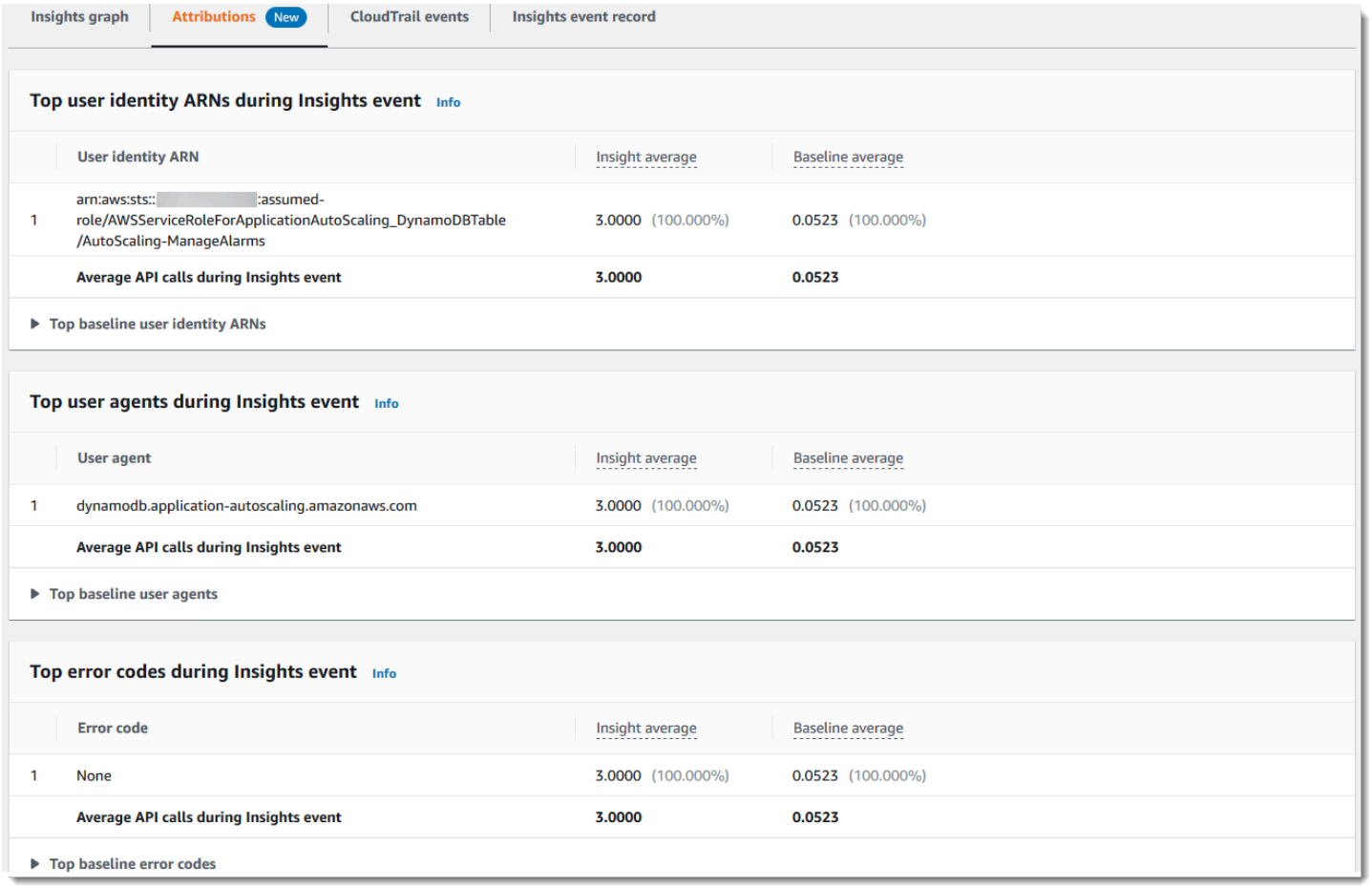


En la siguiente captura de pantalla, se muestra una pestaña gráfica de Insights para un evento de Insights de la tasa de errores de la API. El área resaltada muestra que se registró un evento de Insights debido a que aumentaron las ocurrencias del error `NoSuchEntityException` en la llamada a la API de IAM `GetRolePolicy` por encima del promedio de referencia de 0,0017 errores `NoSuchEntityException` por minuto en esta llamada a la API, con un promedio de 18 errores por minuto durante el periodo de información. El número de eventos de CloudTrail que desencadenaron el evento Insights coincide con el promedio de Insights de 18 errores `NoSuchEntityException` en un minuto, en este ejemplo. A diferencia de un gráfico de tasa de llamadas de API, la tasa de errores de la API muestra dos líneas, en colores contrastantes: una línea que mide llamadas a la API de IAM, `GetRolePolicy`, que dio lugar a un número inusual de errores y una línea que mide el error en el que se registró una actividad inusual, `NoSuchEntityException`.

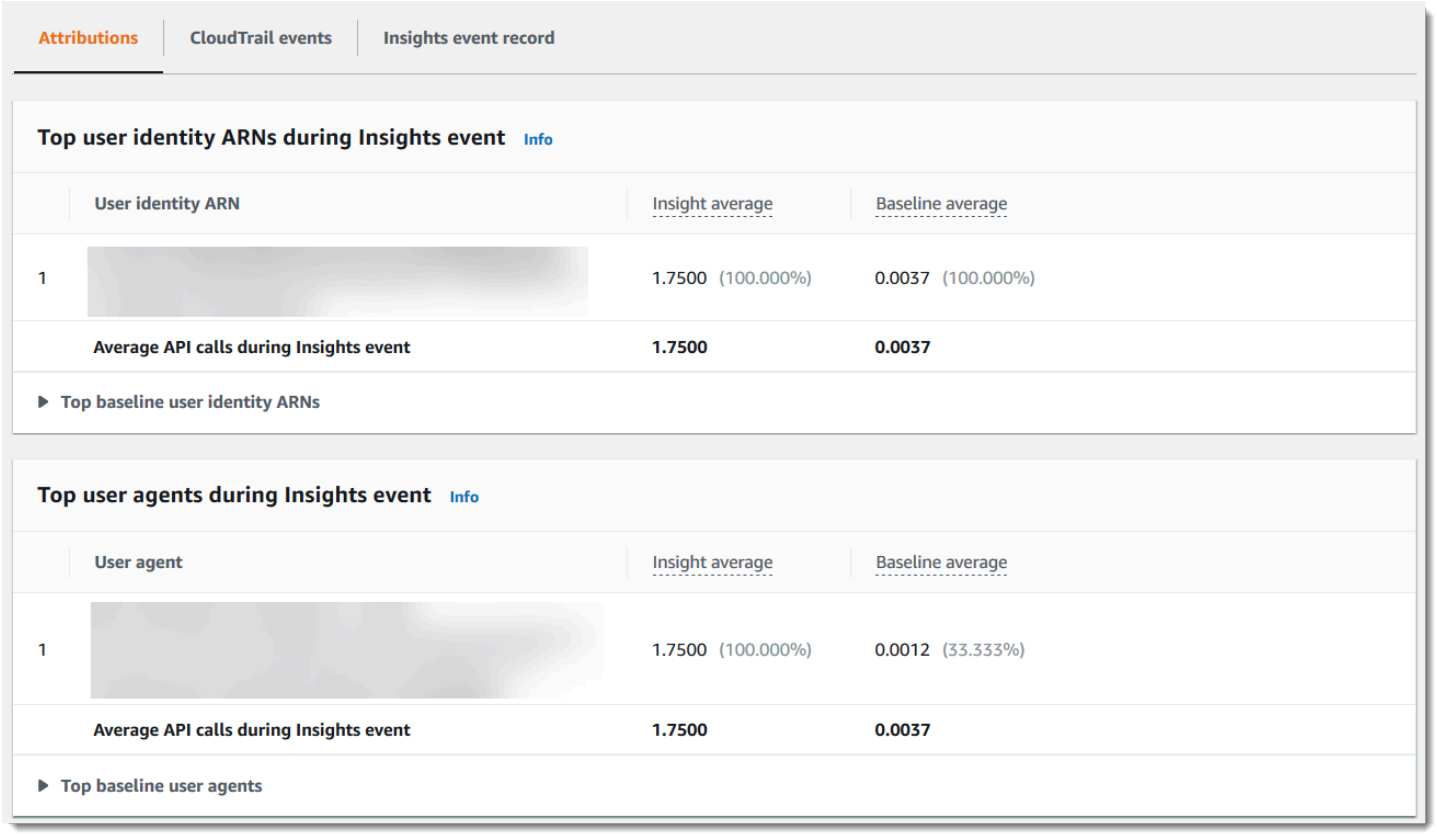


Pestaña Atributions (Atribuciones)

La pestaña Attributions (Atribuciones) muestra la siguiente información sobre un evento de Insights. Información sobre la pestaña Attributions (Atribuciones) puede ayudarle a identificar las causas y los orígenes de la actividad de Insights. Expanda las áreas de referencia principales para comparar la identidad del usuario, el agente de usuario y la actividad del código de error durante los periodos normales con las atribuidas durante la actividad de Insights. En Top baseline user identity ARNs (Principales ARN de identidad de usuario de línea de referencia), Top baseline user agents (Principales agentes de usuario de referencia) y Top baseline error codes (Principales códigos de error de referencia), solo se muestra el promedio de referencia; el promedio histórico de eventos de la API que registra la identidad del usuario, el agente de usuario o que dan lugar al código de error, aproximadamente los siete días anteriores a la hora de inicio del evento Insights.



La pestaña Atributions (Atribuciones) muestra solo los principales ARN de identidad de usuario y los principales agentes de usuario para un evento Insights de tasa de errores, como se muestra en la siguiente imagen. Los códigos de error principales no son necesarios para los eventos de Insights de la tasa de errores.



- Top user identity ARNs (ARN de identidad de usuarios principales): en esta tabla se muestran los cinco usuarios de AWS o roles de IAM (identidades de usuario) principales que contribuyeron a las llamadas a la API durante la actividad inusual y los periodos de referencia, en orden descendente según el promedio de llamadas a la API aportadas. Entre paréntesis se muestra el porcentaje de los valores promedio como un total de la actividad que contribuyó a la actividad inusual. Si más de cinco ARN de identidad de usuario contribuyeron a la actividad inusual, la actividad se resume en la fila Other (Otros).
- Top user agents (Agentes de usuarios principales): en esta tabla se muestran las cinco herramientas de AWS principales mediante las cuales la identidad del usuario contribuyó a las llamadas a la API durante la actividad inusual y los periodos de referencia, en orden descendente según el promedio de llamadas a la API aportadas. Estas herramientas incluyen la AWS Management Console, la AWS CLI o los SDK de AWS. Por ejemplo, un agente de usuario denominado `ec2.amazonaws.com` indica que la consola de Amazon EC2 se encontraba entre las herramientas utilizadas para llamar a la API. Entre paréntesis se muestra el porcentaje de los valores promedio como un total de la actividad que contribuyó a la actividad inusual. Si más de cinco agentes de usuario contribuyeron a la actividad inusual, la actividad se resume en la fila Other (Otros).

- Códigos de error principales: solo se muestra para los eventos de Insights de tasa de llamadas a API. En esta tabla se muestran los cinco códigos de error principales que se produjeron en las llamadas a la API durante la actividad inusual y los periodos de referencia, en orden descendente desde el mayor número de llamadas a la API hasta el menor. Entre paréntesis se muestra el porcentaje de los valores promedio como un total de la actividad que contribuyó a la actividad inusual. Si se produjeron más de cinco códigos de error durante la actividad inusual o de referencia, la actividad se resume en la fila Other (Otros).

  Un valor de `None` como uno de los cinco valores de código de error principales significa que un porcentaje significativo de las llamadas que contribuyeron al evento de Insights no produjo errores. Si el valor del código de error es `None` y no hay otros códigos de error en la tabla, los valores en las columnas Insight average (Promedio de Insights) y Baseline average (Promedio de referencia) son los mismos que aquellos en el evento de Insights en general. También puede ver los valores que se muestran en la leyenda Insight average (Promedio de Insights) y Baseline average (Promedio de referencia) en la pestaña Insights graph (Gráfico de Insights), en API calls per minute (Llamadas a la API por minuto).

Promedio de referencia y media de Insights

El promedio de referencia y el promedio de Insights se muestran para las principales identidades de usuario, los principales agentes de usuario y los principales códigos de error.

- Baseline average (Promedio de referencia): la tasa típica de ocurrencias por minuto a esta API en la que se registró el evento Insights, medido en aproximadamente los siete días anteriores, en una región específica de su cuenta.
- Insights average (Promedio de Insights): la tasa de llamadas o de errores por minuto a esta API que desencadenaron el evento de Insights. El promedio de CloudTrail Insights del evento de inicio es el número de llamadas o errores por minuto a la API que desencadenó el evento de Insights. Por lo general, este es el primer minuto de actividad inusual. El promedio de Insights del evento final es el porcentaje de llamadas o errores por minuto a la API durante la actividad inusual, entre el evento de Insights inicial y el evento de Insights final.

Pestaña CloudTrail events (Eventos de CloudTrail)

En la pestaña CloudTrail events (Eventos de CloudTrail), vea los eventos relacionados que CloudTrail analizó para determinar que se produjo una actividad inusual. De forma predeterminada, ya se aplica un filtro para el nombre del evento de Insights, que también es el nombre de la API

relacionada. A fin de mostrar todos los eventos de CloudTrail registrados durante el periodo de actividad inusual, desactive la opción Only show events for selected Insights event (Solo mostrar eventos para el evento de Insights seleccionado). La pestaña CloudTrail events (Eventos de CloudTrail) muestra los eventos de administración de CloudTrail relacionados con la API en cuestión que se produjeron entre la hora de inicio y finalización del evento de Insights. Estos eventos le ayudan a realizar un análisis más detallado para determinar la causa probable de un evento de Insights y las razones de la actividad de tasa de error y a la API inusual.

Pestaña Insights event record (Registro de eventos de Insights)

Al igual que cualquier evento de CloudTrail, un evento de CloudTrail Insights es un registro en formato JSON. La pestaña Insights event record (Registro de eventos de Insights) muestra la estructura JSON y el contenido de los eventos de inicio y finalización de Insights, a veces denominados eventos de carga. Para obtener más información sobre los campos y el contenido del registro de eventos de Insights, consulte Campos de registro de eventos de Insights y Elemento `insightDetails` CloudTrail Insights en esta guía.

Enviar eventos de registro de seguimiento a Registros de Amazon CloudWatch

CloudTrail admite el envío de eventos de Insights para registros de seguimiento a CloudWatch Logs. Cuando configure su registro de seguimiento para enviar eventos de Insights a su grupo de registros de CloudWatch Logs, CloudTrail Insights envía únicamente los eventos que indique en el registro de seguimiento. Por ejemplo, si configura el registro de seguimiento para que registre eventos de administración e Insights, el registro de seguimiento envía los eventos de administración e Insights a su grupo de registros de CloudWatch Logs. Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Recepción de archivos de registro de CloudTrail de varias regiones

Puede configurar CloudTrail para que envíe los archivos de registro desde varias regiones a un único bucket de S3 de una sola cuenta. Suponga, por ejemplo, que tiene un registro de seguimiento en la región EE. UU. Oeste (Oregón) que está configurado para enviar archivos de registros a un bucket de S3 y un grupo de registros de CloudWatch Logs. Cuando cambia un registro de seguimiento existente de una sola región para registrar todas las regiones, CloudTrail registra los eventos de todas las regiones que están en una única partición de AWS de su cuenta. CloudTrail envía los archivos de registros al mismo bucket de S3 y grupo de registros de CloudWatch Logs. Siempre que CloudTrail tenga permisos para escribir en un bucket de S3, el bucket para un registro de seguimiento de varias regiones no tiene que estar en la región de inicio del registro de seguimiento.

Para registrar eventos en todas las regiones de todas las particiones de AWS de su cuenta, cree un registro de seguimiento de varias regiones en cada partición.

En la consola, de forma predeterminada, cuando crea un registro de seguimiento que registra eventos en todas las Regiones de AWS de la partición de AWS en la que trabaja. Esta es una práctica recomendada. Para registrar eventos en una sola región (no recomendado), utilice la AWS CLI. Para configurar un registro de seguimiento de una sola región existente para que cree registros en todas las regiones, debe utilizar la AWS CLI.

Para cambiar un registro de seguimiento existente de forma que se aplique a todas las regiones, agregue la opción `--is-multi-region-trail` al comando update-trail.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Para confirmar que el registro de seguimiento se aplica ahora a todas las regiones, el elemento `IsMultiRegionTrail` del resultado muestra `true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> Cuando se lanza una nueva región en la partición de `aws`, CloudTrail crea automáticamente un registro de seguimiento en la nueva región con la misma configuración que el registro de seguimiento original.

Para obtener más información, consulte los siguientes recursos:

- ¿Cómo se CloudTrail comporta a nivel regional y global?
- Preguntas frecuentes sobre CloudTrail

Administración de la consistencia de los datos en CloudTrail

CloudTrail utiliza un modelo de computación distribuida denominado coherencia final. Cualquier cambio que realice en su configuración de CloudTrail (o en otros servicios de AWS), incluidas las etiquetas utilizadas en el control de acceso basado en atributos (ABAC), tardará en aparecer en todos los puntos de conexión posibles. Este retraso se debe en parte al tiempo que se tarda en enviar los datos de un servidor a otro, de una zona de replicación a otra y entre regiones de todo el mundo. CloudTrail también utiliza caché para mejorar el rendimiento, pero en algunos casos esto puede añadir tiempo. Es posible que el cambio no sea visible hasta que se agoten los datos previamente almacenados.

Debe diseñar sus aplicaciones teniendo en cuenta estos posibles retrasos. Asegúrese de que funcionan según lo previsto, incluso cuando un cambio realizado en una ubicación no sea visible inmediatamente en otra. Estos cambios incluyen crear o actualizar registros de seguimiento o almacenes de datos de eventos, actualizar los selectores de eventos e iniciar o detener el registro. Al crear o actualizar un registro de seguimiento o un almacén de datos de eventos, CloudTrail envía registros al almacén de datos de eventos o bucket de S3 en función de la última configuración conocida hasta que los cambios se propaguen a todas las ubicaciones.

Para obtener más información acerca del modo en que esto afecta a otros Servicios de AWS, consulte los siguientes recursos:

- Amazon DynamoDB: ¿Cuál es el modelo de coherencia de Amazon DynamoDB? en Preguntas frecuentes sobre DynamoDB, y Coherencia de lectura en la Guía para desarrolladores de Amazon DynamoDB.
- Amazon EC2: coherencia final en la Referencia de la API de Amazon Elastic Compute Cloud.
- Amazon EMR: cómo asegurar la coherencia al utilizar Amazon S3 y Amazon Elastic MapReduce para flujos de trabajo ETL en el blog de Macrodatos de AWS.
- AWS Identity and Access Management (IAM): los cambios que hizo no están siempre visibles inmediatamente en la Guía del usuario de IAM.
- Amazon Redshift: administración de la coherencia de los datos en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Amazon S3: modelo de coherencia de datos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs

Puede configurar CloudTrail con CloudWatch Logs para monitorear los registros de seguimiento y recibir notificaciones cuando se produzca una actividad específica.

1. Configure su registro de seguimiento para enviar eventos de registro a CloudWatch Logs.
2. Defina filtros de métricas de CloudWatch Logs para evaluar los eventos de registro con el fin de encontrar términos, frases o valores coincidentes. Por ejemplo, puede monitorizar eventos `ConsoleLogin`.
3. Asigne métricas de CloudWatch a filtros de métricas.
4. Cree alarmas de CloudWatch que se desencadenen en función de los umbrales y los periodos de tiempo especificados. Puede configurar alarmas para enviar notificaciones cuando se activen las alarmas para que pueda emprender acciones.
5. También puede configurar CloudWatch para que realice de forma automática una acción en respuesta a una alarma.

Se aplican los precios estándar de Amazon CloudWatch y Amazon CloudWatch Logs. Para obtener más información, consulte Precios de Amazon CloudWatch.

Para obtener más información sobre las regiones en las que pueden configurar registros de seguimiento para enviar registros a Registros de CloudWatch, consulte Regiones y cuotas de Registros de Amazon CloudWatch en la Referencia general de AWS.

Temas

- Envío de eventos a Amazon CloudWatch Logs
- Creación de alarmas de CloudWatch para eventos de CloudTrail: ejemplos
- Impedir que CloudTrail envíe eventos a CloudWatch Logs
- Grupo de registros de CloudWatch y nomenclatura de secuencias de registros para CloudTrail
- Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear

Envío de eventos a Amazon CloudWatch Logs

Si configura el registro de seguimiento para enviar eventos a CloudWatch Logs, CloudTrail solo envía los eventos que coinciden con la configuración de este registro. Por ejemplo, si configura el

registro de seguimiento para registrar solo eventos de datos, dicho registro de seguimiento envía los eventos de datos solo al grupo de registros de CloudWatch Logs. CloudTrail admite el envío de datos, información y eventos de administración a CloudWatch Logs. Para obtener más información, consulte Trabajar con archivos de registros de CloudTrail.

> **Note**
>
> Solo la cuenta de administración puede configurar un grupo de registro de CloudWatch Logs para un registro de seguimiento de la organización mediante la consola. El administrador delegado puede configurar un grupo de registro de CloudWatch Logs con la AWS CLI o operaciones `CreateTrail` o `UpdateTrail` de la API de CloudTrail.

Para enviar eventos a un grupo de registros de CloudWatch Logs:

- Asegúrese de tener permisos suficientes para crear o especificar un rol de IAM. Para obtener más información, consulte Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola.
- Si configura el grupo de registro de CloudWatch Logs con la AWS CLI, asegúrese de que posee permisos suficientes para crear un flujo de registro de CloudWatch Logs en el grupo de registro que especifique y enviar eventos de CloudTrail a dicho flujo de registro. Para obtener más información, consulte Creación de un documento de políticas.
- Cree un nuevo registro de seguimiento o especifique uno existente. Para obtener más información, consulte Creación y actualización de un registro de seguimiento con la consola.
- Cree un grupo de registros o especifique uno existente.
- Especifique un rol de IAM. Si modifica un rol de IAM existente para un registro de seguimiento de organización, debe actualizar manualmente la política para permitir el registro del registro de seguimiento de organización. Para obtener más información, consulte este ejemplo de política y Creación de un registro de seguimiento para una organización.
- Asocie una política de rol o utilice la opción predeterminada.

Contenido

- Configuración del monitoreo de CloudWatch Logs con la consola
  - Creación de un grupo de registros o especificación de un grupo de registros existente
  - Especificación de un rol de IAM

- Visualizar eventos en la consola de CloudWatch
- Configuración del monitoreo de CloudWatch Logs con la AWS CLI
  - Creación de un grupo de registros
  - Creación de un rol
  - Creación de un documento de políticas
  - Actualización del registro de seguimiento
- Limitación

Configuración del monitoreo de CloudWatch Logs con la consola

Puede utilizar la AWS Management Console para configurar su registro de seguimiento y enviar eventos a CloudWatch Logs con fines de monitoreo.

Creación de un grupo de registros o especificación de un grupo de registros existente

CloudTrail utiliza un grupo de registros de CloudWatch Logs como punto de enlace para el envío de eventos de registro. Puede crear un grupo de registros o especificar uno existente.

Para crear o especificar un grupo de registro para un registro de seguimiento existente

1. Asegúrese de registrarse con un usuario o un rol administrativo que tenga permisos suficientes para configurar la integración con Registros de CloudWatch. Para obtener más información, consulte Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola.

   > **Note**
   >
   > Solo la cuenta de administración puede configurar un grupo de registro de CloudWatch Logs para un registro de seguimiento de la organización mediante la consola. El administrador delegado puede configurar un grupo de registro de CloudWatch Logs con la AWS CLI o operaciones `CreateTrail` o `UpdateTrail` de la API de CloudTrail.

2. Abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
3. Elija el nombre del registro de seguimiento. Si selecciona un registro de seguimiento aplicable a todas las regiones, se le redirigirá a la región en la que se creó. Puede crear un grupo de registro o elegir un grupo de registro existente en la misma región que el registro de seguimiento.

> **Note**
>
> Un registro de seguimiento que se aplica a todas las regiones envía archivos de registro desde todas las regiones al grupo de registro de Registros de CloudWatch que especifique.

4. En CloudWatch Logs, elija Edit (Editar).
5. En Registros de CloudWatch, seleccione Activado.
6. En Nombre del grupo de registro, seleccione Nuevo para crear un nuevo grupo de registro o Existente para usar uno existente. Si elige New (Nuevo), CloudTrail especifica un nombre para el grupo de registros nuevo o puede escribir un nombre. Para obtener más información sobre la nomenclatura, consulte Grupo de registros de CloudWatch y nomenclatura de secuencias de registros para CloudTrail.
7. Si elige Existing (Existente), elija un grupo de registros en la lista desplegable.
8. En Nombre del rol, seleccione Nuevo para crear un rol de IAM nuevo con permisos para enviar registros a Registros de CloudWatch. Elija Existing (Existente) para elegir un rol de IAM en la lista desplegable. La instrucción de la política para el rol nuevo o existente se muestra al expandir Policy document (Documento de política). Para obtener más información acerca de este rol, consulte Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear.

   > **Note**
   >
   > Cuando configura un registro de seguimiento, puede elegir un bucket de S3 y un tema de SNS que pertenezcan a otra cuenta. Sin embargo, si desea que CloudTrail envíe los eventos a un grupo de archivos de registro de CloudWatch Logs, debe elegir un grupo de archivos de registro que exista en la cuenta actual.

9. Elija Guardar cambios.

Especificación de un rol de IAM

Puede especificar el rol que debe adoptar CloudTrail para enviar eventos a la secuencia de registros.

Para especificar un rol

1. De forma predeterminada, `CloudTrail_CloudWatchLogs_Role` se especifica automáticamente. La política de roles predeterminada posee los permisos necesarios para crear una secuencia de registros de CloudWatch Logs en un grupo de registros que se haya especificado y para enviar eventos de CloudTrail a dicha secuencia.

   > **Note**
   >
   > Si desea utilizar este rol para un grupo de registro para un registro de seguimiento de organización, debe modificar manualmente la política después de crear el rol. Para obtener más información, consulte este ejemplo de política y Creación de un registro de seguimiento para una organización.

   a. Para verificar el rol, vaya a la consola de AWS Identity and Access Management en https://console.aws.amazon.com/iam/.
   b. Elija Roles y, a continuación, seleccione CloudTrail_CloudWatchLogs_Role.
   c. En la pestaña Permisos, expanda la política para ver su contenido.
2. Puede especificar otro rol, pero debe adjuntar la política de roles necesaria al rol existente si desea utilizarlo para enviar eventos a CloudWatch Logs. Para obtener más información, consulte Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear.

Visualizar eventos en la consola de CloudWatch

Después de configurar el registro de seguimiento para enviar eventos al grupo de registros de CloudWatch Logs, puede ver los eventos en la consola de CloudWatch. CloudTrail envía los eventos al grupo de registro cinco minutos después de hacer una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el Acuerdo de nivel de servicios de AWS CloudTrail.

Para visualizar eventos en la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación de la izquierda, en Registros, seleccione Grupos de registros.
3. Elija el grupo de registros especificado para el registro de seguimiento.

4. Seleccione el flujo de registro que desea ver.
5. Para ver los detalles del evento que ha registrado el registro de seguimiento, elija un evento.

> **Note**
>
> La columna Time (UTC) (Hora [UTC]) de la consola de CloudWatch indica cuándo se envió el evento al grupo de registros. Para ver la hora real en la que CloudTrail registró el evento, consulte el campo `eventTime`.

Configuración del monitoreo de CloudWatch Logs con la AWS CLI

Puede utilizar la AWS CLI para configurar CloudTrail y enviar eventos a CloudWatch Logs con fines de monitoreo.

Creación de un grupo de registros

1. Si no dispone de un grupo de registros, cree un grupo de registros de CloudWatch Logs como un punto de enlace de envío para los eventos de registro mediante el comando `create-log-group` de CloudWatch Logs.

   ```
   aws logs create-log-group --log-group-name name
   ```

   El ejemplo siguiente crea un grupo de registros denominado `CloudTrail/logs`:

   ```
   aws logs create-log-group --log-group-name CloudTrail/logs
   ```

2. Recupere el nombre de recurso de Amazon (ARN) del grupo de registros.

   ```
   aws logs describe-log-groups
   ```

Creación de un rol

Cree un rol para CloudTrail que permita enviar eventos al grupo de registros de CloudWatch Logs. El comando `create-role` de IAM utiliza dos parámetros: un nombre de rol y una ruta de archivo a un documento de políticas de roles en formato JSON. El documento de políticas que utiliza concederá

permisos `AssumeRole` a CloudTrail. El comando `create-role` crea el rol con los permisos necesarios.

Para crear el archivo JSON que contendrá el documento de política, abra un editor de texto y guarde el siguiente contenido de política en un archivo denominado `assume_role_policy_document.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Ejecute el siguiente comando para crear el rol con permisos `AssumeRole` para CloudTrail.

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

Cuando el comando se complete, tome nota del ARN del rol en la salida.

Creación de un documento de políticas

Cree el siguiente documento de políticas de roles para CloudTrail. Este documento concede a CloudTrail los permisos necesarios para crear una secuencia de registros de CloudWatch Logs en el grupo de registros que especifique y enviar eventos de CloudTrail a dicha secuencia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
```

```
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

Guarde el documento de políticas en un archivo denominado `role-policy-document.json`.

Si está creando una política que podría utilizarse también para registros de seguimiento de organización, tendrá que configurarla de forma ligeramente distinta. Por ejemplo, la siguiente política concede a CloudTrail los permisos necesarios para crear una secuencia de registros de CloudWatch Logs en el grupo de registros que especifique y para enviar eventos de CloudTrail a esa secuencia de registros tanto para los registros de seguimiento de la cuenta 111111111111 de AWS como para los registros de seguimiento de la organización creados en la cuenta 111111111111 que se aplican a la organización de AWS Organizations con el ID de *o-exampleorgid*:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
```

```
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Para obtener más información acerca de los registros de seguimiento de organización, consulte Creación de un registro de seguimiento para una organización.

Ejecute el siguiente comando para aplicar la política al rol.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

Actualización del registro de seguimiento

Actualice el registro de seguimiento con el grupo de registros y la información de rol mediante el comando `update-trail` de CloudTrail.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

Para obtener más información sobre los comandos de AWS CLI, consulte la Referencia de línea de comandos de AWS CloudTrail.

Limitación

Registros de CloudWatch y EventBridge permiten un tamaño máximo de evento de 256 KB. Aunque la mayoría de los eventos de servicio tienen un tamaño máximo de 256 KB, algunos servicios tienen eventos aún más grandes. CloudTrail no envía estos eventos a Registros de CloudWatch o EventBridge.

A partir de la versión 1.05 de eventos de CloudTrail, los eventos tienen un tamaño máximo de 256 KB. Esto es para ayudar a prevenir la explotación por parte de actores maliciosos y permitir que otros servicios de AWS, como Registros de CloudWatch y EventBridge, consuman los eventos.

Creación de alarmas de CloudWatch para eventos de CloudTrail: ejemplos

En este tema se describe cómo se configuran alarmas para eventos de CloudTrail y se incluyen ejemplos.

Temas

- Requisitos previos
- Creación de un filtro de métricas y de una alarma
- Ejemplo de cambios de configuración del grupo de seguridad
- Ejemplo de errores de inicio de sesión en la AWS Management Console
- Ejemplo: cambios en política de IAM
- Configuración de notificaciones para alarmas de CloudWatch Logs

Requisitos previos

Para poder utilizar los ejemplos en este tema, debe:

- Creación de un registro de seguimiento con la consola o CLI.
- Creación de un grupo de registros como parte de la creación de un registro de seguimiento. Para obtener más información acerca de la creación de un registro de seguimiento, consulte Creación de un registro de seguimiento.
- Especifique o cree un rol de IAM que conceda a CloudTrail permisos para crear una secuencia de registros de CloudWatch Logs en el grupo de registros que especifique y para entregar eventos de CloudTrail a dicha secuencia de registros. El valor predeterminado `CloudTrail_CloudWatchLogs_Role` se encarga de ello por usted.

Para obtener más información, consulte Envío de eventos a Amazon CloudWatch Logs. Los ejemplos de esta sección se realizan en la consola de Amazon CloudWatch Logs. Para obtener más información sobre cómo crear alarmas y filtros de métricas, consulte Creación de métricas a partir de eventos de registro mediante filtros y Uso de alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Creación de un filtro de métricas y de una alarma

Para crear una alarma, primero debe crear un filtro de métricas y, a continuación, configurar una alarma en función del filtro. Los procedimientos se muestran para todos los ejemplos. Para obtener más información sobre la sintaxis de los filtros de métricas y los patrones de los eventos de registro de CloudTrail, consulte las secciones relacionadas con JSON de Filtros y sintaxis de patrones en la guía del usuario de Amazon CloudWatch Logs.

Ejemplo de cambios de configuración del grupo de seguridad

Siga este procedimiento para crear una alarma de Amazon CloudWatch que se desencadene cuando se produzcan cambios en la configuración de grupos de seguridad.

Creación del filtro de métricas

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, en Registros, seleccione Grupos de registros.
3. En la lista de grupos de registro, seleccione el grupo de registro que ha creado para el registro de seguimiento.
4. En el menú Filtros de métrica o Acciones, seleccione Crear filtro de métrica.
5. En la página Define pattern (Definir patrón), vaya a Create filter pattern (Crear patrón de filtro) e ingrese lo siguiente para Filter pattern (Patrón de filtro).

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. En Test pattern (Probar patrón), deje los valores predeterminados. Elija Next (Siguiente).
7. En la página Asignar métrica, vaya a Nombre de filtro e introduzca **`SecurityGroupEvents`**.
8. En Detalles de métrica, active Crear nueva y, a continuación, introduzca **`CloudTrailMetrics`** en Espacio de nombres de métrica.

9. En Nombre de métrica, escriba **`SecurityGroupEventCount`**.
10. En Valor de la métrica, escriba **`1`**.
11. Deje Default value (Valor predeterminado) en blanco.
12. Elija Next (Siguiente).
13. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Seleccione Create metric filter (Crear filtro de métricas) para crear el filtro, o elija Edit (Editar) para volver y cambiar los valores.

Crear una alarma

Después de crear el filtro de métricas, se abre la página de detalles del grupo de registros de CloudWatch Logs para el grupo de registros de seguimiento de CloudTrail. Siga este procedimiento para crear una alarma.

1. En la página Metric filters (Filtros de métricas), busque el filtro de métrica que creó en the section called “Creación del filtro de métricas”. Complete la casilla de verificación del filtro de métricas. En la barra Metric filters (Filtros de métricas), elija Create alarm (Crear alarma).
2. En Especificar métrica y condiciones, introduzca lo siguiente.
   a. Para Graph (Gráfico), la línea se establece en **`1`** en función de otras configuraciones que realice al crear la alarma.
   b. Para Metric name (Nombre de métrica), conserve el nombre de métrica actual, **`SecurityGroupEventCount`**.
   c. Para Statistic (Estadística), conserve el valor predeterminado, **`Sum`**.
   d. Para Period (Periodo), conserve el valor predeterminado, **`5 minutes`**.
   e. En la sección Conditions (Condiciones), vaya a Threshold type (Tipo de umbral) y escriba Static (Estático).
   f. Cuando ***`metric_name`*** es, elija Greater/Equal (Mayor/Igual).
   g. Para el valor de umbral, introduzca **`1`**.
   h. En Additional configuration (Configuración adicional), deje los valores predeterminados. Elija Next (Siguiente).
3. En la página Configurar acciones, seleccione Notificación y, a continuación, seleccione En alarma, que indica que la acción se lleva a cabo cuando se cruza el umbral de un evento de cambio en cinco minutos, y SecurityGroupEventCount está en estado de alarma.

a. En Enviar una notificación al siguiente tema de SNS, seleccione Crear un tema nuevo.

b. Introduzca **`SecurityGroupChanges_CloudWatch_Alarms_Topic`** como el nombre del nuevo tema de Amazon SNS.

c. En Puntos de conexión de correo electrónico que recibirán la notificación, introduzca las direcciones de correo electrónico de los usuarios que desea que reciban notificaciones si se produce esta alarma. Separe las direcciones de email con comas.

   Todos los destinatarios de correo electrónico recibirán un correo electrónico en el que se les solicita que confirmen que desean suscribirse al tema de Amazon SNS.

d. Elija Create new topic.

4. En este ejemplo, omita los otros tipos de acción. Elija Next (Siguiente).
5. En la página Add name and description (Agregar nombre y descripción), ingrese un nombre fácil de recordar para la alarma y una descripción. En este ejemplo, ingrese **`Security group configuration changes`** para el nombre y **`Raises alarms if security group configuration changes occur`** para la descripción. Elija Next (Siguiente).
6. En la página Preview and create (Ver de manera preliminar y crear), revise las opciones seleccionadas. Seleccione Edit (Editar) para realizar cambios, o elija Create alarm (Crear alarma) para crear la alarma.

   Después de crear la alarma, CloudWatch abre la página Alarms (Alarmas). La columna Actions (Acciones) de la alarma muestra Pending confirmation (Confirmación pendiente) hasta que todos los destinatarios de email del tema SNS hayan confirmado que desean suscribirse a las notificaciones de SNS.

Ejemplo de errores de inicio de sesión en la AWS Management Console

Siga este procedimiento para crear una alarma de Amazon CloudWatch que se desencadene cuando se produzcan tres o más errores de inicio de sesión en la AWS Management Console durante un periodo de cinco minutos.

Creación del filtro de métricas

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, en Registros, seleccione Grupos de registros.
3. En la lista de grupos de registro, seleccione el grupo de registro que ha creado para el registro de seguimiento.

4. En el menú Filtros de métrica o Acciones, seleccione Crear filtro de métrica.
5. En la página Define pattern (Definir patrón), vaya a Create filter pattern (Crear patrón de filtro) e ingrese lo siguiente para Filter pattern (Patrón de filtro).

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. En Test pattern (Probar patrón), deje los valores predeterminados. Elija Next (Siguiente).
7. En la página Asignar métrica, vaya a Nombre de filtro e introduzca **`ConsoleSignInFailures`**.
8. En Detalles de métrica, active Crear nueva y, a continuación, introduzca **`CloudTrailMetrics`** en Espacio de nombres de métrica.
9. En Nombre de métrica, escriba **`ConsoleSigninFailureCount`**.
10. En Valor de la métrica, escriba **`1`**.
11. Deje Default value (Valor predeterminado) en blanco.
12. Elija Next (Siguiente).
13. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Seleccione Create metric filter (Crear filtro de métricas) para crear el filtro, o elija Edit (Editar) para volver y cambiar los valores.

Crear una alarma

Después de crear el filtro de métricas, se abre la página de detalles del grupo de registros de CloudWatch Logs para el grupo de registros de seguimiento de CloudTrail. Siga este procedimiento para crear una alarma.

1. En la página Metric filters (Filtros de métricas), busque el filtro de métrica que creó en the section called “Creación del filtro de métricas”. Complete la casilla de verificación del filtro de métricas. En la barra Metric filters (Filtros de métricas), elija Create alarm (Crear alarma).
2. En la página Create Alarm (Crear alarma), vaya a Specify metric and conditions (Especificar métrica y condiciones) e ingrese lo siguiente.
   a. Para Graph (Gráfico), la línea se establece en **`3`** en función de otras configuraciones que realice al crear la alarma.
   b. Para Metric name (Nombre de métrica), conserve el nombre de métrica actual, **`ConsoleSigninFailureCount`**.
   c. Para Statistic (Estadística), conserve el valor predeterminado, **`Sum`**.

d. Para Period (Periodo), conserve el valor predeterminado, **`5 minutes`**.

e. En la sección Conditions (Condiciones), vaya a Threshold type (Tipo de umbral) y escriba Static (Estático).

f. Cuando ***`metric_name`*** es, elija Greater/Equal (Mayor/Igual).

g. Para el valor de umbral, introduzca **`3`**.

h. En Additional configuration (Configuración adicional), deje los valores predeterminados. Elija Next (Siguiente).

3. En la página Configurar acciones, en Notificación, seleccione En alarma, que indica que la acción se lleva a cabo cuando se cruza el umbral de tres eventos de cambio en cinco minutos y que ConsoleSigninFailureCount está en estado de alarma.

   a. En Enviar una notificación al siguiente tema de SNS, seleccione Crear un tema nuevo.

   b. Introduzca **`ConsoleSignInFailures_CloudWatch_Alarms_Topic`** como el nombre del nuevo tema de Amazon SNS.

   c. En Puntos de conexión de correo electrónico que recibirán la notificación, introduzca las direcciones de correo electrónico de los usuarios que desea que reciban notificaciones si se produce esta alarma. Separe las direcciones de email con comas.

      Todos los destinatarios de correo electrónico recibirán un correo electrónico en el que se les solicita que confirmen que desean suscribirse al tema de Amazon SNS.

   d. Elija Create new topic.

4. En este ejemplo, omita los otros tipos de acción. Elija Next (Siguiente).

5. En la página Add name and description (Agregar nombre y descripción), ingrese un nombre fácil de recordar para la alarma y una descripción. En este ejemplo, ingrese **`Console sign-in failures`** para el nombre y **`Raises alarms if more than 3 console sign-in failures occur in 5 minutes`** para la descripción. Elija Next (Siguiente).

6. En la página Preview and create (Ver de manera preliminar y crear), revise las opciones seleccionadas. Seleccione Edit (Editar) para realizar cambios, o elija Create alarm (Crear alarma) para crear la alarma.

   Después de crear la alarma, CloudWatch abre la página Alarms (Alarmas). La columna Actions (Acciones) de la alarma muestra Pending confirmation (Confirmación pendiente) hasta que todos los destinatarios de email del tema SNS hayan confirmado que desean suscribirse a las notificaciones de SNS.

Ejemplo: cambios en política de IAM

Siga este procedimiento para crear una alarma de Amazon CloudWatch que se desencadene cuando se produzca una llamada a la API para cambiar una política de IAM.

Creación del filtro de métricas

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Logs.
3. En la lista de grupos de registro, seleccione el grupo de registro que ha creado para el registro de seguimiento.
4. Elija Actions (Acciones) y, a continuación, seleccione Create metric filter (Crear filtro de métrica).
5. En la página Define pattern (Definir patrón), vaya a Create filter pattern (Crear patrón de filtro) e ingrese lo siguiente para Filter pattern (Patrón de filtro).

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. En Test pattern (Probar patrón), deje los valores predeterminados. Elija Next (Siguiente).
7. En la página Asignar métrica, vaya a Nombre de filtro e introduzca **`IAMPolicyChanges`**.
8. En Detalles de métrica, active Crear nueva y, a continuación, introduzca **`CloudTrailMetrics`** en Espacio de nombres de métrica.
9. En Nombre de métrica, escriba **`IAMPolicyEventCount`**.
10. En Valor de la métrica, escriba **`1`**.
11. Deje Default value (Valor predeterminado) en blanco.
12. Elija Next (Siguiente).
13. En la página Review and create (Revisar y crear), revise las opciones seleccionadas. Seleccione Create metric filter (Crear filtro de métricas) para crear el filtro, o elija Edit (Editar) para volver y cambiar los valores.

Crear una alarma

Después de crear el filtro de métricas, se abre la página de detalles del grupo de registros de CloudWatch Logs para el grupo de registros de seguimiento de CloudTrail. Siga este procedimiento para crear una alarma.

1. En la página Metric filters (Filtros de métricas), busque el filtro de métrica que creó en the section called “Creación del filtro de métricas”. Complete la casilla de verificación del filtro de métricas. En la barra Metric filters (Filtros de métricas), elija Create alarm (Crear alarma).
2. En la página Create Alarm (Crear alarma), vaya a Specify metric and conditions (Especificar métrica y condiciones) e ingrese lo siguiente.

   a. Para Graph (Gráfico), la línea se establece en **1** en función de otras configuraciones que realice al crear la alarma.

   b. Para Metric name (Nombre de métrica), conserve el nombre de métrica actual, **`IAMPolicyEventCount`**.

   c. Para Statistic (Estadística), conserve el valor predeterminado, **`Sum`**.

   d. Para Period (Periodo), conserve el valor predeterminado, **`5 minutes`**.

   e. En la sección Conditions (Condiciones), vaya a Threshold type (Tipo de umbral) y escriba Static (Estático).

   f. Cuando ***`metric_name`*** es, elija Greater/Equal (Mayor/Igual).

   g. Para el valor de umbral, introduzca **`1`**.

   h. En Additional configuration (Configuración adicional), deje los valores predeterminados. Elija Next (Siguiente).

   i.
3. En la página Configurar acciones, en Notificación, seleccione En alarma, que indica que la acción se lleva a cabo cuando se cruza el umbral de un evento de cambio en cinco minutos y que IAMPolicyEventCount está en estado de alarma.

   a. En Enviar una notificación al siguiente tema de SNS, seleccione Crear un tema nuevo.

   b. Introduzca **`IAM_Policy_Changes_CloudWatch_Alarms_Topic`** como el nombre del nuevo tema de Amazon SNS.

   c. En Puntos de conexión de correo electrónico que recibirán la notificación, introduzca las direcciones de correo electrónico de los usuarios que desea que reciban notificaciones si se produce esta alarma. Separe las direcciones de email con comas.

Todos los destinatarios de correo electrónico recibirán un correo electrónico en el que se les solicita que confirmen que desean suscribirse al tema de Amazon SNS.

d. Elija Create new topic.

4. En este ejemplo, omita los otros tipos de acción. Elija Next (Siguiente).
5. En la página Add name and description (Agregar nombre y descripción), ingrese un nombre fácil de recordar para la alarma y una descripción. En este ejemplo, ingrese **`IAM Policy Changes`** para el nombre y **`Raises alarms if IAM policy changes occur`** para la descripción. Elija Next (Siguiente).
6. En la página Preview and create (Ver de manera preliminar y crear), revise las opciones seleccionadas. Seleccione Edit (Editar) para realizar cambios, o elija Create alarm (Crear alarma) para crear la alarma.

   Después de crear la alarma, CloudWatch abre la página Alarms (Alarmas). La columna Actions (Acciones) de la alarma muestra Pending confirmation (Confirmación pendiente) hasta que todos los destinatarios de email del tema SNS hayan confirmado que desean suscribirse a las notificaciones de SNS.

Configuración de notificaciones para alarmas de CloudWatch Logs

Puede configurar CloudWatch Logs para enviar una notificación cuando se desencadene una alarma para CloudTrail. De esta forma, podrá responder de forma rápida a eventos operativos críticos registrados en eventos de CloudTrail y detectados por CloudWatch Logs. CloudWatch utiliza Amazon Simple Notification Service (SNS) para enviar email. Para obtener más información, consulte Configuración de Amazon SNS en la Guía para desarrolladores de CloudWatch.

Impedir que CloudTrail envíe eventos a CloudWatch Logs

Puede dejar de enviar eventos de AWS CloudTrail a Amazon CloudWatch Logs al actualizar un registro de seguimiento para desactivar la configuración de CloudWatch Logs.

Detener el envío de eventos a CloudWatch Logs (consola)

Para dejar de enviar eventos de CloudTrail a CloudWatch Logs

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

2. En el panel de navegación, seleccione Trails.
3. Elija el nombre del registro de seguimiento para el que desea desactivar la integración de CloudWatch Logs.
4. En CloudWatch Logs, elija Edit (Editar).
5. Elimine la selección del recuadro Enabled (Habilitado).
6. Elija Save changes (Guardar cambios).

Dejar de enviar eventos a CloudWatch Logs (CLI)

Para eliminar el grupo de registros de CloudWatch Logs como punto de enlace de entrega, ejecute el comando update-trail. El siguiente comando borra el grupo de registros y el rol de la configuración de registro de seguimiento al reemplazar los valores del ARN del grupo de registros y el ARN del rol de CloudWatch Logs con valores vacíos.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

Grupo de registros de CloudWatch y nomenclatura de secuencias de registros para CloudTrail

Amazon CloudWatch mostrará el grupo de registro que usted creó para eventos de CloudTrail junto con cualquier otro grupo de registro que tenga en una región. Le recomendamos que utilice un nombre de grupo de registros que le permita distinguirlo de otros grupos de registros. Por ejemplo, **`CloudTrail/logs`**.

Cuando asigne un nombre al grupo de registros, siga estas directrices:

- Los nombres de los grupos de registro deben ser únicos en una región para una Cuenta de AWS.
- Los nombres de grupo de registros puede tener de 1 a 512 caracteres de longitud.
- Los nombres del grupo de registros pueden tener los siguientes caracteres: a-z, A-Z, 0-9, '_' (guion bajo), '-' (guion), '/' (barra inclinada), '.' (punto) y '#' (numeral).

Cuando CloudTrail crea un flujo de registro para el grupo de registro, asigna un nombre al flujo de registro conforme al siguiente formato: *account_ID*_CloudTrail_*trail_region*.

> **Note**
>
> Si el volumen de registros de CloudTrail es grande, se pueden crear varias secuencias de registros para enviar datos de registro a su grupo de registros. Cuando hay varios flujos de registro, CloudTrail asigna un nombre a cada flujo de registro según el siguiente formato: *account_ID*_CloudTrail_*trail_region_number*.

Para obtener más información sobre los grupos de registros de CloudWatch, consulte Trabajar con grupos y secuencias de registros. en la Guía del usuario de Amazon CloudWatch Logs y CreateLogGroup en la Referencia de la API de Amazon CloudWatch Logs.

Documento de política de roles CloudTrail para usar CloudWatch registros para monitorear

En esta sección se describe la política de permisos necesaria para que el CloudTrail rol envíe eventos de registro a CloudWatch Logs. Puede adjuntar un documento de política a un rol cuando lo configura CloudTrail para enviar eventos, como se describe enEnvío de eventos a Amazon CloudWatch Logs. También puede crear un rol con IAM. Para obtener más información, consulte Creación de un rol para un AWS servicio (AWS Management Console) o Creación de un rol (CLI y API).

El siguiente documento de política de ejemplo contiene los permisos necesarios para crear un CloudWatch flujo de registro en el grupo de registros que especifique y para enviar CloudTrail eventos a ese flujo de registro en la región EE.UU. Este (Ohio). (Esta es la política predeterminada para el rol de IAM predeterminado `CloudTrail_CloudWatchLogs_Role`).

> **Note**
>
> La política de funciones de supervisión de registros no se aplica a la política de funciones de supervisión de CloudWatch registros. La política de roles no admite el uso de `aws:SourceArn` y`aws:SourceAccount`.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

Si va a crear una política que también se puede utilizar para los registros de seguimiento de organización, deberá modificarla a partir la política predeterminada creada para el rol. *Por ejemplo, la siguiente política otorga CloudTrail los permisos necesarios para crear un flujo de registro de CloudWatch registros en el grupo de registros que especifiques como valor de log_group_name, y para enviar CloudTrail eventos a ese flujo de registro tanto para los registros de la cuenta 1111 como para los registros de la organización creados en la AWS cuenta 1111 que se aplican a la AWS Organizations organización con el identificador de o-exampleorgid:*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
```

```
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Para obtener más información acerca de los registros de seguimiento de organización, consulte Creación de un registro de seguimiento para una organización.

Recepción de archivos de CloudTrail registro de varias cuentas

Puede hacer que CloudTrail entregue archivos de registro de varios Cuentas de AWS a un único bucket de Amazon S3. Por ejemplo, tiene cuatro Cuentas de AWS con los identificadores de cuenta 1111, 222222222222, 333333333333 y 444444444444, y desea configurarlos para entregar los archivos de registro de estas cuatro cuentas CloudTrail a un depósito que pertenece a la cuenta 1111. Para ello, siga los pasos que se describen a continuación por orden:

1. Active un registro de seguimiento en la cuenta a la que pertenecerá el bucket de destino (111111111111 en este ejemplo). No cree ningún registro de seguimiento para las demás cuentas todavía.

Para obtener instrucciones, consulte Creación de un registro de seguimiento en la consola.

2. Actualice la política en su bucket de destino para conceder permisos entre cuentas a CloudTrail.

   Para obtener instrucciones, consulte Configuración de la política de bucket para varias cuentas.

3. Cree un registro de seguimiento en las demás cuentas (222222222222, 333333333333 y 444444444444 en este ejemplo) en las que desee registrar la actividad. Cuando cree el registro de seguimiento en cada cuenta, especifique el bucket de Amazon S3 que pertenece a la cuenta que ha especificado en el paso 1 (111111111111 en este ejemplo). Para obtener instrucciones, consulte Crea registros de seguimiento en cuentas adicionales.

> **Note**
>
> Si decide habilitar el cifrado SSE-KMS, la política de claves de KMS debe permitir el uso de la clave CloudTrail para cifrar los archivos de registro y permitir que los usuarios que especifique lean los archivos de registro sin cifrar. Para obtener más información sobre cómo editar manualmente la política de claves, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

Eliminación de los ID de las cuentas de los propietarios de los buckets para eventos de datos llamados por otras cuentas

Históricamente, si CloudTrail los eventos de datos estaban habilitados en una persona que llamaba a la API Cuenta de AWS de eventos de datos de Amazon S3, se CloudTrail mostraba el ID de cuenta del propietario del bucket de S3 en el evento de datos (por ejemplo,`PutObject`). Esto ocurría incluso si la cuenta del propietario del bucket no tenía activados los eventos de datos de S3.

Ahora, CloudTrail elimina el ID de cuenta del propietario del bucket de S3 del `resources` bloque si se cumplen las dos condiciones siguientes:

- La llamada a la API del evento de datos proviene de un propietario Cuenta de AWS diferente al del bucket de Amazon S3.
- El llamante de la API recibió un error `AccessDenied` que era solo para la cuenta del llamante.

El propietario del recurso en el que se realizó la llamada a la API sigue recibiendo el evento completo.

Los siguientes fragmentos de registro de eventos son un ejemplo del comportamiento esperado. En el fragmento `Historic`, se muestra el ID de cuenta 123456789012 del propietario del bucket de S3 a un llamante de la API de otra cuenta. En el ejemplo del comportamiento actual, no se muestra el ID de la cuenta del propietario del bucket.

```
# Historic

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

El siguiente es el comportamiento actual.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

Temas

- Configuración de la política de bucket para varias cuentas
- Crea registros de seguimiento en cuentas adicionales

Configuración de la política de bucket para varias cuentas

Para que un bucket reciba archivos de registros desde varias cuentas, su política de bucket debe conceder permiso a CloudTrail para escribir los archivos de registros desde todas las cuentas que especifique. Esto significa que debe modificar la política de bucket en su bucket de destino para conceder a CloudTrail permiso para escribir los archivos de registros desde cada cuenta especificada.

> **Note**
>
> Por motivos de seguridad, los usuarios sin autorización no pueden crear un registro de seguimiento que incluya `AWSLogs/` como parámetro `S3KeyPrefix`.

Para modificar los permisos de bucket para que los archivos puedan recibirse desde varias cuentas

1. Inicie sesión en la AWS Management Console con la cuenta que posee el bucket (111111111111 en este ejemplo) y abra la consola de Amazon S3.
2. Elija el bucket al que CloudTrail envía los archivos de registros y, a continuación, elija Permissions (Permisos).
3. Para Bucket policy (Política de bucket), elija Edit (Editar).
4. Modifique la política existente para añadir una línea para cada cuenta adicional cuyos archivos de registro desea enviar a este bucket. Consulte la siguiente política de ejemplo y preste atención a la línea `Resource` subrayada donde se especifica un segundo ID de cuenta. Como práctica recomendada de seguridad, agregue una clave de conción `aws:SourceArn` de la política de bucket de Amazon S3. Esto ayuda a evitar el acceso no autorizado a su bucket de S3. Si tiene trazas existentes, asegúrese de agregar una o más claves de condición.

   > **Note**
   >
   > Un ID de cuenta de AWS es un número de 12 dígitos, incluidos los ceros delanteros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
              "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
            ]
          }
       }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ],
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Crea registros de seguimiento en cuentas adicionales

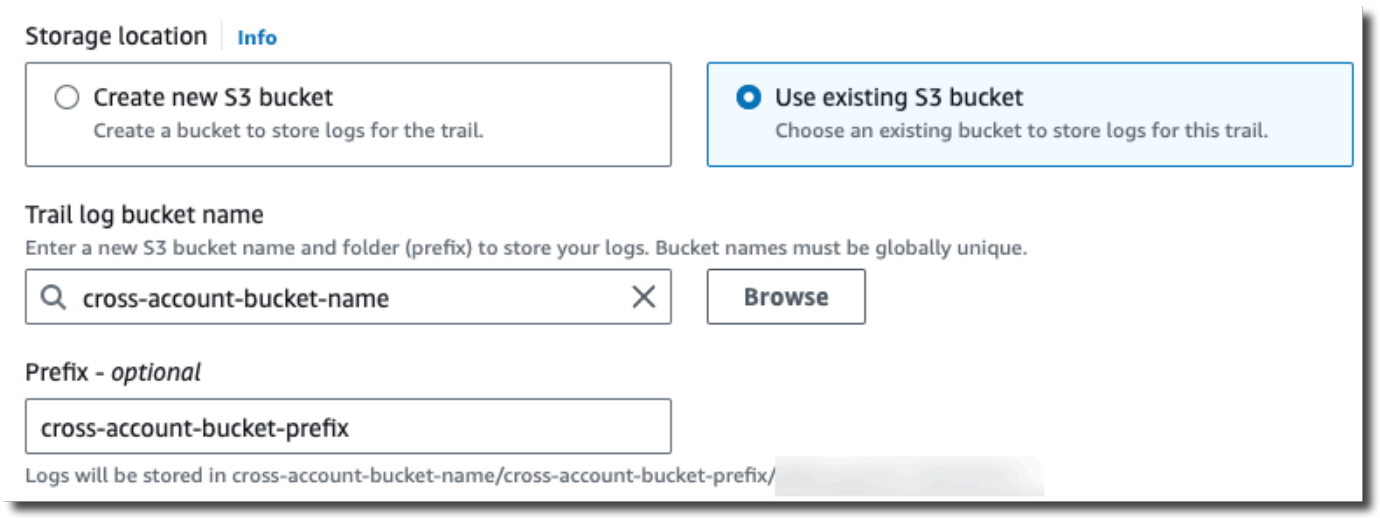
Puede utilizar la consola o la interfaz de la línea de comandos para crear registros de seguimiento en más cuentas de AWS y agregar sus archivos de registro en un bucket de Amazon S3.

Uso de la consola para crear registros de seguimiento en más cuentas de AWS

Puede utilizar la consola de CloudTrail para crear registros de seguimiento en más cuentas.

1. Inicie sesión en la AWS Management Console con la cuenta para la que desea crear un registro de seguimiento. Siga los pasos de Creación de un registro de seguimiento en la consola para crear un registro de seguimiento mediante la consola.
2. En Storage Location (Ubicación de almacenamiento), elija Use existing S3 bucket (Usar bucket de S3 existente). Use la casilla de texto para introducir el nombre del bucket que usa a fin de almacenar los archivos de registro de todas las cuentas.

> **Note**
>
> La política del bucket debe conceder permiso a CloudTrail para escribir en él. Para obtener más información sobre cómo editar manualmente la política del bucket, consulte Configuración de la política de bucket para varias cuentas.



3. En Prefijo, introduzca el prefijo que utiliza para almacenar los archivos de registro en todas las cuentas. Si decide utilizar un prefijo distinto al que especificó en la política del bucket, deberá

editar la política del bucket en su bucket de destino para permitir que CloudTrail escriba archivos de registros en su bucket con este nuevo prefijo.

Uso de la CLI para crear un registro de seguimiento en más cuentas de AWS

Puede utilizar las herramientas de la línea de comandos de AWS para crear registros de seguimiento en más cuentas y agregar sus archivos de registro en un bucket de Amazon S3. Para obtener más información sobre estas herramientas, consulte la Guía del usuario de AWS Command Line Interface.

Cree un registro de seguimiento mediante el comando create-trail y especifique lo siguiente:

- `--name` especifica el nombre del registro de seguimiento.
- `--s3-bucket-name` especifica el bucket de Amazon S3 que utiliza para almacenar los archivos de registro de todas las cuentas.
- `--s3-prefix` especifica un prefijo para la ruta de envío de los archivos de registro (opcional).
- `--is-multi-region-trail` especifica que este registro de seguimiento registrará los eventos en todas las regiones de AWS en la partición en la que trabaja.

Puede crear un registro de seguimiento para cada región en la que una cuenta ejecuta recursos de AWS.

El siguiente comando de ejemplo muestra cómo crear un registro de seguimiento para sus otras cuentas mediante la AWS CLI. Para enviar archivos de registros para estas cuentas al bucket que ha creado en su primera cuenta (en este ejemplo, 111111111111), especifique el nombre del bucket en la opción `--s3-bucket-name`. Los nombres del bucket de Amazon S3 son exclusivos a nivel global.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail
```

Al ejecutar el comando, verá un resultado parecido al siguiente:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
```

```
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

Para obtener más información sobre el uso de CloudTrail desde las herramientas de línea de comandos de AWS, consulte la Referencia de línea de comandos de CloudTrail.

Compartir archivos de registro de CloudTrail entre cuentas de AWS

En esta sección se explica cómo compartir archivos de registro de CloudTrail entre varias cuentas de AWS. El enfoque que utilice para compartir los registros entre Cuentas de AWS depende de la configuración del bucket de S3. Estas son las opciones para compartir archivos de registro:

- Configuración impuesta por el propietario del bucket: S3 Object Ownership es una configuración de nivel de bucket de Amazon S3 que puede usar para controlar la propiedad de los objetos que se cargan en el bucket y para habilitar o deshabilitar las listas de control de acceso (ACL). De forma predeterminada, Object Ownership se establece en la configuración impuesta por el propietario del bucket y todas las ACL están deshabilitadas. Cuando las ACL están deshabilitadas, el propietario del bucket posee todos los objetos del bucket y administra el acceso a los datos de forma exclusiva mediante políticas de administración de acceso. Cuando se establece la opción impuesta por el propietario del bucket, el acceso se administra con la política del bucket, lo que elimina la necesidad de que los usuarios asuman un rol.
- Asumir un rol para compartir los archivos de registro: si no ha elegido la configuración impuesta por el propietario del bucket, los usuarios deberán asumir un rol para acceder a los archivos de registro de su bucket de S3.

Comparta archivos de registros entre cuentas asumiendo un rol

> **Note**
>
> Esta sección se aplica únicamente a los buckets de Amazon S3 que no utilizan la configuración impuesta por el propietario del bucket.

En esta sección, se explica cómo compartir archivos de registro de CloudTrail entre varias Cuentas de AWS mediante la adopción de un rol y se describen los escenarios para compartir archivos de registro.

- Escenario 1: conceder acceso de solo lectura a las cuentas que han generado los archivos de registro ubicados en el bucket de Amazon S3.
- Escenario 2: conceder acceso a todos los archivos de registro de su bucket de Amazon S3 a una cuenta de terceros que pueda analizar los archivos de registro por usted.

Para conceder acceso de solo lectura a los archivos de registro del bucket de Amazon S3

1. Cree un rol de IAM para cada cuenta con la que desea compartir archivos de registro. Debe ser administrador para conceder el permiso.

   Al crear el rol, haga lo siguiente:

   - Elija la opción Otra Cuenta de AWS.
   - Escriba el ID de 12 dígitos de la cuenta para conceder acceso.
   - Marque la casilla Require MFA si desea que el usuario proporcione autenticación multifactor antes de asumir el rol.
   - Elija la política AmazonS3ReadOnlyAccess.

   > **Note**
   >
   > De forma predeterminada, la política AmazonS3ReadOnlyAccess garantiza la recuperación y enumera los derechos a todos los buckets de Amazon S3 en su cuenta.

   A fin de obtener más información sobre la administración de permisos para los roles de IAM, consulte la sección roles de IAM en la Guía del usuario de IAM.
2. Cree una política de acceso que conceda acceso de solo lectura a la cuenta con la que quiere compartir los archivos de registro.
3. Indique a cada cuenta que asuma un rol para recuperar los archivos de registro.

Conceder acceso de solo lectura a los archivos de registro con una cuenta de terceros

1. Cree un rol de IAM para la cuenta de terceros con la que desea compartir archivos de registro. Debe ser administrador para conceder el permiso.

   Al crear el rol, haga lo siguiente:

   - Elija la opción Otra Cuenta de AWS.
   - Escriba el ID de 12 dígitos de la cuenta para conceder acceso.
   - Escriba un ID externo que proporcione más control sobre quién puede asumir el rol. Para obtener más información, consulte Cómo utilizar un ID externo al conceder acceso a los recursos de AWS a terceros en la Guía del usuario de IAM.
   - Elija la política AmazonS3ReadOnlyAccess.

   > **Note**
   >
   > De forma predeterminada, la política AmazonS3ReadOnlyAccess garantiza la recuperación y enumera los derechos a todos los buckets de Amazon S3 en su cuenta.

2. Cree una política de acceso que conceda acceso de solo lectura a la cuenta de terceros con la que quiere compartir los archivos de registro.
3. Indique a la cuenta de terceros que asuma el rol de recuperar los archivos de registro.

En las secciones siguientes, se proporcionan más detalles sobre estos pasos.

Temas

- Crear una política de acceso para conceder acceso a las cuentas de su propiedad
- Crear una política de acceso para conceder acceso a un tercero
- Adopción de un rol
- Dejar de compartir archivos de registros de CloudTrail entre cuentas de AWS

Crear una política de acceso para conceder acceso a las cuentas de su propiedad

Como propietario del bucket de Amazon S3, tiene control completo sobre el bucket de Amazon S3 en el que CloudTrail escribe archivos de registro para las demás cuentas. Debe compartir los archivos

de registro de cada unidad de negocio con la unidad de negocio que los creó. pero no desea que una unidad pueda leer los archivos de registro de las demás unidades.

Por ejemplo, para compartir archivos de registros de la cuenta B con la cuenta B, pero no con la cuenta C, debe crear un nuevo rol de IAM en su cuenta que especifique que la cuenta B es de confianza. Esta política de confianza de rol especifica que se puede confiar en la Cuenta B para que asuma el rol creado por su cuenta y debe ser similar al siguiente ejemplo. La política de confianza se crea automáticamente si crea el rol mediante la consola. Si utiliza el SDK para crear el rol, debe indicar la política de confianza como un parámetro de la API `CreateRole`. Si utiliza la CLI para crear el rol, debe especificar la política de confianza en el comando de CLI `create-role`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Asimismo, debe crear una política de acceso para especificar que la Cuenta B pueda leer desde solo la ubicación en la que la Cuenta B escribió sus archivos de registro. La política de acceso debe tener un aspecto similar al siguiente. Tenga en cuenta que el recurso de ARN incluye el ID de cuenta de doce dígitos de la cuenta B y el prefijo especificado, si hay alguno, cuando activó CloudTrail para la cuenta B durante el proceso de agregación. Para obtener más información sobre cómo especificar un prefijo, consulte Crea registros de seguimiento en cuentas adicionales.

> **Important**
>
> Debe asegurarse de que el prefijo de la política de acceso sea exactamente igual al prefijo especificado cuando activó CloudTrail para la cuenta B. En caso contrario, debe editar la política de acceso del rol de IAM de su cuenta a fin de incorporar el prefijo real de la cuenta B. Si el prefijo de la política de acceso del rol no es exactamente el mismo que el prefijo que

especificó cuando activó CloudTrail en la cuenta B, esta no tendrá acceso a sus archivos de registros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

Utilice el proceso anterior para todas las demás cuentas adicionales.

Una vez creados los roles de cada cuenta y especificadas las políticas de acceso y de confianza correspondientes y cuando el administrador haya concedido acceso a un usuario de IAM de cada cuenta, un usuario de IAM de las cuentas B o C puede adoptar el rol mediante programación.

Para obtener más información, consulte Adopción de un rol.

Crear una política de acceso para conceder acceso a un tercero

Debe crear un rol de IAM independiente para una cuenta de terceros. Al crear el rol, AWS crea automáticamente la relación de confianza, que especifica que se puede confiar en la cuenta de terceros para que asuma el rol. La política de acceso del rol especifica qué acciones puede realizar

esa cuenta. Para obtener más información acerca de cómo crear roles, consulte Creación de un rol de IAM.

Por ejemplo, la relación de confianza creada por AWS especifica que se confía en que la cuenta de terceros (cuenta Z en este ejemplo) asuma el rol que usted creó. A continuación, se muestra un ejemplo de una política de confianza:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole"
    }]
}
```

Si ha especificado un ID externo al crear el rol para la cuenta de terceros, su política de acceso contiene un elemento `Condition` adicional que comprueba el ID exclusivo asignado por esa cuenta. La prueba se realiza cuando se asume el rol. La siguiente política de acceso de ejemplo contiene un elemento `Condition`.

Para obtener más información, consulte Cómo utilizar un ID externo al conceder acceso a los recursos de AWS a terceros en la Guía del usuario de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-account-Z"}}
    }]
}
```

También debe crear una política de acceso para su cuenta para especificar que la cuenta de terceros pueda leer todos los registros del bucket de Amazon S3. La política de acceso tendrá un aspecto similar a la del siguiente ejemplo. El carácter comodín (*) al final del valor de `Resource` indica que la

cuenta de terceros puede tener acceso a cualquier archivo de registro del bucket de S3 para el que se le ha concedido acceso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

Después de crear un rol para la cuenta de terceros y especificar la relación de confianza y la política de acceso correspondientes, un usuario de IAM de la cuenta de terceros debe adoptar el rol mediante programación a fin de poder leer archivos de registro del bucket. Para obtener más información, consulte Adopción de un rol.

Adopción de un rol

Debe designar un usuario de IAM independiente para que asuma cada rol que cree en cada cuenta. A continuación, debe asegurarse de que cada usuario de IAM tenga los permisos adecuados.

Usuarios y roles de IAM

Después de crear los roles y las políticas necesarias, debe designar un usuario de IAM en cada una de las cuentas con las que desea compartir archivos. Cada usuario de IAM asume mediante programación el rol apropiado para acceder a los archivos de registro. Cuando un usuario asume un rol, AWS devuelve las credenciales de seguridad temporales a ese usuario. A continuación, pueden

hacer solicitudes para enumerar, recuperar, copiar o eliminar archivos de registro en función de los permisos concedidos por la política de acceso asociada al rol.

Para obtener más información acerca de cómo trabajar con las identidades de IAM, consulte Identidades de IAM (usuarios, grupos de usuarios y roles).

La principal diferencia en la política de acceso que crea para cada rol de IAM en cada escenario.

- En el escenario 1, la política de acceso limita cada cuenta a leer solo sus propios archivos de registro. Para obtener más información, consulte Crear una política de acceso para conceder acceso a las cuentas de su propiedad.
- En el escenario 2, la política de acceso permite que un tercero lea todos los archivos de registro agregados en el bucket de Amazon S3. Para obtener más información, consulte Crear una política de acceso para conceder acceso a un tercero.

Creación de políticas de permisos para usuarios de IAM

Con el fin de llevar a cabo las acciones que permiten un rol, el usuario de IAM debe tener permiso para llamar a la API de AWS STS `AssumeRole`. Debe editar la política para cada usuario con el fin concederles los permisos pertinentes. Para ello, debe establecer un elemento de recurso en la política que vincule al usuario de IAM. En el ejemplo siguiente, se muestra una política para un usuario de IAM en otra cuenta que permite a este usuario adoptar un rol denominado `Test` creado anteriormente por la cuenta A.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

Para editar una política administrada por el cliente (consola)

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

2. En el panel de navegación, seleccione Policies (Políticas).
3. En la lista de políticas, elija el nombre de la política que desea editar. Puede utilizar el cuadro de búsqueda para filtrar la lista de políticas.
4. Seleccione la pestaña Permisos y, a continuación, Editar.
5. Haga una de las acciones siguientes:

   - Seleccione la opción Visual para cambiar la política sin conocer la sintaxis JSON. Puede realizar cambios en el servicio, acciones, recursos o condiciones opcionales para cada bloque de permisos en su política. También puede importar una política para añadir permisos adicionales en la parte inferior de la política. Cuando haya terminado con los cambios, seleccione Siguiente para continuar.
   - Seleccione la opción JSON para modificar la política escribiendo o pegando texto en el cuadro de texto JSON. También puede importar una política para añadir permisos adicionales en la parte inferior de la política. Resuelva las advertencias de seguridad, errores o advertencias generales generadas durante la validación de política y luego elija Next.

     > **Note**
     >
     > Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual. Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

6. En la página Revisar y guardar, revise los Permisos definidos en esta política y, a continuación, seleccione Guardar cambios para guardar su trabajo.
7. Si la política administrada ya tiene el máximo de cinco versiones, al seleccionar Guardar cambios aparecerá un cuadro de diálogo. Para guardar la nueva versión, se elimina la versión no predeterminada más antigua de la política y se sustituye con esta nueva versión. También puede configurar la nueva versión como versión predeterminada de la política.

   Seleccione Guardar cambios para guardar la nueva versión de la política.

Llamada a AssumeRole

Un usuario puede asumir un rol creando una aplicación que llama a la API `AssumeRole` de AWS STS y pasa el nombre de la sesión del rol, el número de recurso de Amazon (ARN) del rol a asumir

y un ID externo opcional. El nombre de la sesión del rol lo define la cuenta que creó el rol a asumir. El identificador externo, en su caso, lo define la cuenta de terceros y se pasa a la cuenta propietaria para su inclusión durante la creación del rol. Para obtener más información, consulte Cómo utilizar un ID externo al conceder acceso a los recursos de AWS a terceros en la Guía del usuario de IAM. Puede recuperar el ARN de la cuenta A sal abrir la consola de IAM.

Buscar un valor de ARN en la cuenta A con la consola de IAM

1. Elija Roles
2. Seleccione el rol que desea examinar.
3. Busque Role ARN en la sección Summary.

La API AssumeRole devuelve credenciales temporales que se utilizan para acceder a los recursos de la cuenta propietaria. En este ejemplo, los recursos a los que quiere acceder son el bucket de Amazon S3 y los archivos de registro que este contiene. Las credenciales provisionales tienen los permisos que definió en la política de acceso del rol.

El ejemplo siguiente con Python (que utiliza AWS SDK for Python (Boto)) muestra cómo llamar a `AssumeRole` y cómo utilizar las credenciales de seguridad provisionales que se devuelven para mostrar todos los buckets de Amazon S3 bajo control de la cuenta A.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
```

```
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

Dejar de compartir archivos de registros de CloudTrail entre cuentas de AWS

A fin de dejar de compartir archivos de registro con otra Cuenta de AWS, tiene que eliminar el rol que creó para esa cuenta. Para obtener información acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia.

Validar la integridad de los archivos de registros de CloudTrail

Para determinar si un archivo de registros se ha modificado, eliminado o continúa igual después del envío de CloudTrail, puede utilizar la validación de la integridad de los archivos de registros de CloudTrail. Esta característica se compila mediante los algoritmos estándar de la industria: SHA-256 para el hash y SHA-256 con RSA para la firma digital. De ese modo, resulta imposible desde el punto

de vista informático modificar, eliminar o falsificar archivos de registros de CloudTrail sin que se sepa. Puede utilizar la AWS CLI para validar los archivos en la ubicación donde los envió CloudTrail.

¿Por qué utilizarla?

Los archivos de registro validados son muy valiosos para las investigaciones de seguridad y forenses. Por ejemplo, un archivo de registro validado le permite afirmar positivamente que el archivo de registro en sí no ha cambiado, o que determinadas credenciales de usuario han realizado una actividad de la API específica. El proceso de validación de la integridad de los archivos de registros de CloudTrail también le permiten saber si un archivo de registros se ha eliminado o cambiado, o confirmar que no se han enviado archivos de registros a su cuenta durante un periodo de tiempo determinado.

Cómo funciona

Al habilitar la validación de la integridad de los archivos de registros, CloudTrail crea un valor hash para cada archivo de registros que envía. Cada hora, CloudTrail también crea y envía un archivo que hace referencia a los archivos de registros de la última hora y contiene un hash de cada uno de ellos. Este archivo se denomina archivo de resumen. CloudTrail firma cada archivo de resumen con la clave privada de un par de claves pública y privada. Después del envío, puede utilizar la clave pública para validar el archivo de resumen. CloudTrail utiliza pares de claves diferentes para cada Región de AWS.

Los archivos de resumen se envían al mismo bucket de Amazon S3 asociado a su registro de seguimiento como sus archivos de registros de CloudTrail. Si los archivos de registros se envían desde todas las regiones o desde varias cuentas a un solo bucket de Amazon S3, CloudTrail enviará los archivos de resumen desde esas regiones y cuentas al mismo bucket.

Los archivos de resumen se colocan en una carpeta independiente de los archivos de registro. Esta separación de archivos de resumen y archivos de registro le permite aplicar las políticas de seguridad detalladas y permite a las soluciones de procesamiento de registros existentes seguir funcionando sin modificaciones. Cada archivo de resumen también contiene la firma digital del archivo de resumen anterior, si existe. La firma del archivo de resumen actual se almacena en las propiedades de los metadatos del objeto de Amazon S3 del archivo de resumen. Para obtener más información sobre el contenido de los archivos de resumen, consulte Estructura de los archivos de resumen de CloudTrail.

Almacenamiento de los archivos de registro y de resumen

Puede almacenar los archivos de registros y de resumen de CloudTrail en Amazon S3 o S3 Glacier de forma segura, duradera y económica durante un periodo de tiempo indefinido. Para mejorar la seguridad de los archivos de resumen almacenados en Amazon S3, puede utilizar Eliminar Amazon S3 MFA.

Activación de la validación y los archivos de validación

Para habilitar la validación de la integridad de los archivos de registros, puede utilizar la AWS Management Console, la AWS CLI o la API de CloudTrail. Activar la validación de la integridad de los archivos de registro permite a CloudTrail entregar archivos de registro de resumen a su bucket de Amazon S3, pero no valida la integridad de los archivos. Para obtener más información, consulte Habilitación de la validación de la integridad de los archivos de registros de CloudTrail.

Para validar la integridad de los archivos de registros de CloudTrail, puede utilizar la AWS CLI o crear su propia solución. La AWS CLI validará archivos en la ubicación donde los ha enviado CloudTrail. Si desea validar los registros que ha movido a otra ubicación, ya sea en Amazon S3 o en algún otro lugar, puede crear sus propias herramientas de validación.

Para obtener información acerca de la validación de los registros con AWS CLI, consulte Validación de la integridad de los archivos de registros de CloudTrail con la AWS CLI. Para obtener más información sobre el desarrollo de las implementaciones personalizadas para la validación de los archivos de registros de CloudTrail, consulte Implementaciones personalizadas de la validación de la integridad de los archivos de CloudTrail registro.

Habilitación de la validación de la integridad de los archivos de registros de CloudTrail

Puede habilitar la validación de la integridad de los archivos de registros mediante la AWS Management Console, la interfaz de línea de comandos (AWS CLI) de AWS o la API de CloudTrail. CloudTrail empieza a enviar archivos de resumen en aproximadamente una hora.

AWS Management Console

Para habilitar la validación de la integridad de los archivos de registros con la consola de CloudTrail, elija Yes (Sí) en la opción Enable log file validation (Habilitar validación de archivos de registros) cuando cree o actualice un registro de seguimiento. De forma predeterminada, este rol está

habilitado en los nuevos registros de seguimiento. Para obtener más información, consulte Creación y actualización de un registro de seguimiento con la consola.

AWS CLI

Para habilitar la validación de la integridad de los archivos de registro con la AWS CLI, utilice la opción `--enable-log-file-validation` con los comandos create-trail o update-trail. Para deshabilitar la validación de la integridad de los archivos de registro, utilice la opción `--no-enable-log-file-validation`.

Ejemplo

El siguiente comando `update-trail` permite la validación de archivos de registros y comienza a enviar archivos de resumen al bucket de Amazon S3 del registro de seguimiento indicado.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

API de CloudTrail

Para habilitar la validación de la integridad de los archivos de registros con la API de CloudTrail, defina el parámetro de la solicitud `EnableLogFileValidation` como `true` cuando llame a `CreateTrail` o `UpdateTrail`.

Para obtener más información, consulte CreateTrail y UpdateTrail en la AWS CloudTrailReferencia de la API.

Validación de la integridad de los archivos de registros de CloudTrail con la AWS CLI

Para validar los registros con la AWS Command Line Interface, utilice el comando `validate-logs` de CloudTrail. Para realizar la validación, el comando utiliza los archivos de resumen enviados a su bucket de Amazon S3. Para obtener más información sobre los archivos de resumen, consulte Estructura de los archivos de resumen de CloudTrail.

La AWS CLI le permite detectar los siguientes tipos de cambios:

- Modificación o eliminación de archivos de registros de CloudTrail
- Modificación o eliminación de archivos de resumen de CloudTrail
- Modificación o eliminación de ambos tipos de archivo

> **Note**
>
> La AWS CLI valida únicamente los archivos de registro a los que hacen referencia los archivos de resumen. Para obtener más información, consulte Verificación del envío de un archivo determinado por parte de CloudTrail.

Requisitos previos

Para validar la integridad de los archivos de registro con la AWS CLI, deben cumplirse las siguientes condiciones:

- Debe disponer de conectividad en línea a AWS.
- Debe disponer de acceso de lectura al bucket de Amazon S3 que contiene los archivos de resumen y de registro.
- Los archivos de registros y de resumen no deben haberse transferido desde la ubicación de Amazon S3 original a donde los envió CloudTrail.

> **Note**
>
> Los archivos de registro descargados al disco local no se pueden validar con la AWS CLI. Para obtener instrucciones sobre cómo crear sus propias herramientas para la validación, consulte Implementaciones personalizadas de la validación de la integridad de los archivos de CloudTrail registro.

validate-logs

Sintaxis

A continuación se presenta la sintaxis de `validate-logs`. Los parámetros opcionales se muestran entre corchetes.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> El comando `validate-logs` es específico de la región. Debe especificar la opción global `--region` para validar los registros de una Región de AWS específica.

Opciones

A continuación se enumeran las opciones de la línea de comandos para `validate-logs`. Las opciones `--trail-arn` y `--start-time` son obligatorias. La opción `--account-id` también es necesaria para los registros de seguimiento organizativos.

`--start-time`

Especifica que se validarán los archivos de registro enviados en o después del valor de la marca temporal de inicio UTC especificada. Ejemplo: `2015-01-08T05:21:42Z`.

`--end-time`

De forma opcional, especifica que se validarán los archivos de registro enviados en o antes del valor de la marca temporal de inicio UTC especificada. El valor predeterminado es la hora UTC actual (`Date.now()`). Ejemplo: `2015-01-08T12:31:41Z`.

> **Note**
>
> Para el intervalo de tiempo especificado, el comando `validate-logs` verifica únicamente los archivos de registros a los que se hace referencia en los archivos de resumen correspondientes. No se verifica ningún otro archivo de registros en el bucket de Amazon S3. Para obtener más información, consulte Verificación del envío de un archivo determinado por parte de CloudTrail.

`--s3-bucket`

De forma opcional, especifica el bucket de Amazon S3 donde se almacenan los archivos de resumen. Si no se especifica un nombre de bucket, la AWS CLI lo recuperará llamando `DescribeTrails()`.

`--s3-prefix`

De forma opcional, especifica el prefijo de Amazon S3 donde se almacenan los archivos de resumen. Si no se especifica, AWS CLI lo recuperará llamando a `DescribeTrails()`.

> **Note**
>
> Debe utilizar esta opción sólo si el prefijo actual es diferente del prefijo en uso durante el intervalo de tiempo especificado.

`--account-id`

También se puede especificar la cuenta para validar los registros. Este parámetro es obligatorio en los registros de seguimiento de la organización para validar los registros de una cuenta específica dentro de una organización.

`--trail-arn`

Especifica el nombre de recurso de Amazon (ARN) del registro de seguimiento a validar. El formato de un ARN de registro de seguimiento es como sigue.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> Para obtener el ARN de un registro de seguimiento, puede utilizar el comando `describe-trails` antes de ejecutar `validate-logs`.
> Se recomienda especificar el nombre del bucket y el prefijo además del ARN del registro de seguimiento si los archivos de registro se han enviado a más de un bucket en el intervalo de tiempo especificado, y si desea restringir la validación a los archivos de registro en tan solo uno de los buckets.

`--verbose`

De forma opcional, emite información de validación para cada archivo de resumen o de registro en el intervalo de tiempo especificado. El resultado indica si el archivo no ha cambiado, se ha

modificado o se ha eliminado. En el modo no detallado (predeterminado), la información se muestra sólo para aquellos casos en los que se ha producido un error de validación.

Ejemplo

En el siguiente ejemplo se validan archivos de registros desde la hora de inicio especificada hasta el momento actual, a través del bucket de Amazon S3 configurado para el registro de seguimiento actual y especificando resultados detallados.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

Cómo funciona **`validate-logs`**

El comando `validate-logs` empieza validando el archivo de resumen más reciente en el intervalo de tiempo especificado. En primer lugar, verifica que el archivo de resumen se haya descargado desde la ubicación a la que dice pertenecer. En otras palabras, si la CLI descarga el archivo de resumen `df1` desde la ubicación de S3 `p1`, validate-logs comprobará que `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`.

Si la firma del archivo de resumen es válida, verifica el valor hash de cada uno de los registros a los que se hace referencia en el archivo de resumen. A continuación, el comando va hacia atrás en el tiempo y valida los archivos de resumen anteriores y sus archivos de registro de referencia sucesivamente. Continúa así hasta llegar al valor especificado para `start-time` o hasta que finalice la cadena de resumen. Si falta un archivo de resumen o no es válido, el intervalo de tiempo que no se puede validar aparecerá en el resultado.

Resultados de la validación

Los resultados de la validación comienzan con un encabezado de resumen con el siguiente formato:

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

Cada línea del resultado principal contiene los resultados de validación de un único archivo de registro o de resumen y con el siguiente formato:

```
<Digest file | Log file> <S3 path> <Validation Message>
```

En la siguiente tabla se describen los posibles mensajes de validación para los archivos de registro y de resumen.

Tipo de archivo	Mensaje de validación	Descripción
Digest file	`valid`	La firma del archivo de resumen es válida. También se pueden verificar los archivos de registro a los que hace referencia. Este mensaje se incluirá solo en el modo detallado.
Digest file	`INVALID: has been moved from its original location`	El bucket o el objeto de S3 desde el que se ha tomado el archivo de resumen no coincide con las ubicaciones del bucket o el objeto de S3 registradas en el propio archivo de resumen.
Digest file	`INVALID: invalid format`	El formato del archivo de resumen no es válido. Los archivos de registro correspon dientes al intervalo de tiempo que represent a el archivo de resumen no se pueden validar.
Digest file	`INVALID: not found`	No se ha encontrado el archivo de resumen. Los archivos de registro correspondientes al intervalo de tiempo que representa el archivo de resumen no se pueden validar.
Digest file	`INVALID: public key not found for fingerprint` *`Huella digital`*	No se ha encontrado la clave pública correspondiente a la huella digital registrad a en el archivo de resumen. El archivo de resumen no se puede validar.
Digest file	`INVALID: signature verification failed`	La firma del archivo de resumen no es válida. Dado que el archivo de resumen no es válido, los archivos de registro a los que hace referencia no se pueden validar y

Tipo de archivo	Mensaje de validación	Descripción
		no se pueden hacer afirmaciones sobre la actividad de la API en dichos archivos.
`Digest file`	`INVALID: Unable to load PKCS #1 key with fingerprint` *`Huella digital`*	Dado que no se ha podido cargar la clave pública codificada DER en formato PKCS #1 que contiene la huella digital especific ada, no se ha podido validar el archivo de resumen.
`Log file`	`valid`	El archivo de registro se ha validado y no se ha modificado desde el momento del envío. Este mensaje se incluirá solo en el modo detallado.
`Log file`	`INVALID: hash value doesn't match`	El hash para el archivo de registro no coincide. El archivo de registros se ha modificado después del envío de CloudTrail.
`Log file`	`INVALID: invalid format`	El formato del archivo de registro no es válido. El archivo de registro no se puede validar.
`Log file`	`INVALID: not found`	No se ha encontrado el archivo de registro y no se puede validar.

La salida incluye información resumida sobre los resultados emitidos.

Ejemplos de resultados

Detallado

El siguiente comando `validate-logs` de ejemplo, usa el indicador `--verbose` y produce la salida de ejemplo que se indica a continuación. `[...]` indica que la salida de muestra se ha abreviado.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

No detallado

El siguiente comando `validate-logs` de ejemplo no utiliza el indicador `--verbose`. En el resultado de ejemplo que sigue ha surgido un error. Solo devuelve la información del encabezado, de error y de resumen.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

Verificación del envío de un archivo determinado por parte de CloudTrail

Para verificar si CloudTrail ha enviado un archivo determinado a su bucket, ejecute `validate-logs` en el modo detallado para el periodo de tiempo que incluye el archivo. Si el archivo aparece en el resultado de `validate-logs`, significa que CloudTrail lo ha enviado.

Estructura de los archivos de resumen de CloudTrail

Cada archivo de resumen contiene los nombres de los archivos de registros que se enviaron al bucket de Amazon S3 durante la última hora, los valores hash de esos archivos de registros y la firma digital del archivo de resumen anterior. La firma del archivo de resumen actual se almacena en las propiedades de los metadatos del objeto de archivo de resumen. Las firmas digitales y los valores hash se utilizan para validar la integridad de los archivos de registro y del archivo de resumen en sí.

Ubicación del archivo de resumen

Los archivos de resumen se envían a una ubicación de bucket de Amazon S3 con la siguiente sintaxis.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> Para los registros de seguimiento de organización, la ubicación del bucket también incluye el ID de la unidad organizativa, tal y como se indica a continuación:
>
> ```
> s3://s3-bucket-name/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

Contenido del archivo de resumen de ejemplo

El siguiente ejemplo de archivo de resumen contiene información de un registro de CloudTrail.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
```

```
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```

Descripciones de los campos de los archivos de resumen

A continuación de describe cada campo del archivo de resumen:

`awsAccountId`

El ID de la cuenta de AWS para que el que se ha enviado el archivo de resumen.

`digestStartTime`

El intervalo de tiempo UTC inicial que cubre el archivo de resumen, donde se toma como referencia la hora en que CloudTrail envió los archivos de registros. Esto significa que, si el intervalo de tiempo es [Ta, Tb], el resumen contendrá todos los archivos de registro que se enviaron al cliente entre Ta y Tb.

`digestEndTime`

El intervalo de tiempo UTC final que cubre el archivo de resumen, donde se toma como referencia la hora en que CloudTrail envió los archivos de registros. Esto significa que, si el intervalo de tiempo es [Ta, Tb], el resumen contendrá todos los archivos de registro que se enviaron al cliente entre Ta y Tb.

`digestS3Bucket`

El nombre del bucket de Amazon S3 donde se envió el archivo de resumen actual.

`digestS3Object`

La clave de objeto de Amazon S3 (es decir, la ubicación del bucket de Amazon S3) del archivo de resumen actual. Las dos primeras regiones en la cadena muestran la región desde la que se ha enviado el archivo de resumen. La última región (después de `your-trail-name`) es la región principal del registro de seguimiento. La región principal es la región en la que se creó el archivo de seguimiento. Cuando el archivo de seguimiento se refiere a múltiples regiones, esta puede diferir de la región desde la que se envió el archivo de resumen.

`newestEventTime`

La hora UTC del evento más reciente de todos los eventos en los archivos de registro del resumen.

`oldestEventTime`

La hora UTC del evento más antiguo de todos los eventos en los archivos de registro del resumen.

> **Note**
>
> Si el archivo de resumen se envía tarde, el valor de `oldestEventTime` será anterior al valor de `digestStartTime`.

`previousDigestS3Bucket`

El bucket de Amazon S3 donde se envió el archivo de resumen anterior.

`previousDigestS3Object`

La clave de objeto de Amazon S3 (es decir, la ubicación del bucket de Amazon S3) del archivo de resumen anterior.

`previousDigestHashValue`

El valor de hash codificado hexadecimal de los contenidos sin comprimir del archivo de resumen anterior.

`previousDigestHashAlgorithm`

El nombre del algoritmo hash que se utilizó para resumir el archivo de resumen anterior.

`publicKeyFingerprint`

La huella digital codificada hexadecimal de la clave pública que coincide con la clave privada utilizada para firmar este archivo de resumen. Puede recuperar las claves públicas del intervalo de tiempo correspondiente para el archivo de resumen mediante la AWS CLI o la API de CloudTrail. De las claves públicas que se devuelven, se podrá utilizar para validar el archivo de resumen aquella cuya huella digital coincida con este valor. Para obtener información sobre cómo recuperar claves públicas para archivos de resumen, consulte el comando `list-public-keys` de la AWS CLI o la API `ListPublicKeys` de CloudTrail.

> **Note**
>
> CloudTrail utiliza diferentes pares de claves públicas y privadas por región. Cada archivo de resumen se firma con una clave privada única para su región. Por tanto, al validar un archivo de resumen proveniente de una región determinada, será preciso que busque en esa misma región la clave pública correspondiente.

`digestSignatureAlgorithm`

El algoritmo que se utiliza para firmar el archivo de resumen.

`logFiles.s3Bucket`

El nombre del bucket de Amazon S3 para el archivo de registros.

`logFiles.s3Object`

La clave de objeto de Amazon S3 del archivo de registros actual.

`logFiles.newestEventTime`

La hora UTC del evento más reciente en el archivo de registro. Este momento también se corresponde con la marca temporal del propio archivo de registro.

`logFiles.oldestEventTime`

La hora UTC del evento más antiguo en el archivo de registro.

`logFiles.hashValue`

El valor hash codificado hexadecimal del contenido del archivo de registro sin comprimir.

`logFiles.hashAlgorithm`

El algoritmo hash que se utiliza para el archivo de registro.

Archivo de resumen de inicio

Cuando se empieza a validar la integridad del archivo de registro, se genera un archivo de resumen de inicio. También se genera un archivo de resumen de inicio cuando se reinicia la validación de la integridad del archivo de registro (para ello se deshabilita y, después, se vuelve a habilitar la validación de la integridad del archivo, o bien, se detiene el registro y, más adelante, este se reinicia con la validación habilitada). En un archivo de resumen de inicio, los siguientes campos relativos al archivo de resumen anterior tendrán un valor NULL:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

Archivos de resumen “vacíos”

CloudTrail enviará un archivo de resumen incluso cuando no hubiera habido actividad de la API en su cuenta durante el periodo de una hora que representa el archivo de resumen. Esto puede resultar

útil cuando necesite confirmar que no se enviaron archivos de registro durante la hora de la que informa el archivo de resumen.

El ejemplo siguiente muestra el contenido de un archivo de resumen correspondiente a una hora en la que no hubo actividad en la API. Tenga en cuenta que el campo `logFiles:[ ]` al final del contenido del archivo de resumen está vacío.


```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```


Firma del archivo de resumen

La información de la firma de un archivo de resumen se encuentra en dos propiedades de los metadatos del objeto del archivo de resumen de Amazon S3. Cada archivo de resumen presenta las siguientes entradas de metadatos:

- `x-amz-meta-signature`

  El valor codificado hexadecimal de la firma del archivo de resumen. A continuación se muestra un ejemplo de firma:

```
3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
```

- `x-amz-meta-signature-algorithm`

  A continuación se muestra un ejemplo de valor del algoritmo que se utilizó para generar la firma del resumen:

  `SHA256withRSA`

Encadenado de archivos de resumen

Dado que cada archivo de resumen contiene una referencia al archivo de resumen anterior, es posible "encadenar"; esto permite utilizar herramientas de validación, como la AWS CLI, para detectar si se ha eliminado un archivo de resumen. También hace posible que los archivos de resumen en un intervalo de tiempo determinado se puedan inspeccionar sucesivamente; se empieza por el más reciente.

> **Note**
>
> Cuando se deshabilita la validación de la integridad de los archivos de registro, la cadena de archivos de resumen se rompe después de una hora. CloudTrail no crea archivos de resumen para archivos de registro que se enviaron durante un periodo en el que no estaba habilitada la validación de la integridad de los archivos de registro. Por ejemplo, si habilita la validación de la integridad de los archivos de registro a las 12:00 del medio día del 1 de enero, la deshabilita el 2 enero a la misma hora y la vuelve a habilitar el 10 de enero, también a la misma hora, no se crearán archivos de resumen para los archivos de registro enviados desde las 12 del medio día del 2 de enero hasta el 10 de enero a la misma hora. Lo mismo sucede cuando se detiene el registro de CloudTrail o se elimina un registro de seguimiento.

Si se detiene la operación de registro o se elimina el registro de seguimiento, CloudTrail enviará un archivo de resumen final. Este archivo de resumen puede contener información sobre los archivos de registro restantes que cubren eventos hasta el evento `StopLogging`, e inclusive.

Implementaciones personalizadas de la validación de la integridad de los archivos de CloudTrail registro

Como CloudTrail utiliza algoritmos criptográficos y funciones de hash estándares del sector y disponibles de forma abierta, puede crear sus propias herramientas para validar la integridad de los archivos de CloudTrail registro. Cuando la validación de integridad de los archivos de registro está habilitada, CloudTrail envía los archivos de resumen a su bucket de Amazon S3. Puede utilizar estos archivos para implementar su propia solución de validación. Para obtener más información sobre los archivos de resumen, consulte Estructura de los archivos de resumen de CloudTrail.

En este tema se describe cómo se firman los archivos de resumen. A continuación, se detallan los pasos que debe seguir para implementar una solución que valide los archivos de resumen y los archivos de registro a los que hacen referencia.

Comprenda cómo se firman los archivos de CloudTrail resumen

CloudTrail los archivos de resumen se firman con firmas digitales RSA. Para cada archivo de resumen, CloudTrail hace lo siguiente:

1. Crea una cadena para firmar datos en función de campos del archivo de resumen designados (que se describen en la sección siguiente).
2. Obtiene una clave privada única para la región.
3. Pasa el hash SHA-256 de la cadena y la clave privada al algoritmo de firma RSA, que produce una firma digital.
4. Codifica el código de bytes de la firma en formato hexadecimal.
5. Coloca la firma digital en la propiedad de metadatos `x-amz-meta-signature` del objeto del archivo de resumen de Amazon S3.

Contenido de la cadena de firma de datos

Los siguientes CloudTrail objetos se incluyen en la cadena para la firma de datos:

- La marca de tiempo de finalización del archivo de resumen en formato extendido UTC (por ejemplo, `2015-05-08T07:19:37Z`)
- La ruta S3 del archivo de resumen actual
- El hash SHA-256 en codificación hexadecimal del archivo de resumen actual

- La firma en codificación hexadecimal del archivo de resumen anterior

Más adelante en este documento se proporciona el formato de cálculo de esta cadena y una cadena de ejemplo.

Pasos de implementación de la validación personalizada

Cuando implemente una solución de validación personalizada, deberá validar en primer lugar el archivo de resumen y, a continuación, los archivos de registro a los que hace referencia.

Validar el archivo de resumen

Para validar un archivo de resumen, necesita su firma, la clave pública cuya clave privada se ha utilizado para firmarlo y una cadena de firma de datos que debe calcular.

1. Obtenga el archivo de resumen.
2. Compruebe que el archivo de resumen se haya recuperado de su ubicación original.
3. Obtenga la firma en codificación hexadecimal del archivo de resumen.
4. Obtenga la huella en codificación hexadecimal de la clave pública cuya clave privada se ha utilizado para firmar el archivo de resumen.
5. Recupere las claves públicas para el intervalo de tiempo correspondiente al archivo de resumen.
6. De entre las claves públicas recuperadas, elija la clave pública cuya huella coincida con la del archivo de resumen.
7. Con el hash y otros campos del archivo de resumen, vuelva a crear la cadena de firma que se utiliza para verificar la firma de dicho archivo.
8. Valide la firma pasando el hash SHA-256 de la cadena, la clave pública y la firma como parámetros al algoritmo de verificación de firmas RSA. Si el resultado es verdadero, el archivo de resumen es válido.

Validar los archivos de registros

Si el archivo de resumen es válido, valide cada uno de los archivos de registro a los que hace referencia.

1. Para validar la integridad de un archivo de registro, calcule su valor de hash SHA-256 en su contenido sin comprimir y compare los resultados con el hash del archivo de registro (registrado en formato hexadecimal) en el resumen. Si los hash coinciden, el archivo de registro es válido.

2. Sírvase de la información del archivo de resumen anterior que se incluye en el archivo de resumen actual para validar los archivos de resumen anteriores y sus correspondientes archivos de registro de manera sucesiva.

En las siguientes secciones se describen estos pasos de manera detallada.

A. Obtener el archivo de resumen

Los primeros pasos sirven para obtener el archivo de resumen más reciente, verificar que lo ha recuperado de la ubicación original, verificar su firma digital y obtener la huella de la clave pública.

1. Utilice `S3 Get` o la clase AmazonS3Client (por ejemplo) para obtener el archivo de resumen más reciente de su bucket de Amazon S3 para el intervalo de tiempo que desee validar.
2. Verifique que el bucket de S3 y el objeto de S3 utilizados para recuperar el archivo coinciden con las ubicaciones del objeto S3 y el bucket de S3 registradas en el propio archivo de resumen.
3. A continuación, obtenga la firma digital del archivo de resumen desde la propiedad de metadatos `x-amz-meta-signature` del objeto del archivo de resumen en Amazon S3.
4. En el archivo de resumen, obtenga la huella de la clave pública cuya clave privada se ha utilizado para firmar el archivo de resumen en el campo `digestPublicKeyFingerprint`.

B. Recuperar la clave pública para validar el archivo de resumen

Para obtener la clave pública que valide el archivo de resumen, puedes usar la API AWS CLI o la CloudTrail API. En ambos casos, debe especificar un intervalo de tiempo (es decir, una hora de inicio y una de finalización) para los archivos de resumen que desea validar. Se podrían devolver una o varias claves públicas para el intervalo de tiempo que se especifique. Las claves devueltas pueden tener intervalos de tiempo de validez que se solapan.

> **Note**
>
> Como CloudTrail utiliza diferentes pares de claves públicas y privadas por región, cada archivo de resumen se firma con una clave privada exclusiva de su región. Por lo tanto, al validar un archivo de resumen desde una región determinada, debe recuperar su clave pública desde la misma región.

Utilizar la AWS CLI para recuperar claves públicas

A fin de recuperar las claves públicas para los archivos de resumen mediante la AWS CLI, utilice el comando `cloudtrail list-public-keys`. El comando tiene el siguiente formato:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

Los parámetros de la hora de inicio y de finalización son marcas de tiempo UTC (opcionales). Si no se especifica, se utiliza la hora actual y se devuelven las claves públicas que actualmente están activas.

Respuesta de ejemplo

La respuesta será una lista de objetos JSON que representan las claves devueltas:


```
{
    "publicKeyList": [
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
```

```
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

Utilice la CloudTrail API para recuperar las claves públicas

Para recuperar las claves públicas de los archivos de resumen mediante la CloudTrail API, transfiere los valores de la hora de inicio y finalización a la `ListPublicKeys` API. La API `ListPublicKeys` devuelve las claves públicas cuyas claves privadas se han utilizado para firmar archivos de resumen en el intervalo de tiempo especificado. Para cada clave pública, la API también devuelve la huella correspondiente.

`ListPublicKeys`

En esta sección se describen los parámetros de solicitud y los elementos de respuesta de la API `ListPublicKeys`.

> **Note**
>
> La codificación de los campos binarios de `ListPublicKeys` está sujeta a cambios.

Parámetros de solicitud

Name	Descripción
`StartTime`	Si lo desea, especifica, en UTC, el inicio del intervalo de tiempo para buscar las claves públicas de los archivos de CloudTrail resumen. Si no StartTime se especifica, se utiliza la hora actual y se devuelve la clave pública actual. Tipo: DateTime
`EndTime`	Si lo desea, especifica, en UTC, el final del intervalo de tiempo para buscar las claves públicas de los archivos de CloudTrail resumen. Si no EndTime se especifica, se utiliza la hora actual.

Name	Descripción
	Tipo: DateTime

Elementos de respuesta

`PublicKeyList`, una matriz de objetos `PublicKey` que contiene:

Nombre	Descripción
`Value`	El valor de clave pública codificado de DER en formato PKCS # 1. Tipo: Blob
`ValidityStartTime`	La hora de inicio de la validez de la clave pública. Tipo: DateTime
`ValidityEndTime`	La hora de finalización de la validez de la clave pública. Tipo: DateTime
`Fingerprint`	La huella de la clave pública. La huella puede utilizarse para identificar la clave pública que debe usar para validar el archivo de resumen. Tipo: cadena

C. Elegir la clave pública que va a utilizar para la validación

De entre las claves públicas recuperadas por `list-public-keys` o `ListPublicKeys`, elija la clave pública devuelta cuya huella coincida con la registrada en el campo `digestPublicKeyFingerprint` del archivo de resumen. Esta es la clave pública que utilizará para validar el archivo de resumen.

D. Volver a crear la cadena de la firma de datos

Ahora que ya tiene la firma del archivo de resumen y la clave pública asociada, debe calcular la cadena de firma de datos. Después de haber calculado la cadena de la firma de datos, tendrá las entradas necesarias para verificar la firma.

La cadena de firma de datos tiene el siguiente formato:

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

Este es un ejemplo de `Data_To_Sign_String`.

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

Después de volver a crear esta cadena, puede validar el archivo de resumen.

E. Validar el archivo de resumen

Pase el hash SHA-256 de la cadena de firma de datos recreada, la firma digital y la clave pública al algoritmo de verificación de la firma RSA. Si el resultado es verdadero, la firma del archivo de resumen se verifica y el archivo de resumen es válido.

F. Validar los archivos de registros

Una vez que haya validado el archivo de resumen, puede validar los archivos de registro a los que hace referencia. El archivo de resumen contiene hashes SHA-256 de los archivos de registro. Si uno de los archivos de registro se modificó después de CloudTrail entregarlo, los hashes del SHA-256 cambiarán y la firma del archivo de resumen no coincidirá.

A continuación se muestra cómo validar los archivos de registro:

1. Realice una operación `S3 Get` para el archivo de registro utilizando la información de la ubicación de S3 en los campos `logFiles.s3Bucket` y `logFiles.s3Object` del archivo de resumen.
2. Si la operación `S3 Get` se realiza correctamente, itérela en los archivos de registro que se encuentran en la matriz logFiles del archivo de resumen mediante los siguientes pasos:

a. Recupere el hash original del archivo desde el campo `logFiles.hashValue` del registro correspondiente en el archivo de resumen.
b. Convierta en hash el contenido sin comprimir del archivo de registro con el algoritmo de hash especificado en `logFiles.hashAlgorithm`.
c. Compare el valor de hash que ha generado con el valor para el registro en el archivo de resumen. Si los hash coinciden, el archivo de registro es válido.

G. Validar los archivos de registros y de resumen adicionales

En cada archivo de resumen, los siguientes campos proporcionan la ubicación y la firma del archivo de resumen anterior:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

Utilice esta información para visitar archivos de resumen anteriores de forma secuencial. Para ello, valide la firma de cada archivo de resumen y de los archivos de registro a los que hacen referencia mediante los pasos que se indican en las secciones anteriores. La única diferencia es que, para los archivos de resumen anteriores, no es necesario recuperar la firma digital de las propiedades de los metadatos de Amazon S3 del objeto del archivo de resumen. La firma del archivo de resumen anterior se proporciona automáticamente en el campo `previousDigestSignature`.

Puede retroceder hasta llegar al archivo de resumen de partida o hasta que la cadena de archivos de resumen se rompa, lo que ocurra primero.

Validación de archivos de registros y de resumen sin conexión

Cuando valida archivos de registro y de resumen sin conexión, generalmente puede seguir los procedimientos descritos en las secciones anteriores. No obstante, debe tener en cuenta lo siguiente:

Uso del archivo de resumen más reciente

La firma digital del archivo de resumen más reciente (es decir, “actual”) se encuentra en las propiedades de metadatos de Amazon S3 del objeto del archivo de resumen. En una situación sin conexión, la firma digital del archivo de resumen actual no estará disponible.

Hay dos maneras posibles de abordar esta situación:

- Como la firma digital del archivo de resumen anterior se encuentra en el archivo de resumen actual, comience a validar desde el archivo de resumen. next-to-last Con este método, el archivo de resumen más reciente no se puede validar.
- Como primer paso, obtenga la firma del archivo de resumen actual de las propiedades de metadatos del objeto del archivo de resumen y, a continuación, guárdelo de forma segura sin conexión. Esto permite que el archivo de resumen actual se valide junto con los archivos anteriores de la cadena.

Resolución de la ruta de acceso

Los campos de los archivos de resumen descargados, como `s3object` y `previousDigestS3object`, seguirán apuntando a ubicaciones de Amazon S3 en línea para archivos de registros y archivos de resumen. Las soluciones sin conexión deben encontrar una forma de volverlos a direccionar a la ruta actual de los archivos de registro y de resumen descargados.

Claves públicas

Para realizar la validación sin conexión, primero se deben obtener en línea todas las claves públicas que necesita para validar los archivos de registro en un intervalo de tiempo determinado (llamando a `ListPublicKeys`, por ejemplo) y, a continuación, guardarlos de forma segura sin conexión. Este paso debe repetirse siempre que desee validar más archivos fuera del intervalo de tiempo inicial especificado.

Fragmento de código de validación de ejemplo

El siguiente fragmento de ejemplo proporciona un código básico para validar los archivos de CloudTrail resumen y registro. El código básico no depende del estado en línea o sin conexión; es decir, el usuario es quien debe decidir si lo implementará en línea o sin conexión a AWS. La implementación sugerida utiliza Java Cryptography Extension (JCE) y Bouncy Castle como proveedor de seguridad.

En el fragmento de código de ejemplo, se muestra lo siguiente:

- Cómo crear la cadena de firma de datos que se utiliza para validar la firma de archivos de resumen.
- Cómo verificar la firma de archivos de resumen.
- Cómo verificar los valores hash del archivo de registro.
- Una estructura de código para validar una cadena de archivos de resumen.

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
 digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
 as part of the data to sign
```

```
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:

                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
```

```
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
                    messageDigest.update(logFileContent);
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
```

```
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

Uso de la biblioteca de procesamiento de CloudTrail

La biblioteca de procesamiento de CloudTrail es una biblioteca Java que ofrece una forma sencilla de procesar los registros de AWS CloudTrail. Proporcione los detalles de configuración de la cola de SQS de CloudTrail y escriba código para procesar eventos. La biblioteca de procesamiento de CloudTrail se ocupa del resto. Sondea la cola de Amazon SQS, lee y analiza los mensajes de la cola, descarga archivos de registro de CloudTrail, analiza los eventos de los archivos de registros y pasa los eventos a su código como objetos Java.

La biblioteca de procesamiento de CloudTrail es altamente escalable y tolerante a errores. Se ocupa del procesamiento paralelo de archivos de registro, de modo que pueden procesarse tantos registros como sea necesario. Gestiona los errores de red relacionados con tiempos de espera y recursos inaccesibles.

El siguiente tema muestra cómo utilizar la biblioteca de procesamiento de CloudTrail para procesar registros de CloudTrail en los proyectos Java.

La biblioteca se suministra como un proyecto de código abierto con licencia de Apache y está disponible en GitHub: https://github.com/aws/aws-cloudtrail-processing-library. El código fuente de la biblioteca incluye código de muestra, que puede utilizar como base para sus propios proyectos.

Temas

- Requisitos mínimos
- Procesamiento de registros de CloudTrail
- Temas avanzados
- Recursos adicionales

Requisitos mínimos

Para utilizar la biblioteca de procesamiento de CloudTrail, debe disponer de lo siguiente:

- AWS SDK for Java 1,11.830
- Java 1,8 (Java SE 8)

Procesamiento de registros de CloudTrail

Procesar registros de CloudTrail en la aplicación de Java:

1. Agregar la biblioteca de procesamiento de CloudTrail al proyecto
2. Configuración de la biblioteca de procesamiento de CloudTrail
3. Implementación del procesador de eventos
4. Invocación y ejecución del ejecutor de procesos

Agregar la biblioteca de procesamiento de CloudTrail al proyecto

Para utilizar la biblioteca de procesamiento de CloudTrail, debe agregarla a la variable classpath del proyecto de Java.

Contenido

- Agregar la biblioteca a un proyecto Apache Ant
- Agregar la biblioteca a un proyecto Apache Maven
- Agregar la biblioteca a un proyecto Eclipse
- Agregar la biblioteca a un proyecto IntelliJ

Agregar la biblioteca a un proyecto Apache Ant

Agregar la biblioteca de procesamiento de CloudTrail a un proyecto Apache Ant

1. Descargue o clone el código fuente de la biblioteca de procesamiento de CloudTrail desde GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Cree el archivo .jar desde la fuente tal y como se describe en README (LÉAME):

```
mvn clean install -Dgpg.skip=true
```

3. Copie el archivo resultante .jar en el proyecto y añádalo al archivo `build.xml` del proyecto. Por ejemplo:

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

Agregar la biblioteca a un proyecto Apache Maven

La biblioteca de procesamiento de CloudTrail está disponible para Apache Maven. Puede añadirla a su proyecto escribiendo una única dependencia en su archivo `pom.xml` de proyectos.

Agregar la biblioteca de procesamiento de CloudTrail a un proyecto Maven

- Abra su archivo `pom.xml` de proyecto Maven y añada la siguiente dependencia:

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

Agregar la biblioteca a un proyecto Eclipse

Agregar la biblioteca de procesamiento de CloudTrail a un proyecto Eclipse

1. Descargue o clone el código fuente de la biblioteca de procesamiento de CloudTrail desde GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Cree el archivo .jar desde la fuente tal y como se describe en README (LÉAME):

```
mvn clean install -Dgpg.skip=true
```

3. Copie el archivo compilado aws-cloudtrail-processing-library-1.6.1.jar en un directorio del proyecto (por lo general, `lib`).
4. Haga clic con el nombre de su proyecto Project Explorer de Eclipse, elija Build Path y, a continuación, elija Configure
5. En la ventana Java Build Path, elija la pestaña Libraries.
6. Seleccione Agregar archivos JAR… y vaya a la ruta donde copió aws-cloudtrail-processing-library-1.6.1.jar.
7. Elija OK para completar la adición de la `.jar` a su proyecto.

Agregar la biblioteca a un proyecto IntelliJ

Agregar la biblioteca de procesamiento de CloudTrail a un proyecto IntelliJ

1. Descargue o clone el código fuente de la biblioteca de procesamiento de CloudTrail desde GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Cree el archivo .jar desde la fuente tal y como se describe en README (LÉAME):

```
mvn clean install -Dgpg.skip=true
```

3. En File, seleccione Project Structure.
4. Elija Modules y, a continuación, elija Dependencies.
5. Elija + JARS or Directories (+ JARS o directorios) y, a continuación, vaya a la ruta en la que hubiera creado el `aws-cloudtrail-processing-library-1.6.1.jar`.
6. Elija Apply y, a continuación, elija OK para completar la adición de la `.jar` a su proyecto.

Configuración de la biblioteca de procesamiento de CloudTrail

Puede configurar la biblioteca de procesamiento de CloudTrail al crear un archivo de propiedades de classpath que se cargará en el tiempo de ejecución o mediante la creación de un objeto `ClientConfiguration` y al establecer las opciones de configuración de forma manual.

Proporcionar un archivo de propiedades

Puede escribir un archivo de propiedades classpath que proporcione las opciones de configuración para la aplicación. El siguiente ejemplo muestra el archivo de opciones que puede definir:

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

Se requieren los siguientes parámetros:

- `sqsUrl`: proporciona la URL para extraer las notificaciones de CloudTrail. Si no especifica este valor, `AWSCloudTrailProcessingExecutor` toma una `IllegalStateException`.

- `accessKey`: un identificador único para la cuenta, como AKIAIOSFODNN7EXAMPLE.
- `secretKey`: un identificador único para la cuenta, como wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

Los parámetros `accessKey` y `secretKey` proporcionan sus credenciales de AWS a la biblioteca, para que esta pueda obtener acceso a AWS en su nombre.

Los valores predeterminados del resto de parámetros los establece la biblioteca. Para obtener más información, consulte la Referencia de la biblioteca de procesamiento de AWS CloudTrail.

Creación de una ClientConfiguration

En lugar de establecer opciones a través de las propiedades de classpath, puede proporcionar opciones para `AWSCloudTrailProcessingExecutor` inicializando y definiendo opciones en un objeto `ClientConfiguration`, como se muestra en el ejemplo siguiente:

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

Implementación del procesador de eventos

Para procesar los registros de CloudTrail, debe implementar un `EventsProcessor` que reciba los datos del registro de CloudTrail. A continuación se muestra una implementación de ejemplo:

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

Cuando se implementa un `EventsProcessor`, debe poner en práctica la devolución de llamada `process()` que `AWSCloudTrailProcessingExecutor` utiliza para enviarle eventos de CloudTrail. Los eventos se suministran en una lista de objetos `CloudTrailClientEvent`.

El objeto `CloudTrailClientEvent` proporciona un `CloudTrailEvent` y `CloudTrailEventMetadata` que puede utilizar para leer el evento de CloudTrail y enviar información.

Este sencillo ejemplo imprime la información de eventos para todos los eventos pasados a `SampleEventsProcessor`. En su propia implementación, puede procesar registros según estime más conveniente. `AWSCloudTrailProcessingExecutor` sigue enviando eventos a su `EventsProcessor` siempre que tenga eventos que enviar y se siga ejecutando.

Invocación y ejecución del ejecutor de procesos

Después de escribir un `EventsProcessor` y establecer los valores de configuración para la biblioteca de procesamiento de CloudTrail (ya sea en un archivo de propiedades o mediante el uso de la clase `ClientConfiguration`), puede utilizar estos elementos a fin de iniciar y utilizar un `AWSCloudTrailProcessingExecutor`.

Utilizar **`AWSCloudTrailProcessingExecutor`** para procesar eventos de CloudTrail

1. Cree una instancia para el objeto `AWSCloudTrailProcessingExecutor.Builder`. El constructor de `Builder` toma un objeto `EventsProcessor` y un nombre de archivo de propiedades de classpath.
2. Llame al método predeterminado `build()` de `Builder` para configurar y obtener un objeto `AWSCloudTrailProcessingExecutor`.
3. Utilice los métodos `start()` y `stop()` de `AWSCloudTrailProcessingExecutor` para comenzar y finalizar el procesamiento de eventos de CloudTrail.

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
```

```
  }
}
```

Temas avanzados

Temas

- Filtrado de los eventos que se van a procesar
- Procesamiento de eventos de datos
- Notificación del progreso
- Gestión de errores

Filtrado de los eventos que se van a procesar

De forma predeterminada, todos los registros del bucket de S3 de la cola de Amazon SQS y todos los eventos que contienen se envían al `EventsProcessor`. La biblioteca de procesamiento de CloudTrail proporciona interfaces opcionales que puede implementar a fin de filtrar las fuentes que se utilizan para obtener registros de CloudTrail y filtrar los eventos que le interesa procesar.

`SourceFilter`

Puede implementar la interfaz `SourceFilter` para elegir si procesa o no los registros desde un origen que se haya proporcionado. `SourceFilter` declara un método único de devolución de llamada, `filterSource()`, que recibe un objeto `CloudTrailSource`. Para evitar procesar eventos desde un origen, devuelve `false` desde `filterSource()`.

La biblioteca de procesamiento de CloudTrail llama al método `filterSource()` después de que esta sondea si hay registros en la cola de Amazon SQS. Esto ocurre antes de que la biblioteca comience el filtrado de eventos o el procesamiento de los registros.

A continuación se muestra una implementación de ejemplo:

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
```

```
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

Si no proporciona su propio `SourceFilter`, en ese caso se utilizará `DefaultSourceFilter`, lo que permite procesar todos los orígenes (siempre devuelve `true`).

`EventFilter`

Puede implementar la interfaz `EventFilter` para elegir si un evento de CloudTrail se envía al `EventsProcessor`. `EventFilter` declara un método único de devolución de llamada, `filterEvent()`, que recibe un objeto `CloudTrailEvent`. Para evitar que se procese el evento, devuelve `false` desde `filterEvent()`.

La biblioteca de procesamiento de CloudTrail llama al método `filterEvent()` después de que la biblioteca sondea si hay registros en la cola Amazon SQS y después del filtrado de la fuente. Esto ocurre antes de que la biblioteca comience el procesamiento de eventos de los registros.

Consulte la siguiente implementación de ejemplo:

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
```

```
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

Si no proporciona su propio `EventFilter`, en ese caso se utilizará `DefaultEventFilter`, lo que permite procesar todos los eventos (siempre devuelve `true`).

Procesamiento de eventos de datos

Cuando CloudTrail procesa eventos de datos, conserva los números en su formato original, ya sea un entero (`int`) o un `float` (un número que contiene un decimal). En eventos que tienen enteros en los campos de un evento de datos, CloudTrail ha procesado históricamente estos números como flotantes. Actualmente, CloudTrail procesa números en estos campos y mantiene su formato original.

Como práctica recomendada, con el fin de evitar la interrupción de las automatizaciones, sea flexible en cualquier código o automatización que utilice para procesar o filtrar eventos de datos de CloudTrail y permita números `int` y `float`. Para obtener los mejores resultados, utilice la versión 1.4.0 o posterior de la biblioteca de procesamiento de CloudTrail.

En el siguiente fragmento de ejemplo se muestra un número `float`, `2.0`, para el parámetro `desiredCount` en el bloque `ResponseParameters` de un evento de datos.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

En el siguiente fragmento de ejemplo se muestra un número `int`, 2, para el parámetro `desiredCount` en el bloque `ResponseParameters` de un evento de datos.

```
"eventName": "CreateService",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

Notificación del progreso

Implemente la interfaz `ProgressReporter` para personalizar los informes de progreso de la biblioteca de procesamiento de CloudTrail. `ProgressReporter` declara dos métodos: `reportStart()` y `reportEnd()`, a los que se llama al principio y al final de las siguientes operaciones:

- Sondeo de mensajes desde Amazon SQS
- Análisis de mensajes desde Amazon SQS
- Procesamiento de una fuente de Amazon SQS para registros de CloudTrail
- Eliminación de mensajes desde Amazon SQS
- Descarga de un archivo de registros de CloudTrail
- Procesamiento del archivo de registros de CloudTrail

Ambos métodos reciben un objeto `ProgressStatus` que contiene información sobre la operación realizada. El miembro `progressState` es miembro de la enumeración `ProgressState` que identifica la operación actual. Este miembro puede contener información adicional en el miembro `progressInfo`. Por otra parte, cualquier objeto que se devuelva desde `reportStart()` se pasa a `reportEnd()`, de forma que podrá proporcionar información contextualizada como, por ejemplo, el momento en que se comenzó a procesar el evento.

A continuación viene una implementación de ejemplo que proporciona información sobre cuánto tiempo tarda una operación en completarse:

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
```

```
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

Si no implementa su propio `ProgressReporter`, en ese caso se sustituirá por `DefaultExceptionHandler`, que imprime el nombre del estado que se esté ejecutando.

Gestión de errores

Con la interfaz `ExceptionHandler` puede controlar de forma especial las excepciones que se produzcan durante el procesamiento de los registros. `ExceptionHandler` declara un método único de devolución de llamada, `handleException()`, que recibe un objeto `ProcessingLibraryException` con contexto sobre la excepción que se ha producido.

Puede utilizar el método `ProcessingLibraryException` de `getStatus()` transferido para saber qué operación se ejecutó cuando se produjo la excepción y obtener información adicional sobre el estado de la operación. `ProcessingLibraryException` se deriva de la clase `Exception` estándar de Java, por lo que también puede recuperar información sobre la excepción invocando a cualquiera de los métodos de excepción.

Consulte la siguiente implementación de ejemplo:

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
```

```
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

Si no proporciona su propio `ExceptionHandler`, en ese caso se sustituirá por `DefaultExceptionHandler`, que imprime un mensaje de error estándar.

> **Note**
>
> Si el parámetro `deleteMessageUponFailure` es `true`, la biblioteca de procesamiento de CloudTrail no distingue las excepciones generales de los errores de procesamiento y puede eliminar mensajes de la cola.
>
> 1. Por ejemplo, utilice la marca `SourceFilter` para filtrar los mensajes por marca de tiempo.
> 2. Sin embargo, no tiene los permisos necesarios para acceder al bucket de S3 que recibe los archivos de registros de CloudTrail. Dado que no dispone de los permisos necesarios, se lanza un `AmazonServiceException`. La biblioteca de procesamiento de CloudTrail incluye esto en una `CallBackException`.
> 3. `DefaultExceptionHandler` registra esto como un error, pero no identifica la causa raíz, que es el hecho de que no dispone de los permisos necesarios. La biblioteca de procesamiento de CloudTrail considera esto un error de procesamiento y elimina el mensaje, aún si este incluye un archivo de registros de CloudTrail válido.
>
> Si desea filtrar los mensajes con `SourceFilter`, verifique que su `ExceptionHandler` puede distinguir las excepciones de servicio de los errores de procesamiento.

Recursos adicionales

Para obtener más información sobre la biblioteca de procesamiento de CloudTrail, consulte lo siguiente:

- El proyecto GitHub de la biblioteca de procesamiento de CloudTrail, que incluye el código de muestra que ilustra cómo implementar una aplicación de la biblioteca de procesamiento de CloudTrail.
- Documentación del paquete Java de la biblioteca de procesamiento de CloudTrail.

Configuración

Puede utilizar la página de configuración de la CloudTrail consola para configurar y revisar las CloudTrail opciones.

Para acceder a la página de configuración

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. Selecciona Configuración en el panel de navegación izquierdo de la CloudTrail consola.
3. Revise y actualice la configuración según sea necesario.

Está disponible la siguiente configuración:

- Administrador delegado de la organización— Cuando lo utilices CloudTrail con una AWS Organizations organización, puedes asignar cualquier cuenta de la organización para que actúe como administrador CloudTrail delegado y gestione los almacenes de datos de rutas y eventos de la organización en nombre de la organización.
- Canales vinculados a servicios— AWS los servicios pueden crear un canal vinculado a los servicios para recibir CloudTrail eventos en tu nombre. El AWS servicio que crea el canal vinculado al servicio configura selectores de eventos avanzados para el canal y especifica si el canal se aplica a todos o a uno solo. Regiones de AWS Región de AWS

Administrador delegado de la organización

Cuando lo utilizas CloudTrail con una AWS Organizations organización, puedes asignar cualquier cuenta de la organización para que actúe como administrador CloudTrail delegado y gestione las rutas y los almacenes de datos de eventos de la organización en nombre de la organización. Un administrador delegado es una cuenta de miembro de una organización que puede realizar las mismas tareas administrativas (salvo que se indique lo contrario) que la cuenta de administración. CloudTrail

Si selecciona un administrador delegado, esa cuenta de miembro tendrá permisos administrativos en todos los registros de seguimiento de la organización y los almacenes de datos de eventos de la organización. Agregar un administrador delegado no altera la administración ni el funcionamiento de los registros de seguimiento ni de los almacenes de datos de eventos de la organización.

La primera vez que se agrega un administrador delegado a la CloudTrail consola, o mediante la CloudTrail API, se CloudTrail comprueba si la AWS CLI cuenta de administración de la organización tiene una función vinculada al servicio. Si la cuenta de administración no tiene un rol vinculado al servicio, CloudTrail crea el rol vinculado al servicio para la cuenta de administración. Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios de AWS CloudTrail.

> **Note**
>
> Cuando agrega un administrador delegado mediante la operación AWS Organizations CLI o API, el rol vinculado al servicio no se crea si no existe. El rol vinculado al servicio solo se crea cuando se hace una llamada desde la cuenta de administración directamente al CloudTrail servicio, por ejemplo, cuando se agrega un administrador delegado o se crea un registro de la organización o un almacén de datos de eventos mediante la consola o la API. CloudTrail AWS CLI CloudTrail

Toma nota de los siguientes factores que definen el funcionamiento del administrador delegado. CloudTrail

La cuenta de administración sigue siendo la propietaria de todos los recursos de la CloudTrail organización que cree el administrador delegado.

> La cuenta de administración de la organización sigue siendo la propietaria de todos los recursos de la CloudTrail organización que cree el administrador delegado, como los almacenes de datos de rutas y eventos. Esto proporciona continuidad a la organización en el caso de que el administrador delegado cambie.

Al eliminar una cuenta de administrador delegado, no se elimina ningún recurso de CloudTrail la organización que haya creado.

> Los registros de la organización y los almacenes de datos de eventos creados por el administrador delegado no se eliminan al eliminar al administrador delegado, ya que la cuenta de administración siempre actúa como propietaria de los recursos de la CloudTrail organización, independientemente de si los ha creado el administrador delegado o la cuenta de administración.

Una organización puede tener un máximo de tres CloudTrail administradores delegados.

> Puede tener un máximo de tres administradores CloudTrail delegados por organización. Para obtener más información acerca de cómo eliminar un administrador delegado, consulte Eliminar un administrador CloudTrail delegado.

En la siguiente tabla se muestran las capacidades de la cuenta de administración, las cuentas de administrador delegado y las cuentas que son miembros de la AWS Organizations organización.

Capacidades	Cuenta de administración	Cuenta de administrador delegado	Cuentas de miembros
Agregar o eliminar las cuentas de administrador delegado.	Sí	No	No
Crear un registro de seguimiento de la organización.	Sí	Sí[1]	No
Ver una lista de los registros de seguimiento de la organización.	Sí	Sí	Sí
Actualizar un registro de seguimiento de la organización.	Sí	Sí[1, 2]	No
Eliminar un registro de seguimiento de la organización.	Sí	Sí	No
Cree un almacén de datos de eventos de la organización para CloudTrail los eventos o los elementos AWS Config de configuración.	Sí	Sí	No
Habilite Insights en un almacén de datos de eventos de la organización.	Sí	No	No
Actualizar un almacén de datos de eventos de la organización.	Sí	Sí[2]	No

Capacidades	Cuenta de administración	Cuenta de administrador delegado	Cuentas de miembros
Habilitar la federación de consultas de Lake en un almacén de datos de eventos de la organización [3].	Sí	Sí	No
Deshabilitar la federación de consultas de Lake en un almacén de datos de eventos de la organización.	Sí	Sí	No
Eliminar un almacén de datos de eventos de la organización.	Sí	Sí	No
Copiar eventos de registro de seguimiento en un almacén de datos de eventos de la organización.	Sí	No	No
Ejecutar consultas en almacenes de datos de eventos de la organización.	Sí	Sí	No
Consultar el panel de Lake de un almacén de datos de eventos de la organización.	Sí	Sí	No

[1] El administrador delegado solo puede configurar un grupo de CloudWatch registros mediante las operaciones AWS CLI o CloudTrail `CreateTrail` o de la `UpdateTrail` API. Tanto el grupo de CloudWatch registros como la función de registro deben existir en la cuenta que realiza la llamada.

[2] Solo la cuenta de administración puede convertir un almacén de datos de registros o eventos de la organización en un banco de datos de registros o eventos a nivel de cuenta, o convertir un banco de datos de registros o eventos a nivel de cuenta en un banco de datos de registros o eventos de la organización. Estas acciones no están permitidas para el administrador delegado porque los registros de seguimiento y los almacenes de datos de eventos de la organización solo existen en la cuenta de administración. Cuando un banco de datos de registros o eventos de una organización se convierte en un banco de datos de registros o eventos a nivel de cuenta, solo la cuenta de administración tiene acceso al banco de datos de eventos o senderos.

[3] Solo una cuenta de administrador delegado o la cuenta de administración pueden habilitar la federación en el almacén de datos de eventos de una organización. Otras cuentas de administrador delegado pueden consultar y compartir información mediante la característica de uso compartido de datos de Lake Formation. Cualquier cuenta de administrador delegado, así como la cuenta de administración de la organización, pueden deshabilitar la federación.

Temas

- Permisos necesarios para designar un administrador delegado
- Agrega un administrador delegado CloudTrail
- Eliminar un administrador CloudTrail delegado

Permisos necesarios para designar un administrador delegado

Al asignar un administrador CloudTrail delegado, debe disponer de los permisos necesarios para añadir y eliminar al administrador delegado CloudTrail, así como de determinadas acciones de AWS Organizations API y permisos de IAM que se indican en la siguiente declaración de política.

Puede agregar la siguiente instrucción al final de una política de IAM para otorgar estos permisos:

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
    "Resource": "*"
}
```

Agrega un administrador delegado CloudTrail

Puede añadir un administrador delegado para gestionar los CloudTrail recursos de una organización, como los almacenes de datos de rutas y eventos.

Puede añadir un administrador CloudTrail delegado para su AWS organización mediante la CloudTrail consola o el. AWS CLI

Antes de agregar un administrador delegado, asegúrese de tener una cuenta en la organización y de haber iniciado sesión con la cuenta de administración de la organización. Para obtener información sobre cómo crear una AWS cuenta nueva para su organización, consulte Crear una AWS cuenta en su organización. Para obtener información sobre cómo invitar a una AWS cuenta existente a su organización, consulte Invitar una AWS cuenta a unirse a su organización.

CloudTrail console

El siguiente procedimiento muestra cómo añadir un administrador CloudTrail delegado mediante la CloudTrail consola.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. Selecciona Configuración en el panel de navegación izquierdo de la CloudTrail consola.
3. En la sección Organization delegated administrators (Administradores delegados de la organización), seleccione Register administrator (Registrar administrador).
4. Introduzca el ID de AWS cuenta de doce dígitos de la cuenta que desee asignar como administrador CloudTrail delegado de los almacenes de datos de senderos y eventos de la organización.
5. Elija Register administrator (Registrar administrador).

   Luego de agregar al administrador delegado, solo tiene que usar la cuenta de administración de la organización para cambiar o eliminar la cuenta de administrador delegado.

AWS CLI

En el siguiente ejemplo, se agrega un administrador delegado CloudTrail .

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

Este comando no genera ningún resultado si se utiliza correctamente.

Eliminar un administrador CloudTrail delegado

Puede eliminar un administrador CloudTrail delegado mediante la CloudTrail consola o el. AWS CLI

CloudTrail console

El siguiente procedimiento muestra cómo eliminar un administrador CloudTrail delegado mediante la CloudTrail consola.

1. Inicie sesión en la CloudTrail consola AWS Management Console y ábrala en https://console.aws.amazon.com/cloudtrail/.
2. Selecciona Configuración en el panel de navegación izquierdo de la CloudTrail consola.
3. En la sección Organization delegated administrators (Administradores delegados de la organización), elija el administrador delegado que desea eliminar.
4. Seleccione Remove administrator (Eliminar administrador).
5. Confirme que desea eliminar al administrador delegado y, a continuación, seleccione Remove administrator (Eliminar administrador).

AWS CLI

El siguiente comando elimina un administrador CloudTrail delegado.

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

Este comando no genera ningún resultado si se utiliza correctamente.

Canales vinculados a servicios

AWSlos servicios pueden crear un canal vinculado a un servicio para recibir CloudTrail eventos en su nombre. El AWS servicio que crea el canal vinculado al servicio configura selectores de eventos avanzados para el canal y especifica si el canal se aplica a todos o a uno solo. Regiones de AWS Región de AWS

Temas

- Visualización de canales vinculados a servicios con la consola

- Visualización de canales vinculados a servicios con la AWS CLI

Visualización de canales vinculados a servicios con la consola

Mediante la CloudTrail consola, puede ver información sobre cualquier canal vinculado a un CloudTrail servicio creado por los servicios. AWS La tabla está vacía si la cuenta no tiene ningún canal vinculado a un servicio.

Utilice el siguiente procedimiento para ver la información sobre un canal vinculado a un servicio.

1. Selecciona Configuración en el panel de navegación izquierdo de la CloudTrail consola.
2. En Canales vinculados a servicios, elija un canal vinculado a un servicio para ver sus detalles.
3. En la página de detalles, revise los ajustes configurados para el canal vinculado al servicio.

   Puede ver la siguiente información en la página de detalles:

   - Nombre del canal: el nombre completo del canal. El formato del nombre del canal es `aws-service-channel/`*`AWS_service_name`*`/slc`, donde *`AWS_service_name`* representa el nombre del servicio de AWS que administra el canal.
   - ARN del canal: el ARN del canal, que puede usar en una solicitud de API para obtener detalles sobre el canal.
   - Todas las regiones: el valor es `Yes` si el canal está configurado para todas las Regiones de AWS.
   - Servicio de AWS: el nombre del servicio de AWS que administra el canal.
   - Eventos de administración: muestra todos los eventos de administración configurados para el canal.
   - Eventos de datos: muestra todos los eventos de datos configurados para el canal.

Visualización de canales vinculados a servicios con la AWS CLI

Con la AWS CLI, puede ver la información sobre cualquier canal vinculado a servicios de CloudTrail creado por los servicios de AWS.

Temas

- Obtener un canal vinculado a servicios de CloudTrail
- Enumerar todos los canales vinculados a servicios de CloudTrail

- Eventos de servicios de AWS en canales vinculados a servicios

Obtener un canal vinculado a servicios de CloudTrail

El siguiente comando de la AWS CLI de ejemplo devuelve información sobre un canal vinculado a servicios de CloudTrail específico, incluido el nombre del servicio de AWS de destino, cualquier selector avanzado configurado para el canal y si este se aplica a todas las regiones o a una sola.

Debe especificar un ARN o el sufijo de ID de un ARN para `--channel`.

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

A continuación, se muestra un ejemplo de respuesta. En este ejemplo, `AWS_service_name` representa el nombre del servicio de AWS que creó el canal.

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
                        ]
                    }
                ]
            }
        ]
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
```

```
    ]
}
```

Enumerar todos los canales vinculados a servicios de CloudTrail

El siguiente comando de la AWS CLI de ejemplo devuelve información sobre todos los canales vinculados a servicios de CloudTrail que se crearon en su nombre. Los parámetros opcionales incluyen `--max-results` para especificar el número máximo de resultados que desea que el comando devuelva en una sola página. Si hay más resultados que el valor `--max-results` especificado, ejecute el comando de nuevo agregando el valor devuelto `NextToken` para obtener la siguiente página de resultados.

```
aws cloudtrail list-channels
```

A continuación, se muestra un ejemplo de respuesta. En este ejemplo, `AWS_service_name` representa el nombre del servicio de AWS que creó el canal.

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

Eventos de servicios de AWS en canales vinculados a servicios

El servicio de AWS que administra el canal vinculado a servicios puede iniciar acciones en el canal (por ejemplo, crear o actualizar un canal vinculado a servicios). CloudTrail registra estas acciones como Eventos de servicios de AWS y los envía al Historial de eventos y a todos los registros de seguimiento activos y los almacenes de datos de eventos configurados para los eventos de administración. Para estos eventos, el campo `eventType` tiene el valor `AwsServiceEvent`.

A continuación, se muestra un ejemplo de entrada en el archivo de registro para un evento de servicio de AWS por la creación de un canal vinculado a servicios.

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
   "eventSource":"cloudtrail.amazonaws.com",
   "eventName":"CreateServiceLinkedChannel",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"AWS Internal",
   "requestParameters":null,
   "responseElements":null,
   "requestID":"564f004c-EXAMPLE",
   "eventID":"234f004b-EXAMPLE",
   "readOnly":false,
   "resources":[
      {
         "accountId":"184434908391",
         "type":"AWS::CloudTrail::Channel",
         "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
      }
   ],
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "recipientAccountId":"111122223333",
   "eventCategory":"Management"
}
```

Seguridad en AWS CloudTrail

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. 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 sobre los programas de conformidad que se aplican a AWS CloudTrail, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación lo ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida cuando se utiliza CloudTrail. En los siguientes temas, se muestra cómo configurar CloudTrail para satisfacer los objetivos de seguridad y conformidad. También obtendrá información sobre cómo utilizar otros servicios de AWS que lo ayudarán a monitorear y proteger los recursos de CloudTrail.

Temas

- Protección de los datos en AWS CloudTrail
- Administración de identidades y accesos para AWS CloudTrail
- Validación de conformidad en AWS CloudTrail
- Resiliencia en AWS CloudTrail
- Seguridad de la infraestructura en AWS CloudTrail
- Prevención del suplente confuso entre servicios
- Mejores prácticas de seguridad en AWS CloudTrail
- Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS)

Protección de los datos en AWS CloudTrail

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos de AWS CloudTrail. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la 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 conceden a cada usuario los permisos necesarios para cumplir con 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 trabaje con CloudTrail 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.

De forma predeterminada, los archivos de registros de eventos de CloudTrail se cifran mediante el cifrado del lado del servidor (SSE) de Amazon S3. También puede optar por cifrar los archivos de registro con una clave AWS Key Management Service (AWS KMS). Puede almacenar sus archivos de registro en el bucket de durante el tiempo que quiera. También puede definir reglas de ciclo de vida de Amazon S3 para archivar o eliminar archivos de registros de forma automática. Si desea recibir notificaciones sobre el envío y la validación de archivos de registros, puede configurar las notificaciones de Amazon SNS.

Las siguientes prácticas recomendadas sobre seguridad también evalúan la protección de datos en CloudTrail:

- Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS)
- Política de bucket de Amazon S3 para CloudTrail
- Validar la integridad de los archivos de registros de CloudTrail
- Compartir archivos de registro de CloudTrail entre cuentas de AWS

Dado que los archivos de registro de CloudTrail se almacenan en uno o varios buckets en Amazon S3, también debe revisar la información sobre protección de datos en la Guía del usuario de Amazon Simple Storage Service. Para obtener más información, consulte Protección de datos en Amazon S3.

Administración de identidades y accesos para AWS CloudTrail

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. CloudTrail IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- Público
- Autenticación con identidades

- Administración de acceso mediante políticas
- Cómo funciona AWS CloudTrail con IAM
- Ejemplos de políticas basadas en identidades de AWS CloudTrail
- Ejemplos de políticas basadas en recursos de AWS CloudTrail
- Política de bucket de Amazon S3 para CloudTrail
- Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake
- Política temática de Amazon SNS para CloudTrail
- Solución de problemas de identidades de AWS CloudTrail y accesos
- Uso de roles vinculados a servicios de AWS CloudTrail
- Políticas administradas de AWS para AWS CloudTrail

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en CloudTrail.

Usuario del servicio: si utiliza el CloudTrail servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más CloudTrail funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en CloudTrail, consulte Solución de problemas de identidades de AWS CloudTrail y accesos.

Administrador de servicios: si estás a cargo de CloudTrail los recursos de tu empresa, probablemente tengas acceso total a ellos CloudTrail. Su trabajo consiste en determinar a qué CloudTrail funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM CloudTrail, consulteCómo funciona AWS CloudTrail con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas CloudTrail basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidades de AWS CloudTrail

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 de AWS IAM Identity Center. Los usuarios (del IAM Identity Center), 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 a 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 utiliza las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que utilice, 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 IAM Identity Center 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.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulte ¿Qué es el IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad en su 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 Consolecambiando 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 IAM Identity Center.
- 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 asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre 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 al servicio: un rol vinculado al 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 la 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 asociado 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 obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de 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.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario

raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del rol de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los

administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas de AWS en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para Desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del Usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de

la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario AWS Organizations.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del Usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona AWS CloudTrail con IAM

Antes de utilizar IAM para gestionar el acceso CloudTrail, infórmese sobre las funciones de IAM disponibles para su uso. CloudTrail

Características de IAM que puede utilizar con AWS CloudTrail

Característica de IAM	CloudTrail soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Parcial
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	No
ACL	No

Característica de IAM	CloudTrail soporte
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo CloudTrail funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWSlos servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para CloudTrail

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre los elementos que puede utilizar en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para CloudTrail

Para ver ejemplos de políticas CloudTrail basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS CloudTrail

Políticas basadas en recursos incluidas CloudTrail

Compatibilidad con las políticas basadas en recursos	Parcial

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de Servicios de AWS.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del Usuario de IAM.

CloudTrail apoya las políticas basadas en los recursos en los canales utilizados para las integraciones de CloudTrail Lake con fuentes de eventos externas a ellas. AWS La política basada en recursos del canal define qué entidades principales (cuentas, usuarios, roles y usuarios federados) pueden llamar a `PutAuditEvents` en el canal para enviar eventos al almacén de datos de eventos de destino. Para obtener más información sobre la creación de integraciones con CloudTrail Lake, consulte. Creación de una integración con un origen de eventos externo a AWS

Ejemplos

Para ver ejemplos de políticas CloudTrail basadas en recursos, consulte. Ejemplos de políticas basadas en recursos de AWS CloudTrail

Acciones políticas para CloudTrail

Admite acciones de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de CloudTrail acciones, consulte las acciones definidas por AWS CloudTrail en la Referencia de autorización del servicio.

Las acciones políticas CloudTrail utilizan el siguiente prefijo antes de la acción:

```
cloudtrail
```

Por ejemplo, para conceder a alguien permiso para crear una lista de las etiquetas de un registro de seguimiento con la operación `ListTags` de la API, incluya la acción `cloudtrail:ListTags` en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. CloudTrail define su propio conjunto de acciones que describen las tareas que puede realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
```

```
      "cloudtrail:RemoveTags
```

Puede utilizar caracteres comodín (*) para especificar varias acciones. Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción:

```
"Action": "cloudtrail:Get*"
```

Recursos de políticas para CloudTrail

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de CloudTrail recursos y sus ARN, consulte los recursos definidos por AWS CloudTrail en la Referencia de autorización de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS CloudTrail.

En CloudTrail, hay tres tipos de recursos: rutas, almacenes de datos de eventos y canales. Cada recurso tiene asociado un nombre de recurso de Amazon (ARN) único. En una política, se utiliza un ARN para identificar el recurso al que se aplica la política. CloudTrail actualmente no admite otros tipos de recursos, que a veces se denominan subrecursos.

El recurso de CloudTrail ruta tiene el siguiente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

El recurso del almacén de datos de CloudTrail eventos tiene el siguiente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

El recurso de CloudTrail canal tiene el siguiente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Por ejemplo, en el caso de una Cuenta de AWS con el ID *123456789012*, para especificar un registro de seguimiento denominado *My-Trail* que existe en la región Este de EE. UU. (Ohio), utilice el siguiente ARN:

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

Para especificar todos los registros de seguimiento que pertenezcan a una cuenta específica de esa Región de AWS, utilice el carácter comodín (*):

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

Algunas CloudTrail acciones, como las de creación de recursos, no se pueden realizar en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "*"
```

Muchas acciones CloudTrail de la API implican varios recursos. Por ejemplo, `CreateTrail` requiere un bucket de Amazon S3 para almacenar los archivos de registro, por lo que un debe tener permisos para escribir en el bucket. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
```

```
        "resource1",
        "resource2"
```

Claves de condición de la política para CloudTrail

Admite claves de condición de políticas específicas del servicio	No

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del Usuario de IAM.

CloudTrail no define sus propias claves de condición, pero admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver una lista de claves de CloudTrail condición, consulte las claves de condición AWS CloudTrail en la Referencia de autorización de servicio. Para obtener más información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por AWS CloudTrail.

ACL en CloudTrail

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con CloudTrail

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del Usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del Usuario de IAM.

Aunque puede adjuntar etiquetas a CloudTrail los recursos, CloudTrail solo permite controlar el acceso a los canales y almacenes de datos de eventos de CloudTrail Lake en función de las etiquetas. No se puede controlar el acceso a los registros de seguimiento en función de etiquetas.

Puedes adjuntar etiquetas a CloudTrail los recursos o pasarles etiquetas en una solicitud CloudTrail. Para obtener más información sobre el etiquetado de CloudTrail recursos, consulte Creación de un registro de seguimiento yCreación, actualización y gestión de senderos con AWS Command Line Interface.

Uso de credenciales temporales con CloudTrail

Admite el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utilice credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para CloudTrail

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo 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.

Roles de servicio para CloudTrail

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume 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.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir CloudTrail la funcionalidad. Edite las funciones de servicio solo cuando se CloudTrail proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para CloudTrail

Compatible con roles vinculados al servicio	Sí

Un rol vinculado al 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.

CloudTrail admite un rol vinculado al servicio para su integración con. AWS Organizations Este rol es necesario para crear un registro de seguimiento de la organización o un almacén de datos de eventos. Los registros de seguimiento de la organización y los almacenes de datos de eventos registran los eventos de todas las Cuentas de AWS de una organización. Para obtener más información sobre la creación o la administración de funciones CloudTrail vinculadas a un servicio, consulte. Uso de roles vinculados a servicios de AWS CloudTrail

Ejemplos de políticas basadas en identidades de AWS CloudTrail

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de CloudTrail. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos CloudTrail, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de la Referencia de AWS CloudTrail autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Ejemplo: permitir y denegar acciones para un registro de seguimiento especificado
- Ejemplos: creación y aplicación de políticas para acciones en registros de seguimiento específicos
- Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas
- Mediante la consola de CloudTrail
- Permitir a los usuarios consultar sus propios permisos
- Otorgar permisos personalizados a los CloudTrail usuarios

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear CloudTrail recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las

políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. xPara más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

CloudTrail no tiene claves de contexto específicas del servicio que pueda utilizar en el `Condition` elemento de las declaraciones de políticas.

Ejemplo: permitir y denegar acciones para un registro de seguimiento especificado

En el ejemplo siguiente, se muestra una política que permite a los usuarios que la tienen ver el estado y la configuración de un registro de seguimiento e iniciar y detener el registro de un registro de seguimiento denominado *My-First-Trail*. Este registro de seguimiento se creó en la región Este de EE. UU. (Ohio) (su región principal) en la Cuenta de AWS con el ID *123456789012*.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

El siguiente ejemplo muestra una política que deniega de forma explícita cualquier CloudTrail acción en cualquier ruta que no se llame My-First-Trail.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
```

```
  ]
}
```

Ejemplos: creación y aplicación de políticas para acciones en registros de seguimiento específicos

Puedes usar permisos y políticas para controlar la capacidad de un usuario de realizar acciones específicas en CloudTrail los senderos.

Por ejemplo, no le interesa que los usuarios del grupo de desarrolladores de su empresa inicien o detengan un registro de seguimiento específico. Sin embargo, tal vez le interese concederles permiso para que lleven a cabo las acciones `DescribeTrails` y `GetTrailStatus` que se hagan en el registro de seguimiento. Desea que los usuarios del grupo de desarrolladores realicen las acciones `StartLogging` o `StopLogging` en los registros de seguimiento que ellos administran.

Puede crear dos instrucciones de política y adjuntarlas al grupo de desarrolladores que cree en IAM. Para obtener más información sobre los grupos de IAM, consulte Grupos de IAM en la Guía del usuario de IAM .

En la primera, deniega las acciones `StartLogging` y `StopLogging` del ARN del registro de seguimiento que especifique. En el ejemplo siguiente, el ARN del registro de seguimiento es `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

En la segunda política, se permiten `GetTrailStatus` las acciones `DescribeTrails` y en todos los CloudTrail recursos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Si un usuario del grupo de desarrolladores intenta iniciar o detener el registro de seguimiento que ha especificado en la primera política, ese usuario obtiene una excepción de acceso denegado. Los usuarios del grupo de desarrolladores pueden iniciar y detener los registros de seguimiento que crean y administran.

En los siguientes ejemplos, se muestra el grupo de desarrolladores configurado en un perfil de AWS CLI denominado `devgroup`. En primer lugar, un usuario de `devgroup` ejecuta el comando `describe-trails`.

```
$ aws --profile devgroup cloudtrail describe-trails
```

El comando se completa correctamente con el resultado siguiente:

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
```

```
            "S3BucketName": "myS3bucket ",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

El usuario ejecuta el comando `get-trail-status` en el registro de seguimiento que ha especificado en la primera política.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

El comando se completa correctamente con el resultado siguiente:

```
{
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

A continuación, un usuario del grupo `devgroup` ejecuta el comando `stop-logging` en el mismo registro de seguimiento.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

El comando devuelve una excepción de acceso denegado, como la siguiente:

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

El usuario ejecuta el comando `start-logging` en el mismo registro de seguimiento.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

De nuevo, el comando devuelve una excepción de acceso denegado, como la siguiente:

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

Ejemplos: Denegación de acceso para crear o eliminar almacenes de datos de eventos en función de etiquetas

En el siguiente ejemplo de política, se deniega el permiso para crear un almacén de datos de eventos con `CreateEventDataStore` si no se cumple al menos una de las siguientes condiciones:

- El almacén de datos de eventos no tiene una clave de etiqueta de `stage` aplicada a sí mismo
- El valor de la etiqueta de la etapa no es `alpha`, `beta`, `gamma` ni `prod`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
            }
        }
    ]
```

```
}
```

En el siguiente ejemplo de política, se deniega el permiso para eliminar un almacén de datos de eventos con `DeleteEventDataStore` si el almacén de datos de eventos tiene la etiqueta `stage` con un valor de `prod`. Una política similar puede ayudar a proteger un almacén de datos de eventos de una eliminación accidental.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

Mediante la consola de CloudTrail

Para acceder a la consola de AWS CloudTrail, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los CloudTrail recursos de su propiedadCuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

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 AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Otorgar permisos de CloudTrail administración

Para permitir que las funciones o los usuarios de IAM administren un CloudTrail recurso, como una ruta, un almacén de datos de eventos o un canal, debes conceder permisos explícitos para realizar las acciones asociadas a las CloudTrail tareas. En la mayoría de las situaciones, puede utilizar una política administrada de AWS que contenga los permisos predefinidos.

> **Note**
>
> Los permisos que concede a los usuarios para realizar tareas de CloudTrail administración no son los mismos que CloudTrail los permisos necesarios para entregar archivos de registro a los buckets de Amazon S3 o enviar notificaciones a los temas de Amazon SNS. Para obtener más información acerca de estos permisos, consulte Política de bucket de Amazon S3 para CloudTrail.
>
> Si configura la integración con Amazon CloudWatch Logs, CloudTrail también se requiere un rol que pueda asumir para entregar eventos a un grupo de CloudWatch registros de Amazon Logs. Debe crear el rol que CloudTrail utiliza. Para obtener más información, consulte Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola y Envío de eventos a Amazon CloudWatch Logs.

Las siguientes políticas AWS administradas están disponibles para CloudTrail:

- AWSCloudTrail_FullAccess— Esta política proporciona acceso total a CloudTrail las acciones en CloudTrail los recursos, como las rutas, los almacenes de datos de eventos y los canales. Esta política proporciona los permisos necesarios para crear, actualizar y eliminar CloudTrail rutas, almacenes de datos de eventos y canales.

  Esta política también proporciona permisos para administrar el bucket de Amazon S3, el grupo de CloudWatch registros de Logs y un tema de Amazon SNS para un rastro. Sin embargo, la política `AWSCloudTrail_FullAccess` gestionada no proporciona permisos para eliminar el bucket de Amazon S3, el grupo de CloudWatch registros de Logs o un tema de Amazon SNS. Para obtener información sobre las políticas administradas para otros servicios de AWS, consulte la Guía de referencia de políticas administradas de AWS.

  > **Note**
  >
  > La política AWSCloudTrail_FullAccess no se ha concebido para compartirla ampliamente en la Cuenta de AWS. Los usuarios con este rol pueden desactivar o reconfigurar las funciones de auditoría más importantes y confidenciales de su Cuentas de AWS. Por este motivo, solo debe aplicar esta política a los administradores de cuentas. Debe controlar y supervisar de cerca el uso de esta política.

- AWSCloudTrail_ReadOnlyAccess— Esta política otorga permisos para ver la CloudTrail consola, incluidos los eventos recientes y el historial de eventos. Esta política también le permite ver los

registros de seguimiento, los almacenes de datos de eventos y los canales existentes. Los roles y los usuarios sujetos a esta política pueden descargar el historial de eventos, pero no pueden crear ni actualizar registros de seguimiento, almacenes de datos de eventos ni canales.

Para dar acceso, añada 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) Asocie una política directamente a un usuario o añada 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.

Recursos adicionales

Para obtener más información sobre el uso de IAM para dar acceso a los recursos de su cuenta a identidades, como usuarios y roles, consulte Cómo configurar IAM y Administración de acceso para los recursos de AWS en la Guía del usuario de IAM.

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 AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorgar permisos personalizados a los CloudTrail usuarios

CloudTrail las políticas otorgan permisos a los usuarios que trabajan con CloudTrail. Si necesita conceder permisos diferentes a los usuarios, puede adjuntar una CloudTrail política a un grupo de IAM o a un usuario. Puede editar la política para incluir o excluir permisos específicos. También puede crear su propia política personalizada. Las políticas son documentos JSON que definen las acciones que puede realizar un usuario y los recursos en los que este puede llevar a cabo dichas acciones. Para ver ejemplos específicos, consulte Ejemplo: permitir y denegar acciones para un

registro de seguimiento especificado y Ejemplos: creación y aplicación de políticas para acciones en registros de seguimiento específicos.

Contenido

- Acceso de solo lectura
- Acceso completo de
- Otorgar permiso para ver AWS Config información en la consola CloudTrail
- Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola
- Información adicional

Acceso de solo lectura

En el siguiente ejemplo, se muestra una política que concede acceso de solo lectura a las rutas. CloudTrail Equivale a la política administrada AWSCloudTrail_ReadOnlyAccess. Se concede permiso a los usuarios para ver la información de los registros de seguimiento, pero no para crear o actualizar registros de seguimiento.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:Get*",
                "cloudtrail:Describe*",
                "cloudtrail:List*",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

En las declaraciones de políticas, el elemento `Effect` especifica si las acciones se permiten o se niegan. El elemento `Action` enumera las acciones específicas que puede realizar el usuario. El elemento `Resource` enumera los recursos de AWS en los que el usuario puede realizar estas

acciones. En el caso de las políticas que controlan el acceso a CloudTrail las acciones, el `Resource` elemento suele estar * establecido en un comodín que significa «todos los recursos».

Los valores en el elemento `Action` corresponden a las API que admiten los servicios. Las acciones están precedidas por `cloudtrail:` para indicar que se refieren a acciones de CloudTrail . Puede utilizar el carácter comodín * en el elemento `Action`, como en los siguientes ejemplos:

- `"Action": ["cloudtrail:*Logging"]`

  Esto permite todas CloudTrail las acciones que terminan en «Registro» (`StartLogging`,`StopLogging`).
- `"Action": ["cloudtrail:*"]`

  Esto permite todas CloudTrail las acciones, pero no las acciones de otros AWS servicios.
- `"Action": ["*"]`

  Esto permite todas las acciones de AWS. Este permiso es adecuado para un usuario que actúa como administrador de AWS en su cuenta.

La política de solo lectura no concede permiso al usuario para las acciones `CreateTrail`, `UpdateTrail`, `StartLogging` y `StopLogging`. Los usuarios con esta política no pueden crear y actualizar registros de seguimiento, ni activar y desactivar los registros. Para ver la lista de CloudTrail acciones, consulta la referencia de la AWS CloudTrail API.

Acceso completo de

El siguiente ejemplo muestra una política que otorga acceso total a CloudTrail. Equivale a la política administrada AWSCloudTrail_FullAccess. Concede a los usuarios el permiso para realizar todas CloudTrail las acciones. También permite a los usuarios registrar eventos de datos en Amazon S3 y AWS Lambda gestionar los archivos de los buckets de Amazon S3, gestionar la forma en que CloudWatch Logs supervisa los eventos de CloudTrail registro y gestionar los temas de Amazon SNS en la cuenta a la que está asociado el usuario.

> **Important**
>
> La política AWSCloudTrail_FullAccess o los permisos equivalentes no se han concebido para compartirse ampliamente en la cuenta de AWS. Los usuarios con este rol o un acceso equivalente tienen la capacidad de desactivar o reconfigurar las funciones de auditoría más importantes y confidenciales en sus cuentas de AWS. Por este motivo, esta política

debe aplicarse únicamente a los administradores de cuentas y su uso debe ser controlado y monitorizado estrictamente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Otorgar permiso para ver AWS Config información en la consola CloudTrail

Puede ver la información del evento en la CloudTrail consola, incluidos los recursos relacionados con ese evento. Para estos recursos, puede elegir el icono de AWS Config para ver el calendario de ese recurso en la consola de AWS Config. Adjunte esta política a los usuarios para concederles acceso de solo lectura a AWS Config. La política no les concede permiso para cambiar los ajustes en AWS Config.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

Para obtener más información, consulte Ver los recursos a los que se hace referencia AWS Config.

Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola

Puede ver y configurar la entrega de eventos a CloudWatch Logs en la CloudTrail consola si tiene los permisos suficientes. Estos permisos pueden ser más amplios que los que se conceden a los administradores de CloudTrail. Adjunte esta política a los administradores que configurarán y gestionarán CloudTrail la integración con CloudWatch los registros. La política no les concede permisos directos para entrar en los CloudWatch registros CloudTrail o en ellos, sino que les concede los permisos necesarios para crear y configurar la función que CloudTrail asumirá para entregar correctamente los eventos a su grupo de CloudWatch registros.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.

Información adicional

Para obtener más información sobre el uso de IAM para dar acceso a los recursos de su cuenta a identidades, como usuarios y roles, consulte Introducción y Administración de acceso para los recursos de AWS en la Guía del usuario de IAM.

Ejemplos de políticas basadas en recursos de AWS CloudTrail

CloudTrail admite políticas de permisos basadas en recursos para los CloudTrail canales utilizados en las integraciones de CloudTrail Lake. Para obtener más información sobre la creación de integraciones con CloudTrail Lake, consulte. Creación de una integración con un origen de eventos externo a AWS

La información necesaria para la política está determinada por el tipo de integración.

- Para una integración directa, es CloudTrail necesario que la política contenga Cuenta de AWS los ID del socio y que introduzca el identificador externo exclusivo proporcionado por el socio. CloudTrail añade automáticamente los Cuenta de AWS ID del socio a la política de recursos al crear una integración mediante la CloudTrail consola. Consulte la documentación de socios para obtener información sobre cómo obtener los números de Cuenta de AWS necesarios para la política.
- Para la integración de una solución, debe especificar al menos un ID de Cuenta de AWS como entidad principal y, si lo desea, puede introducir un ID externo para evitar un suplente confuso.

Estos son los requisitos de la política basada en recursos:

- El ARN del recurso definido en la política debe coincidir con el ARN del canal al que está asociada la política.
- La política contiene solo una acción: `cloudtrail-data:PutAuditEvents`
- La política contiene como mínimo una instrucción. La política puede tener como máximo 20 instrucciones.
- Cada instrucción contiene como mínimo una entidad principal. Una instrucción puede tener como máximo 50 entidades principales.

El propietario del canal puede llamar a la API `PutAuditEvents` en el canal a menos que la política le niegue el acceso al recurso.

Temas

- Ejemplo: proporcionar acceso al canal a las entidades principales.
- Ejemplo: usar un ID externo para evitar un suplente confuso.

Ejemplo: proporcionar acceso al canal a las entidades principales.

El siguiente ejemplo otorga permisos a los principales con los ARN y `arn:aws:iam::111122223333:root` `arn:aws:iam::123456789012:root` para llamar a la PutAuditEventsAPI en el CloudTrail canal con el ARN. `arn:aws:iam::444455556666:root` `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Ejemplo: usar un ID externo para evitar un suplente confuso.

En el siguiente ejemplo se utiliza un ID externo para direccionar y evitar que haya un suplente confuso. El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción.

El socio de integración crea el ID externo para usarlo en la política. A continuación, se proporciona el ID externo como parte de la creación de la integración. Este valor puede ser cualquier cadena única, como, por ejemplo, una frase de contraseña o un número de cuenta.

El ejemplo otorga permisos a los principales con los ARN `arn:aws:iam::111122223333:root` y permite llamar `arn:aws:iam::123456789012:root` a la PutAuditEventsAPI en el recurso del CloudTrail canal si la llamada a la `PutAuditEvents` API incluye el valor de ID externo definido en la política. `arn:aws:iam::444455556666:root`

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "uniquePartnerExternalID"
                }
            }
        }
    ]
}
```

Política de bucket de Amazon S3 para CloudTrail

De forma predeterminada, los buckets y los objetos de Amazon S3 son privados. Solo el propietario del recurso (la cuenta de AWS que creó el bucket) puede tener acceso al bucket y a los objetos que contiene. El propietario del recurso puede conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Si desea crear o modificar un bucket de Amazon S3 para que reciba los archivos de registro de un registro de traza de organización, deberá modificar aún más la política del bucket. Para obtener más información, consulte Crear un registro para una organización con AWS Command Line Interface.

Para enviar archivos de registro a un depósito de S3, CloudTrail debe tener los permisos necesarios y no puede configurarse como un depósito que el solicitante paga.

CloudTrail añade los siguientes campos a la política por usted:

- Los SID permitidos
- El nombre del bucket
- El nombre principal del servicio para CloudTrail
- El nombre de la carpeta en la que se almacenan los archivos de registro, incluido el nombre del depósito, un prefijo (si lo especificó) y el identificador de su AWS cuenta

Como práctica recomendada de seguridad, agregue una clave de conción `aws:SourceArn` de la política de bucket de Amazon S3. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que solo se CloudTrail escriba en el bucket de S3 para una o varias rutas específicas. El valor de `aws:SourceArn` siempre es el ARN de la traza (o matriz de ARN de senderos) que utiliza el bucket para almacenar registros. Asegúrese de agregar la clave de condición `aws:SourceArn` en las políticas de bucket de S3 para las trazas existentes.

La siguiente política permite CloudTrail escribir archivos de registro en el bucket desde lo compatible Regiones de AWS. Sustituya *myBucketName[OptionalPrefix]/*, *myAccountID*, *region* y *TrailName* por los valores adecuados para su configuración.

Política de bucket de S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Para obtener más información al respecto, consulte. Regiones de AWSCloudTrail regiones compatibles

Contenido

- Especificar un depósito existente para la entrega de CloudTrail registros
- Recibir archivos de registro de otras cuentas
- Creación o actualización de un bucket de Amazon S3 para utilizarlo a fin de almacenar los archivos de registros de un registro de seguimiento de organización
- Solucionar problemas con la política de bucket de Amazon S3
  - Errores comunes en la configuración de la política de Amazon S3
  - Cambiar un prefijo de un bucket existente
- Recursos adicionales de

Especificar un depósito existente para la entrega de CloudTrail registros

Si especificó un depósito de S3 existente como ubicación de almacenamiento para la entrega de los archivos de registro, debe adjuntar una política CloudTrail al depósito que permita escribir en él.

> **Note**
>
> Como práctica recomendada, utilice un depósito de S3 dedicado a los CloudTrail registros.

Para añadir la CloudTrail política requerida a un bucket de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el depósito en el que quiere CloudTrail entregar los archivos de registro y, a continuación, elija Permisos.
3. Elija Editar.
4. Copie S3 bucket policy en la ventana Bucket Policy Editor. Sustituya los marcadores de posición en cursiva por los nombres del prefijo del bucket y el número de cuenta. Si especificó un prefijo cuando creó el registro de seguimiento, inclúyalo aquí. El prefijo es un añadido opcional a la clave del objeto de S3 que crea una organización en forma de carpeta en su bucket.

   > **Note**
   >
   > Si el depósito existente ya tiene una o más políticas adjuntas, añada las instrucciones para CloudTrail acceder a esa política o políticas. Evalúe el conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que van a tener acceso al bucket.

Recibir archivos de registro de otras cuentas

Puede configurarlo CloudTrail para entregar los archivos de registro de varias AWS cuentas a un único depósito de S3. Para obtener más información, consulte Recepción de archivos de CloudTrail registro de varias cuentas.

Creación o actualización de un bucket de Amazon S3 para utilizarlo a fin de almacenar los archivos de registros de un registro de seguimiento de organización

Debe especificar un bucket de Amazon S3 para recibir los archivos de registros de un registro de seguimiento de organización. Este depósito debe tener una política que permita CloudTrail colocar los archivos de registro de la organización en el depósito.

El siguiente es un ejemplo de política para un bucket de Amazon S3 denominado *myOrganizationBucket*, que es propiedad de la cuenta de administración de la organización. Sustituya *myOrganizationBucket*, *region*, *managementAccountID*, *TrailName* y *O-OrganizationID por los valores de su organización*

Esta política de bucket contiene tres instrucciones.

- La primera afirmación permite llamar CloudTrail a la `GetBucketAcl` acción de Amazon S3 en el bucket de Amazon S3.
- La segunda instrucción permite el registro en caso de que se cambie el registro de seguimiento de uno de organización a otro solo para esa cuenta.
- La tercera instrucción permite registrar el registro de seguimiento de una organización.

La política de ejemplo incluye una clave de condición `aws:SourceArn` para la política de bucket de Amazon S3. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que solo se CloudTrail escriba en el bucket de S3 para una o varias rutas específicas. En una traza de organización, el valor de `aws:SourceArn` debe ser un ARN de seguimiento que pertenece a la cuenta de administración y utilice el ID de cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
```

```
}
```

Esta política de ejemplo no permite que ningún usuario de las cuentas miembro obtenga acceso a los archivos de registro creados para la organización. De forma predeterminada, solo la cuenta de administración tendrá acceso a los archivos de registros de organización. Para obtener información sobre cómo permitir a los usuarios de IAM de las cuentas miembro el acceso de lectura al bucket de Amazon S3, consulte Compartir archivos de registro de CloudTrail entre cuentas de AWS.

Solucionar problemas con la política de bucket de Amazon S3

En las secciones siguientes se describe cómo solucionar problemas con la política de bucket de S3.

Errores comunes en la configuración de la política de Amazon S3

Al crear un nuevo depósito como parte de la creación o actualización de un sendero, CloudTrail adjunta los permisos necesarios al depósito. La política de segmentos usa el nombre principal del servicio`"cloudtrail.amazonaws.com"`, lo que permite CloudTrail entregar registros para todas las regiones.

Si no entrega registros para una región, CloudTrail es posible que su depósito tenga una política anterior que especifique los ID de CloudTrail cuenta de cada región. Esta política permite CloudTrail entregar registros solo para las regiones especificadas.

Como práctica recomendada, actualice la política para usar un permiso con el director del CloudTrail servicio. Para ello, sustituya los ARN del ID de cuenta por el nombre principal del servicio: `"cloudtrail.amazonaws.com"`. Esto permite CloudTrail entregar registros para las regiones actuales y nuevas. Como práctica recomendada de seguridad, agregue una clave de condición `aws:SourceArn` o `aws:SourceAccount` a la política de bucket de Amazon S3. Esto ayuda a evitar el acceso no autorizado de la cuenta a su bucket de S3. Si tiene trazas existentes, asegúrese de agregar una o más claves de condición. A continuación se muestra un ejemplo de configuración de política recomendada: Sustituya *`myBucketName[OptionalPrefix]/`*, *`myAccountID`*, *`region`* y *`TrailName`* por los valores adecuados para su configuración.

Example Ejemplo de política de bucket con nombre principal del servicio

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
```

```
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Cambiar un prefijo de un bucket existente

Si intenta agregar, modificar o eliminar el prefijo de un archivo de registro para un bucket de S3 que recibe registros de una traza, puede que aparezca el error: There is a problem with the bucket policy (Hay un problema con la política de bucket). Una política de bucket con un prefijo incorrecto puede impedir que su registro de seguimiento envíe archivos de registro al bucket. Para resolver este problema, utilice la consola Amazon S3 para actualizar el prefijo de la política de bucket y, a continuación, utilice la CloudTrail consola para especificar el mismo prefijo para el bucket de la ruta.

Para actualizar el prefijo del archivo de registros de un bucket de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el bucket para el que desea modificar el prefijo y, a continuación, seleccione Permissions (Permisos).

3. Elija Editar.
4. En la política del bucket, en la acción `s3:PutObject`, edite la entrada `Resource` para añadir, modificar o eliminar el *`prefijo`* del archivo de registro según sea necesario.

```
"Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
```

5. Seleccione Guardar.
6. Abra la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/.
7. Elija su registro de seguimiento y, en Storage location, haga clic en el icono del lápiz para editar la configuración del bucket.
8. En S3 bucket, elija el bucket con el prefijo que va a cambiar.
9. En Log file prefix, actualice el prefijo de forma que coincida con el prefijo que ha escrito en la política del bucket.
10. Seleccione Guardar.

Recursos adicionales de

Para obtener más información sobre los buckets de S3 y las políticas, consulte la Guía del usuario de Amazon Simple Storage Service.

Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake

De forma predeterminada, los buckets y los objetos de Amazon S3 son privados. Solo el propietario del recurso (la cuenta de AWS que creó el bucket) puede tener acceso al bucket y a los objetos que contiene. El propietario del recurso puede conceder permisos de acceso a otros recursos y usuarios escribiendo una política de acceso.

Para enviar resultados de consultas de CloudTrail Lake a un bucket de S3, CloudTrail debe tener los permisos necesarios y no puede configurarse como un bucket de pago por solicitante.

CloudTrail agrega de forma automática los siguientes campos a la política:

- Los SID permitidos
- El nombre del bucket
- El nombre principal del servicio para CloudTrail.

Como práctica recomendada de seguridad, agregue una clave de conción `aws:SourceArn` de la política de bucket de Amazon S3. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que CloudTrail escribe en el bucket de S3 solo para el almacén de datos de eventos.

La siguiente política permite a CloudTrail entregar resultados de consultas en el bucket desde Regiones de AWS compatibles. Reemplace *myBucketName* (Nombre del bucket), *myAccountID* (ID de la cuenta) y *myQueryRunningRegion* (Mi región de ejecución de la consulta) por los valores adecuados para su configuración. *myAccountID* (ID de la cuenta) es el ID de la cuenta de AWS usado para CloudTrail Lake, que puede no ser el ID de la cuenta de AWS del bucket de S3.

> **Note**
>
> Si su política de bucket incluye una instrucción para una clave de KMS, le recomendamos que use un ARN de la clave de KMS totalmente calificada. Si, en su lugar, utiliza un alias de clave de KMS, AWS KMS resolverá la clave dentro de la cuenta del solicitante. Esto puede dar como resultado datos cifrados con una clave de KMS que pertenece al solicitante y no al propietario del bucket.
> Si se trata de un almacén de datos de eventos de la organización, el ARN del almacén de datos de eventos debe incluir el ID de la cuenta de AWS para la cuenta de administración. Esto se debe a que la cuenta de administración mantiene la propiedad de todos los recursos de la organización.

Política de bucket de S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
```

```
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

Contenido

- Especificar un bucket existente para resultados de consultas de CloudTrail Lake
- Recursos adicionales

Especificar un bucket existente para resultados de consultas de CloudTrail Lake

Si especificó un bucket de S3 existente como ubicación de almacenamiento para el envío de resultados de consultas de CloudTrail Lake, debe adjuntar una política al bucket que permita a CloudTrail entregar los resultados de consultas al bucket.

> **Note**
>
> Es recomendable que use un bucket de S3 dedicado para los resultados de consultas de CloudTrail.

Para agregar la política de CloudTrail necesaria a un bucket de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Elija el bucket donde desea que CloudTrail envíe los resultados de consultas y, a continuación, elija Permissions (Permisos).
3. Elija Editar.
4. Copie S3 bucket policy for query results en la ventana Bucket Policy Editor. Reemplace los marcadores de posición en cursiva por los nombres del bucket, de la región y del ID de cuenta.

> **Note**
>
> Si el bucket existente ya tiene una o varias políticas asociadas, agregue las instrucciones para que CloudTrail tenga acceso a dicha política o políticas. Evalúe el conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que tienen acceso al bucket.

Recursos adicionales

Para obtener más información acerca de las políticas y los buckets de S3, consulte Uso de políticas de bucket en la Guía del usuario de Amazon Simple Storage Service.

Política temática de Amazon SNS para CloudTrail

Para enviar notificaciones a un tema de SNS, CloudTrail debe tener los permisos necesarios. CloudTrailadjunta automáticamente los permisos necesarios al tema cuando crea un tema de Amazon SNS como parte de la creación o actualización de una ruta en CloudTrail la consola.

> **Important**
>
> Como práctica recomendada de seguridad, para restringir el acceso al tema de SNS, se aconseja firmemente que después de crear o actualizar un registro de seguimiento para enviar notificaciones de SNS, edite de forma manual la política de IAM adjunta al tema de SNS para agregar claves de condición. Para obtener más información, consulte the section called “Práctica recomendada de seguridad para la política de temas SNS” en este tema.

CloudTrail añade automáticamente la siguiente declaración a la política con los siguientes campos:

- Los SID permitidos
- El nombre principal del servicio de CloudTrail.
- El tema de SNS, incluida la región, el ID de cuenta y el nombre del tema.

La siguiente política permite CloudTrail enviar notificaciones sobre la entrega de archivos de registro desde las regiones compatibles. Para obtener más información, consulte CloudTrail regiones compatibles. Esta es la política predeterminada que se adjunta a una política de tema de SNS nueva o existente al crear o actualizar un registro de seguimiento, y elige habilitar las notificaciones SNS.

Política de temas de SNS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
        }
    ]
}
```

Para utilizar un tema AWS KMS de Amazon SNS cifrado para enviar notificaciones, también debe habilitar la compatibilidad entre la fuente del evento CloudTrail () y el tema cifrado añadiendo la siguiente declaración a la política del. AWS KMS key

Política de claves de KMS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
```

```
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Habilitar la compatibilidad entre las fuentes de eventos de AWS los servicios y los temas cifrados.

Contenido

- Práctica recomendada de seguridad para la política de temas SNS
- Especificación de un tema existente para enviar notificaciones
- Resolución de problemas de la política de temas de SNS
  - CloudTrail no envía notificaciones para una región
  - CloudTrail no envía notificaciones para una cuenta de miembro de una organización
- Recursos adicionales de

Práctica recomendada de seguridad para la política de temas SNS

De forma predeterminada, la declaración de política de IAM que se CloudTrail adjunta a su tema de Amazon SNS permite al director CloudTrail del servicio publicar en un tema de SNS, identificado por un ARN. Para evitar que un atacante acceda a su tema de SNS y envíe notificaciones en su nombre a los destinatarios del tema, edite manualmente su política de temas de CloudTrail SNS CloudTrail para añadir una clave de `aws:SourceArn` condición a la declaración de política adjunta por. CloudTrail El valor de esta clave es el ARN de la traza o una matriz de ARN de traza que utilizan el tema SNS. Ya que incluye tanto el ID del registro de seguimiento específico como el ID de la cuenta propietaria del registro de traza y restringe el acceso al tema SNS solo a aquellas cuentas que tienen permiso para administrar el registro de traza. Antes de añadir claves condicionales a tu política de temas de SNS, obtén el nombre del tema de SNS en la configuración de tu ruta en la consola. CloudTrail

La clave de condición `aws:SourceAccount` también se admite, aunque no se recomienda.

Para agregar la clave de condición **`aws:SourceArn`** a la política de temas de SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Temas.
3. Elija el tema SNS que se muestra en la configuración del registro de seguimiento y, a continuación, Edit (Editar).
4. Expanda Política de acceso.
5. En el editor JSON de Access policy (Política de acceso), busque un bloque similar al siguiente ejemplo.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Agregue un bloque nuevo para una condición, `aws:SourceArn` como se muestra en el siguiente ejemplo. El valor de `aws:SourceArn` es el ARN del registro de seguimiento sobre el que se envían notificaciones a SNS.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. Cuando haya terminado de editar la política de temas de SNS, elija Save changes (Guardar cambios).

Para agregar la clave de condición **`aws:SourceAccount`** a la política de temas de SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Temas.
3. Elija el tema SNS que se muestra en la configuración del registro de seguimiento y, a continuación, Edit (Editar).
4. Expanda Política de acceso.
5. En el editor JSON de Access policy (Política de acceso), busque un bloque similar al siguiente ejemplo.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Agregue un bloque nuevo para una condición, `aws:SourceAccount` como se muestra en el siguiente ejemplo. El valor de `aws:SourceAccount` es el ID de la cuenta propietaria del CloudTrail sendero. En este ejemplo, se restringe el acceso al tema de SNS únicamente a los usuarios que pueden iniciar sesión en la AWS cuenta 123456789012.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. Cuando haya terminado de editar la política de temas de SNS, elija Save changes (Guardar cambios).

Especificación de un tema existente para enviar notificaciones

Puede añadir manualmente los permisos de un tema de Amazon SNS a su política de temas en la consola de Amazon SNS y, a continuación, especificar el tema en la consola. CloudTrail

Para actualizar manualmente una política de temas de SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Elija Topics y, a continuación, seleccione el tema.
3. Selecciona Editar y, a continuación, desplázate hacia abajo hasta Política de acceso.
4. Agrega el extracto de SNS topic policy con los valores correspondientes a la región, el identificador de la cuenta y el nombre del tema.
5. Si tu tema es un tema cifrado, debes CloudTrail permitir tener `kms:GenerateDataKey*` los `kms:Decrypt` permisos necesarios. Para obtener más información, consulte Encrypted SNS topic KMS key policy.
6. Seleccione Guardar cambios.
7. Regrese a la CloudTrail consola y especifique el tema de la ruta.

Resolución de problemas de la política de temas de SNS

En las secciones siguientes se describe cómo solucionar problemas de la política de temas de SNS.

Escenarios:

- CloudTrail no envía notificaciones para una región
- CloudTrail no envía notificaciones para una cuenta de miembro de una organización

CloudTrail no envía notificaciones para una región

Cuando creas un tema nuevo como parte de la creación o actualización de una ruta, CloudTrail adjuntas los permisos necesarios a tu tema. La política temática utiliza el nombre principal del servicio`"cloudtrail.amazonaws.com"`, lo que permite enviar notificaciones CloudTrail a todas las regiones.

Si no envía notificaciones para una región, CloudTrail es posible que su tema tenga una política anterior que especifique los ID de CloudTrail cuenta de cada región. Esta política permite CloudTrail enviar notificaciones solo a las regiones especificadas.

La siguiente política temática permite CloudTrail enviar notificaciones únicamente a las nueve regiones especificadas:

Example política del tema con ID de la cuenta

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

Esta política utiliza un permiso basado en los ID de CloudTrail cuenta individuales. Para entregar los registros de una nueva región, debes actualizar manualmente la política para incluir el ID de CloudTrail cuenta de esa región. Por ejemplo, dado que CloudTrail se agregó compatibilidad con la región EE.UU. Este (Ohio), debe actualizar la política para agregar el identificador de cuenta ARN para esa región:. `"arn:aws:iam::475085895292:root"`

Como práctica recomendada, actualice la política para usar un permiso con el director del CloudTrail servicio. Para ello, sustituya los ARN del ID de cuenta por el nombre principal del servicio: `"cloudtrail.amazonaws.com"`.

Esto permite CloudTrail enviar notificaciones para las regiones actuales y nuevas. A continuación se incluye una versión actualizada de la política anterior:

Example política del tema con el nombre principal del servicio

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

Compruebe que la política tiene los valores correctos:

- En el campo `Resource`, especifique el número de cuenta del propietario del tema. Para temas que haya creado usted, especifique su número de cuenta.
- Especifique los valores adecuados para la región y el nombre del tema de SNS.

CloudTrail no envía notificaciones para una cuenta de miembro de una organización

Si una cuenta de miembro con un registro de AWS Organizations la organización no envía notificaciones de Amazon SNS, podría haber un problema con la configuración de la política de temas de Amazon SNS. CloudTrail crea registros organizativos en las cuentas de los miembros incluso si se produce un error en la validación de un recurso; por ejemplo, el tema de SNS del registro de la organización no incluye todos los ID de las cuentas de los miembros. Si la política de temas de SNS es incorrecta, se produce un error de autorización.

Para comprobar si la política de temas de SNS de una ruta tiene un error de autorización:

- Desde la CloudTrail consola, consulta la página de detalles del sendero. Si se produce un error en la autorización, la página de detalles incluye una advertencia `SNS authorization failed` e indica que hay que corregir la política de temas de SNS.

- Desde AWS CLI, ejecute el get-trail-statuscomando. Si se produce un error de autorización, el resultado del comando incluye el `LastNotificationError` campo con un valor de`AuthorizationError`.

Recursos adicionales de

Para obtener más información sobre los temas de SNS y suscribirse a ellos, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Solución de problemas de identidades de AWS CloudTrail y accesos

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con CloudTrail un IAM.

Temas

- No estoy autorizado a realizar ninguna acción en CloudTrail
- No tengo autorización para realizar iam:PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos CloudTrail
- No tengo autorización para llevar a cabo iam:PassRole
- Recibo una excepción NoManagementAccountSLRExistsException cuando intento crear un registro de seguimiento de la organización o un almacén de datos de eventos

No estoy autorizado a realizar ninguna acción en CloudTrail

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `cloudtrail:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `cloudtrail:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Si la AWS Management Console le indica que no tiene autorización para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario de `mateojackson` IAM intenta utilizar la consola para ver los detalles de una ruta, pero no tiene la política de CloudTrail gestión adecuada o los permisos equivalentes aplicados a su cuenta. AWSCloudTrail_FullAccessAWSCloudTrail_ReadOnlyAccess

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

En este caso, Mateo solicita a su administrador que actualice sus políticas para que pueda tener acceso a la información del registro de seguimiento y al estado en la consola.

Si inicias sesión con un usuario o rol de IAM que tiene la política AWSCloudTrail_FullAccessadministrada o sus permisos equivalentes y no puedes configurar AWS Config la integración de Amazon CloudWatch Logs con una ruta, es posible que te falten los permisos necesarios para la integración con esos servicios. Para obtener más información, consulte Otorgar permiso para ver AWS Config información en la consola CloudTrail y Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la CloudTrail consola.

No tengo autorización para realizar **`iam:PassRole`**

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a CloudTrail.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en CloudTrail. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos CloudTrail

Puedes crear un rol y compartir CloudTrail información entre variosCuentas de AWS. Para obtener más información, consulte Compartir archivos de registro de CloudTrail entre cuentas de AWS.

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si CloudTrail es compatible con estas funciones, consulteCómo funciona AWS CloudTrail con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para obtener información sobre 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.

No tengo autorización para llevar a cabo **iam:PassRole**

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a CloudTrail.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en CloudTrail. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Recibo una excepción **NoManagementAccountSLRExistsException** cuando intento crear un registro de seguimiento de la organización o un almacén de datos de eventos

La excepción `NoManagementAccountSLRExistsException` se produce cuando la cuenta de administración no tiene ningún rol vinculado al servicio. Al agregar un administrador delegado mediante la operación AWS Organizations de la AWS CLI o la API, el rol vinculado al servicio no se crea si no existe.

Al utilizar la cuenta de administración de su organización para añadir un administrador delegado o crear un registro de la organización o un almacén de datos de eventos en la CloudTrail consola, o al utilizar la AWS CLI CloudTrail API, crea CloudTrail automáticamente un rol vinculado al servicio para su cuenta de administración si aún no existe uno.

Si no has agregado un administrador delegado, usa la CloudTrail consola AWS CLI o la CloudTrail API para agregar el administrador delegado. Para obtener más información sobre

cómo añadir un administrador delegado, consulte Agrega un administrador delegado CloudTrail y RegisterOrganizationDelegatedAdmin(API).

Si ya has agregado al administrador delegado, usa la cuenta de administración para crear el registro de la organización o el almacén de datos de eventos en la CloudTrail consola, o usa la API AWS CLI o CloudTrail . Para obtener más información sobre la creación de un registro de la organizaciónCreación de un registro de seguimiento para la organización en la consola, consulteCrear un registro para una organización con AWS Command Line Interface, y CreateTrail(API).

Uso de roles vinculados a servicios de AWS CloudTrail

AWS CloudTrail utiliza roles vinculados a un servicio de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a CloudTrail. Los roles vinculados a servicios están predefinidos por CloudTrail e incluyen todos los permisos que el servicio requiere para llamar a otros Servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de CloudTrail porque ya no tendrá que agregar de forma manual los permisos necesarios. CloudTrail define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo CloudTrail puede adoptar sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

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 servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para CloudTrail

CloudTrail utiliza el rol vinculado al servicio denominado AWSServiceRoleForCloudTrail: este rol vinculado al servicio se utiliza respaldar los registros de seguimiento de la organización y los almacenes de datos de eventos de la organización.

El rol vinculado a un servicio AWSServiceRoleForCloudTrail confía en que los siguientes servicios adopten el rol:

- `cloudtrail.amazonaws.com`

Este rol se utiliza para respaldar la creación y la administración de registros de seguimiento de organización de CloudTrail y los almacenes de datos de eventos de la organización CloudTrail Lake en CloudTrail. Para obtener más información, consulte Creación de un registro de seguimiento para una organización.

La política CloudTrailServiceRolePolicy adjunta al rol permite que CloudTrail realice las siguientes acciones en los recursos especificados:

- Acciones sobre todos los recursos de CloudTrail:
  - `All`
- Acciones en todos los recursos de AWS Organizations:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- Acciones en todos los recursos de Organizations para que la entidad principal de servicio de CloudTrail enumere los administradores delegados de la organización:
  - `organizations:ListDelegatedAdministrators`
- Acciones para deshabilitar la federación de Lake en el almacén de datos de eventos de una organización:
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para CloudTrail

No necesita crear manualmente un rol vinculado a servicios. Al crear un registro de seguimiento de la organización o un almacén de datos de eventos de la organización, o al agregar un administrador delegado en la consola de CloudTrail o al utilizar la AWS CLI o la operación de la API, CloudTrail crea el rol vinculado al servicio en su nombre, si aún no existe.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un registro de seguimiento de la

organización o un almacén de datos de eventos de la organización, o al agregar un administrador delegado, CloudTrail vuelve a crear el rol vinculado al servicio en su nombre.

Edición de un rol vinculado a un servicio para CloudTrail

CloudTrail no le permite editar el rol vinculado a servicios AWSServiceRoleForCloudTrail. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Modificación de un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio para CloudTrail

No es necesario eliminar de forma manual el rol AWSServiceRoleForCloudTrail. Si una cuenta de Cuenta de AWS se elimina de una organización de Organizations, el rol AWSServiceRoleForCloudTrail se elimina de forma automática de dicha Cuenta de AWS. No puede desconectar ni eliminar políticas del rol AWSServiceRoleForCloudTrail vinculado al servicio en una cuenta de administración de organización sin eliminar la cuenta de la organización.

También puede utilizar la consola de IAM, la AWS CLI o la API de AWS para eliminar de forma manual el rol vinculado al servicio. Para ello, primero debe limpiar manualmente los recursos del rol vinculado a servicio y, a continuación, eliminarlo manualmente.

> **Note**
>
> Si el servicio de CloudTrail está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar un recurso que el rol AWSServiceRoleForCloudTrail está utilizando, puede elegir una de las siguientes opciones:

- Eliminar la Cuenta de AWS de la organización en Organizations.
- Actualizar el registro de seguimiento para que deje de ser un registro de seguimiento de organización. Para obtener más información, consulte Actualización de un registro de seguimiento.
- Actualice el almacén de datos de eventos para que deje de ser un almacén de datos de eventos de la organización. Para obtener más información, consulte Actualización de un almacén de datos de eventos.

- Eliminar el registro de seguimiento. Para obtener más información, consulte Eliminación de un registro de seguimiento.
- Elimine el almacén de datos de eventos. Para obtener más información, consulte Eliminación de un almacén de datos de eventos.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForCloudTrail. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para roles vinculados a servicios de CloudTrail

CloudTrail permite el uso de roles vinculados a servicios en todas las Regiones de AWS en las que tanto CloudTrail como Organizations están disponibles. Para obtener más información, consulte los puntos de conexión de Servicio de AWS en la Referencia general de AWS.

Políticas administradas de AWS para AWS CloudTrail

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le brinden a su equipo solo los permisos necesarios. Para comenzar rápidamente, puede utilizar políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información acerca de las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos en las políticas administradas de AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada de AWS de ReadOnlyAccess proporciona acceso de solo

lectura a todos los servicios y recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripción de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Política administrada de AWS: **AWSCloudTrail_ReadOnlyAccess**

Una identidad de usuario que tenga adjuntada la política AWSCloudTrail_ReadOnlyAccess a su rol puede realizar acciones de solo lectura en CloudTrail, tales como las acciones `Get*`, `List*`, y `Describe*` en registros de seguimiento, almacenes de datos de eventos de CloudTrail Lake o consultas de Lake.

Política administrada de AWS: **AWSServiceRoleForCloudTrail**

La política CloudTrailServiceRolePolicy permite a AWS CloudTrail realizar acciones en los registros de seguimiento de la organización y en los almacenes de datos de eventos de la organización en su nombre. La política incluye los permisos de AWS Organizations necesarios para describir y enumerar las cuentas de la organización y los administradores delegados de una organización de AWS Organizations.

Esta política también incluye los permisos AWS Glue y AWS Lake Formation necesarios para deshabilitar la federación de Lake en el almacén de datos de eventos de una organización.

Esta política va adjunta a un rol vinculado a un servicio AWSServiceRoleForCloudTrail que permite a CloudTrail realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Actualizaciones de CloudTrail para las políticas administradas de AWS

Vea detalles sobre las actualizaciones de las políticas administradas de AWS para CloudTrail. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial del documento de CloudTrail.

Cambio	Descripción	Fecha
`CloudTrailServiceRolePolicy`: actualización de una política actual	Se actualizó la política para permitir las siguiente s acciones en el almacén	26 de noviembre de 2023

Cambio	Descripción	Fecha
	de datos de eventos de una organización cuando la federación está deshabilitada: • `glue:DeleteTable` • `lakeformation:DeregisterResource`	
`AWSCloudTrail_ReadOnlyAccess`: actualización de una política actual	CloudTrail ha cambiado el nombre de la política `AWSCloudTrailReadOnlyAccess` por `AWSCloudTrail_ReadOnlyAccess`. Además, se ha reducido el alcance de los permisos de la política a acciones de CloudTrail. Ya no incluye permisos para acciones de Amazon S3, AWS KMS o AWS Lambda.	6 de junio de 2022
CloudTrail comenzó a realizar un seguimiento de los cambios	CloudTrail comenzó a realizar un seguimiento de los cambios de sus políticas administradas de AWS.	6 de junio de 2022

Validación de conformidad en AWS CloudTrail

Auditores externos evalúan la seguridad y la conformidad de AWS CloudTrail como parte de varios programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para saber si un servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

  > **Note**
  >
  > No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Guías de cumplimiento para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en AWS CloudTrail

La infraestructura global de AWS se compone de regiones de AWS y zonas de disponibilidad de AWS. Las regiones 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 tradicionales de centros de datos únicos o múltiples. Si tiene la necesidad específica de reproducir los archivos de registros de CloudTrail a mayores distancias geográficas, puede utilizar la reproducción entre regiones para los buckets de Amazon S3 del registro de seguimiento, que permite copiar objetos de manera automática y asíncrona entre buckets de distintas regiones de AWS.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, CloudTrail ofrece varias características que lo ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

Registros de seguimiento y almacenes de datos de eventos que registran eventos en todas las regiones de AWS

Cuando se aplica un registro de seguimiento a todas las regiones de AWS, CloudTrail crea registros de seguimiento con una configuración idéntica en el resto de Regiones de AWS de la partición de AWS en la que trabaja. Cuando AWS añade una región, la configuración de ese registro de seguimiento se crea automáticamente en la nueva región.

Cuando crea un almacén de datos de eventos de varias regiones, CloudTrail recopila los eventos que se producen en todas las Regiones de AWS de su cuenta.

Control de versiones, configuración del ciclo de vida y protección del bloqueo de objetos para los datos de registro de CloudTrail

Dado que CloudTrail utiliza buckets de Amazon S3 para almacenar los archivos de registros, también es posible utilizar las características que proporciona Amazon S3 a fin de ayudar a satisfacer las necesidades de resiliencia y copia de seguridad de datos. Para obtener más información, consulte Resiliencia en Amazon S3.

Seguridad de la infraestructura en AWS CloudTrail

Como se trata de un servicio administrado, AWS CloudTrail 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 obtener acceso a CloudTrail 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.

Las siguientes prácticas recomendadas sobre seguridad también tratan la seguridad de la infraestructura en CloudTrail:

- Considerar la posibilidad de utilizar puntos de enlace de Amazon VPC para el acceso de los registros de seguimiento.
- Considere la posibilidad de utilizar puntos de enlace de Amazon VPC para el acceso al bucket de Amazon S3. Para obtener más información, consulte Ejemplo de políticas de bucket para puntos de enlace de la VPC para Amazon S3.
- Identificar y auditar todos los buckets de Amazon S3 que contienen archivos de registros de CloudTrail. Considere la posibilidad de utilizar etiquetas para ayudar a identificar los registros de seguimiento de CloudTrail y los buckets de Amazon S3 que contienen archivos de registros de

CloudTrail. Esto permitirá utilizar grupos de recursos para los recursos de CloudTrail. Para obtener más información, consulte AWS Resource Groups.

Prevención del suplente confuso entre servicios

El problema del suplente confuso es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema del suplente confuso. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos para limitar los permisos que AWS CloudTrail concede a otro servicio para el recurso. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (`*`) para las partes desconocidas del ARN. Por ejemplo, `"arn:aws:cloudtrail:*:AccountID:trail/*"`. Cuando se incluye un comodín, también se debe utilizar el operador de condición `StringLike`.

El valor de `aws:SourceArn` debe ser el ARN del registro de seguimiento, el almacén de datos de eventos o el canal que utiliza el recurso.

En el siguiente ejemplo se muestra cómo se pueden utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en CloudTrail para evitar el problema del adjunto confundido: Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake.

Mejores prácticas de seguridad en AWS CloudTrail

AWS CloudTrail proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Temas

- CloudTrail prácticas recomendadas de seguridad policial
- CloudTrail prácticas recomendadas de seguridad preventiva

CloudTrail prácticas recomendadas de seguridad policial

Crear un registro de seguimiento

Para tener un registro continuo de los eventos de tu AWS cuenta, debes crear un registro. Si bien CloudTrail proporciona información sobre el historial de eventos de 90 días para gestionar los eventos en la CloudTrail consola sin crear un registro, no es un registro permanente y no proporciona información sobre todos los tipos de eventos posibles. Para disponer de un registro continuado con todos los tipos de eventos que especifique, debe crear un registro de seguimiento, que envía los archivos de registros al bucket de Amazon S3 que especifique.

Para ayudar a administrar sus CloudTrail datos, considere la posibilidad de crear un registro que registre todos los eventos de administración y Regiones de AWS, a continuación, crear registros adicionales que registren tipos de eventos específicos para los recursos, como la actividad o AWS Lambda las funciones del bucket de Amazon S3.

Estas son algunas de las acciones que puede realizar:

- Crear una traza para su cuenta de AWS .
- Crear una traza para una organización.

Aplica rutas a todos Regiones de AWS

Para obtener un registro completo de los eventos registrados por una identidad o servicio de IAM en su AWS cuenta, cada ruta debe configurarse para registrar todos Regiones de AWS los eventos. Al registrar todos los eventos Regiones de AWS, se asegura de que se registren todos los eventos

que se produzcan en su AWS cuenta, independientemente de la AWS región en la que se hayan producido. Esto incluye el registro de los eventos del servicio global, que se registran en una AWS región específica de ese servicio. Cuando crea un registro que se aplica a todas las regiones, CloudTrail registra los eventos en cada región y envía los archivos de registro de CloudTrail eventos a un depósito de S3 que especifique. Si se agrega una región de AWS después de crear un registro de seguimiento que se aplica a todas las regiones, la región nueva se incluye automáticamente, y también se registran sus eventos. Esta es la opción predeterminada al crear una ruta en la CloudTrail consola.

Estas son algunas de las acciones que puede realizar:

- Crear una traza para su cuenta de AWS .
- Actualizar una traza existente para registrar los eventos de todas las Regiones de AWS.
- Implemente controles de detección continuos para garantizar que todos los senderos creados registren todos los eventos Regiones de AWS utilizando la regla multi-region-cloud-trailde activación. AWS Config

Habilite la CloudTrail integridad del archivo de registro

Los archivos de registro validados son especialmente valiosos para las investigaciones de seguridad y forenses. Por ejemplo, un archivo de registro validado le permite afirmar positivamente que el archivo de registro en sí no ha cambiado, o que determinadas credenciales de identidad de IAM han llevado a cabo una actividad de la API específica. El proceso de validación de la integridad del archivo de CloudTrail registro también le permite saber si un archivo de registro se ha eliminado o modificado, o bien afirma que no se ha enviado ningún archivo de registro a su cuenta durante un período de tiempo determinado. CloudTrail La validación de la integridad de los archivos de registro utiliza algoritmos estándares del sector: el SHA-256 para el uso de hash y el SHA-256 con RSA para la firma digital. Esto hace que sea inviable desde el punto de vista computacional modificar, eliminar o falsificar los archivos de registro sin ser detectados. CloudTrail Para obtener más información, consulte Activación de la validación y los archivos de validación.

Integración con Amazon CloudWatch Logs

CloudWatch Los registros le permiten monitorear y recibir alertas sobre eventos específicos capturados por CloudTrail. Los eventos que se envían a los CloudWatch registros son aquellos configurados para que los registre su ruta, así que asegúrese de haber configurado su ruta o senderos para registrar los tipos de eventos (eventos de gestión o eventos de datos) que le interesa monitorear.

Por ejemplo, puede supervisar los principales eventos de seguridad y de administración relacionados con la red, como los errores de inicio de AWS Management Console sesión.

Estas son algunas de las acciones que puede realizar:

- Consulte las integraciones de CloudWatch Logs de ejemplo para. CloudTrail
- Configura tu ruta para enviar eventos a CloudWatch Logs.
- Considere la posibilidad de implementar controles de detección continuos para garantizar que todos los rastros envíen los eventos a CloudWatch Logs para que los supervisen mediante la cloud-trail-cloud-watchregla -logs-enabled de AWS Config

Uso AWS Security Hub

Supervise su uso en lo que CloudTrail respecta a las mejores prácticas de seguridad mediante el uso de. AWS Security Hub Security Hub utiliza controles de seguridad de detección 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 CloudTrail los recursos, consulte AWS CloudTrail los controles en la Guía del AWS Security Hub usuario.

CloudTrail prácticas recomendadas de seguridad preventiva

Las siguientes prácticas recomendadas CloudTrail pueden ayudar a prevenir incidentes de seguridad.

Efectuar el registro en un bucket de Amazon S3 dedicado y centralizado

CloudTrail Los archivos de registro son un registro de auditoría de las acciones realizadas por una identidad de IAM o un AWS servicio. La integridad, plenitud y disponibilidad de estos registros es fundamental para fines forenses y de auditoría. Al efectuar el registro en un bucket de Amazon S3 dedicado y centralizado, es posible aplicar controles de seguridad, acceso y separación de funciones estrictos.

Estas son algunas de las acciones que puede realizar:

- Cree una AWS cuenta independiente como cuenta de archivo de registros. Si la usa AWS Organizations, inscriba esta cuenta en la organización y considere la posibilidad de crear un registro de la organización para registrar los datos de todas AWS las cuentas de su organización.

- Si no usa Organizations pero desea registrar los datos de varias AWS cuentas, cree un registro para registrar la actividad en esta cuenta de archivo de registros. Restringir el acceso a esta cuenta únicamente a los usuarios administrativos de confianza que necesiten acceso a los datos de auditoría y de la cuenta.
- Como parte de la creación de una ruta, ya sea una ruta de la organización o una ruta para una sola AWS cuenta, cree un bucket de Amazon S3 dedicado para almacenar los archivos de registro de esta ruta.
- Si desea registrar la actividad de más de una AWS cuenta, modifique la política de bucket para permitir el registro y el almacenamiento de los archivos de registro de todas las AWS cuentas en las que desee registrar la actividad de la AWS cuenta.
- Si no utiliza un registro de seguimiento de organización, cree registros de seguimiento en todas sus cuentas de AWS y especifique el bucket de Amazon S3 en la cuenta de archivos de registro.

Usa el cifrado del lado del servidor con claves administradas AWS KMS

De forma predeterminada, los archivos de registro que se envían CloudTrail al bucket de S3 se cifran mediante el cifrado del lado del servidor con una clave KMS (SSE-KMS). Para usar SSE-KMS CloudTrail, debe crear y administrar una AWS KMS key, también conocida como clave KMS.

> **Note**
>
> Si utiliza SSE-KMS y la validación de archivos de registro, y ha modificado la política de bucket de Amazon S3 para permitir exclusivamente archivos cifrados mediante SSE-KMS, no podrá crear registros de seguimiento que utilicen dicho bucket a menos que modifique la política de bucket para permitir el cifrado AES256 específicamente, tal y como se muestra en el siguiente ejemplo de línea de política.
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

Estas son algunas de las acciones que puede realizar:

- Conocer las ventajas de cifrar los archivos de registro con SSE-KMS.
- Cree una clave de KMS para utilizarla para el cifrado de archivos de registro.
- Configurar el cifrado de los archivos de registro para los registros de seguimiento.

- Considere la posibilidad de implementar controles de detección continuos para garantizar que todos los registros cifren los archivos de registro con SSE-KMS siguiendo la regla que aparece en. cloud-trail-encryption-enabled AWS Config

Agregar una clave de condición a la política de temas de Amazon SNS predeterminada

Al configurar una ruta para enviar notificaciones a Amazon SNS, CloudTrail agrega una declaración de política a la política de acceso a un tema de SNS que permite enviar contenido CloudTrail a un tema de SNS. Como práctica recomendada de seguridad, le recomendamos que añada una clave de condición `aws:SourceArn` (u opcionalmente`aws:SourceAccount`) a la CloudTrail declaración de política. Esto ayuda a evitar el acceso no autorizado de la cuenta al tema de SNS. Para obtener más información, consulte Política temática de Amazon SNS para CloudTrail.

Implementar el acceso con privilegios mínimos a los buckets de Amazon S3 en los que se almacenan los archivos de registro

CloudTrail rastrea los eventos del registro hasta un bucket de Amazon S3 que especifique. Estos archivos de registro contienen un registro de auditoría de las acciones realizadas por las identidades y los AWS servicios de IAM. La integridad y plenitud de estos archivos de registro son fundamentales para fines forenses y de auditoría. Para garantizar esa integridad, debe cumplir con el principio de privilegios mínimos al crear o modificar el acceso a cualquier bucket de Amazon S3 utilizado para almacenar archivos de CloudTrail registro.

Siga estos pasos:

- Examinar la política de bucket de Amazon S3 de todos y cada uno de los buckets en los que se almacenan los archivos de registro y ajustarla si es necesario para eliminar cualquier acceso innecesario. Esta política de bucket se generará automáticamente si crea un registro mediante la CloudTrail consola, pero también se puede crear y administrar manualmente.
- Como práctica recomendada de seguridad, asegúrese de agregar manualmente una clave de condición `aws:SourceArn` de la política de bucket. Para obtener más información, consulte Política de bucket de Amazon S3 para CloudTrail.
- Si utiliza el mismo depósito de Amazon S3 para almacenar los archivos de registro de varias AWS cuentas, siga las instrucciones para recibir los archivos de registro de varias cuentas.
- Si utiliza un registro de seguimiento de organización, no olvide seguir las instrucciones de los registros de seguimiento de organización y examine la política de ejemplo para un bucket de Amazon S3 para el registro de seguimiento de una organización en Crear un registro para una organización con AWS Command Line Interface.

- Consulte la documentación de seguridad de Amazon S3 y la explicación de ejemplo para proteger un bucket.

Habilitar la función de eliminación de la MFA en el bucket de Amazon S3 en el que se almacenan los archivos de registro

Al configurar la autenticación multifactor (MFA), cualquier intento de cambiar el estado de control de versiones del bucket o de eliminar una versión de un objeto requiere una autenticación adicional. De esta forma, incluso si un usuario consigue la contraseña de un usuario de IAM que tenga permisos para eliminar objetos de Amazon S3 de forma definitiva, todavía puede impedir cualquier operación que podría poner en peligro los archivos de registro.

Estas son algunas de las acciones que puede realizar:

- Consulte la guía de eliminación de MFA en la Guía del usuario de Amazon Simple Storage Service.
- Agregue una política de bucket de Amazon S3 que requiera el uso de la MFA.

> **Note**
>
> No se puede utilizar la eliminación de MFA con configuraciones del ciclo de vida. Para obtener más información sobre las configuraciones del ciclo de vida y cómo interactúan con otras configuraciones, consulte Configuraciones del ciclo de vida y otras configuraciones de buckets en la Guía del usuario de Amazon Simple Storage Service.

Configurar la gestión del ciclo de vida de los objetos en el bucket de Amazon S3 en el que se almacenan los archivos de registro

La CloudTrail ruta predeterminada es almacenar los archivos de registro de forma indefinida en el bucket de Amazon S3 configurado para la ruta. Puede utilizar las reglas de administración del ciclo de vida de los objetos de Amazon S3 para definir la política de retención que mejor se adapte a sus necesidades empresariales y de auditoría. Por ejemplo, es posible que desee archivar los archivos de registro que tengan más de un año de antigüedad en Amazon Glacier, o eliminar archivos de registro transcurrido un cierto tiempo.

> **Note**
>
> No se admite la configuración del ciclo de vida en buckets habilitados para autenticación multifactor (MFA).

Limite el acceso a la política AWSCloudTrail_FullAccess

Los usuarios con la AWSCloudTrail_FullAccesspolítica tienen la posibilidad de deshabilitar o reconfigurar las funciones de auditoría más sensibles e importantes de sus AWS cuentas. Esta política no pretende compartirse ni aplicarse ampliamente a las identidades de IAM de su AWS cuenta. Limite la aplicación de esta política al menor número posible de personas, es decir, aquellas que espere que actúen como administradores de la AWS cuenta.

Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS)

De forma predeterminada, los archivos de registro que envía CloudTrail a su depósito se cifran mediante el cifrado del lado del servidor con una clave KMS (SSE-KMS). Si no habilitas el cifrado SSE-KMS, tus registros se cifrarán mediante el cifrado SSE-S3.

> **Note**
>
> La habilitación del cifrado del lado del servidor cifra los archivos de registros, pero no los archivos de resumen, con SSE-KMS. Los archivos de resumen se cifran con claves de cifrado administradas por Amazon S3 (SSE-S3).
> Si utiliza un bucket de S3 existente con una clave de bucket de S3, CloudTrail debe tener permiso en la política de claves para utilizar las acciones y. AWS KMS `GenerateDataKey` `DescribeKey` Si `cloudtrail.amazonaws.com` no tiene estos permisos en la política de claves, no se puede crear ni actualizar un registro de seguimiento.

Para usar SSE-KMS CloudTrail, debe crear y administrar una clave KMS, también conocida como. AWS KMS key Adjunta una política a la clave que determina qué usuarios pueden utilizarla para cifrar y descifrar CloudTrail los archivos de registro. El proceso de descifrado transcurre de manera fluida a través de S3. Cuando los usuarios autorizados de la clave leen los archivos de CloudTrail

registro, S3 gestiona el descifrado y los usuarios autorizados pueden leer los archivos de registro sin cifrar.

Este enfoque tiene las siguientes ventajas:

- Puede crear y administrar las claves de cifrado KMS usted mismo.
- Puede utilizar una única clave de KMS para cifrar y descifrar los archivos de registros de varias cuentas en todas las regiones.
- Usted controla quién puede usar su clave para cifrar y descifrar CloudTrail los archivos de registro. Puede asignar permisos para la clave a los usuarios de su organización, según sus requisitos.
- Aumenta la seguridad. Con esta característica, se necesitan los siguientes permisos para poder leer archivos de registros:
  - Un usuario debe tener permisos de lectura de S3 para el bucket que contiene los archivos de registro.
  - También se debe aplicar a un usuario una política o un rol que la política de la clave de KMS conceda permisos de descifrado.
- Como S3 descifra automáticamente los archivos de registro para las solicitudes de los usuarios autorizados a usar la clave KMS, el cifrado SSE-KMS de los archivos de CloudTrail registro es compatible con versiones anteriores de las aplicaciones que leen datos de registro. CloudTrail

> **Note**
>
> La clave de KMS que elija debe crearse en la misma AWS región que el bucket de Amazon S3 que recibe los archivos de registro. Por ejemplo, si los archivos de registros se almacenarán en un bucket en la región EE. UU. Este (Ohio), debe crear o elegir una clave de KMS que se haya creado en esa región. Para verificar la región a la que pertenece un bucket de Amazon S3, consulte sus propiedades en la consola de Amazon S3.

Activación del cifrado de los archivos de registro

> **Note**
>
> Si crea una clave de KMS en la CloudTrail consola, CloudTrail añade automáticamente las secciones de política clave de KMS necesarias. Siga estos procedimientos si ha creado una

clave en la consola de IAM o AWS CLI si necesita añadir manualmente las secciones de política necesarias.

Para habilitar el cifrado SSE-KMS para los archivos de CloudTrail registro, lleve a cabo los siguientes pasos de alto nivel:

1. Creación de una clave de KMS.

   - Para obtener información sobre cómo crear una clave KMS con AWS Management Console, consulte Creación de claves en la Guía para AWS Key Management Service desarrolladores.
   - Para obtener información sobre cómo crear una clave KMS con AWS CLI, consulte create-key.

   > **Note**
   >
   > La clave de KMS que elija debe estar en la misma región que el bucket de S3 que recibe los archivos de registros. Para verificar la región a la que pertenece un bucket de S3, inspecciones las propiedades del bucket en la consola de S3.

2. Agregue secciones de políticas a la clave que permitan cifrar y CloudTrail a los usuarios descifrar los archivos de registro.

   - Para obtener información sobre qué es lo que debe incluir en la política, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

     > **Warning**
     >
     > Asegúrese de incluir permisos de descifrado en la política para todos los usuarios que necesitan leer archivos de registro. Si no realiza este paso antes de añadir la clave a la configuración del registro de seguimiento, los usuarios que no dispongan de permisos de descifrado no podrán leer archivos cifrados hasta que les conceda esos permisos.

   - Para obtener más información sobre cómo editar una política con la consola de IAM, consulte Edición de una política de claves en la Guía para desarrolladores AWS Key Management Service .

- Para obtener información sobre cómo adjuntar una política a una clave de KMS con el AWS CLI, consulte. put-key-policy

3. Actualice su ruta para usar la clave de KMS cuya política modificó. CloudTrail

   - Para actualizar la configuración de su ruta mediante la CloudTrail consola, consulteActualización de un recurso para que utilice su clave de KMS.
   - Para actualizar la configuración de su sendero mediante el AWS CLI, consulteHabilitar y deshabilitar el cifrado de archivos de registros de CloudTrail con la AWS CLI.

CloudTrail también admite claves AWS KMS multirregionales. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en la Guía para desarrolladores de AWS Key Management Service .

En la siguiente sección, se describen las secciones de política con CloudTrail las que debe utilizarse su política de claves de KMS.

Conceder permisos para crear una clave de KMS

Puede conceder permiso a los usuarios para crear una AWS KMS key con la política `AWSKeyManagementServicePowerUser`.

Para conceder permiso para crear una clave de KMS

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Elija el usuario o grupo al que desea conceder permiso.
3. Elija Permissions y, a continuación, seleccione Attach Policy.
4. Busque AWSKeyManagementServicePowerUser, elija la política y después elija Attach policy (Adjuntar política).

   El usuario ahora tiene permiso para crear una clave de KMS. Si desea crear políticas personalizadas para los usuarios, consulte Creación de políticas administradas por el cliente en la Guía del usuario de IAM.

Configurar políticas de clave de AWS KMS para CloudTrail

Puede crear una AWS KMS key de tres maneras:

- En la consola de CloudTrail
- La consola de administración de AWS
- Con la AWS CLI

> **Note**
>
> Si crea una clave de KMS en la consola de CloudTrail, CloudTrail agrega la política de claves de KMS necesaria. No es necesario que añada manualmente las instrucciones de política. Consulte Política de claves de KMS predeterminada creada en la consola de CloudTrail.

Si crea una clave de KMS en la administración de AWS o la AWS CLI, debe agregar secciones de política a la clave para poder usarla con CloudTrail. La política debe permitir que CloudTrail utilice la clave para cifrar los archivos de registro y los almacenes de datos de eventos. También debe permitir que los usuarios especificados lean archivos de registro en formato no cifrado.

Consulte los siguientes recursos:

- Para crear una clave de KMS con la AWS CLI, consulte create-key.
- Para editar una política de claves de KMS para CloudTrail, consulteEdición de una política de claves en la AWS Key Management Service Guía para desarrolladores.
- Para obtener detalles técnicos sobre cómo CloudTrail utiliza AWS KMS, consulte ¿Cómo AWS CloudTrail utiliza AWS KMS? en la Guía para desarrolladores de AWS Key Management Service.

Secciones de política de clave de KMS necesarias para utilizar con CloudTrail

Si creó una clave de KMS con la consola de administración de AWS o la AWS CLI , debe agregar, como mínimo, las siguientes instrucciones a la política de claves de KMS para que funcione con CloudTrail.

Temas

- Elementos de política de clave de KMS necesarios para los registros de seguimiento
- Elementos de política de clave de KMS necesarios para los almacenes de datos de eventos

Elementos de política de clave de KMS necesarios para los registros de seguimiento

1. Habilitar los permisos de cifrado de registros de CloudTrail. Consulte Concesión de permisos de cifrado.
2. Habilite los permisos de descifrado de registros de CloudTrail Consulte Concesión de permisos de descifrado. Si está utilizando un bucket de S3 existente con una Clave de bucket de S3, los permisos `kms:Decrypt` son necesarios para crear o actualizar un registro de seguimiento con el cifrado SSE-KMS habilitado.
3. Habilite CloudTrail para describir las propiedades de la clave de KMS. Consulte Habilitar CloudTrail para describir las propiedades de la clave de KMS.

Como práctica recomendada de seguridad, agregue una clave de condición `aws:SourceArn` a la política de claves de KMS. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que CloudTrail utilice la clave KMS solo para una traza o trazas específicas. El valor de `aws:SourceArn` siempre es el ARN de traza (o matriz de ARN de traza) que utiliza la clave KMS. Asegúrese de agregar la clave de condiciones `aws:SourceArn` de las políticas clave de KMS para las trazas existentes.

La clave de condición `aws:SourceAccount` también se admite, aunque no se recomienda. El valor de `aws:SourceAccount` es el ID de cuenta del propietario del traza, para las trazas de la organización, el ID de cuenta de administración.

> **Important**
>
> Cuando agregue las secciones nuevas a su política de clave de KMS, no cambie las secciones existentes en la política.
> Si el cifrado está habilitado en un registro de traza y la clave de KMS está deshabilitada o la política de claves de KMS no está correctamente configurada para CloudTrail, CloudTrail no enviará archivos de registros.

Elementos de política de clave de KMS necesarios para los almacenes de datos de eventos

1. Habilitar los permisos de cifrado de registros de CloudTrail. Consulte Concesión de permisos de cifrado.
2. Habilite los permisos de descifrado de registros de CloudTrail Consulte Concesión de permisos de descifrado.

3. Conceda permiso a los usuarios y a los roles para cifrar y descifrar datos del almacén de datos de eventos con la clave de KMS.

   Tanto para crear un almacén de datos de eventos y cifrarlo con una clave de KMS como para ejecutar consultas en un almacén de datos de eventos que esté cifrando con una clave de KMS, debe tener acceso de escritura a la clave de KMS. La política de clave de KMS debe tener acceso a CloudTrail, y los usuarios que ejecuten operaciones (como consultas) en el almacén de datos de eventos deben contar con la posibilidad de administrar la clave de KMS.
4. Habilite CloudTrail para describir las propiedades de la clave de KMS. Consulte Habilitar CloudTrail para describir las propiedades de la clave de KMS.

Las claves de condición `aws:SourceArn` y `aws:SourceAccount` no se admiten en las políticas de claves de KMS para los almacenes de datos de eventos.

> **Important**
>
> Cuando agregue las secciones nuevas a su política de clave de KMS, no cambie las secciones existentes en la política.
> Si el cifrado está habilitado en un almacén de datos de eventos y la clave de KMS está desactivada o eliminada, o bien, si la política de clave de KMS no está configurada correctamente para CloudTrail, dicho servicio no podrá enviar eventos al almacén de datos de eventos.

Concesión de permisos de cifrado

Example Permita a CloudTrail cifrar archivos de registros en nombre de cuentas específicas.

CloudTrail necesita permisos explícitos para utilizar la clave de KMS para cifrar archivos de registros en nombre de cuentas específicas. Para especificar una cuenta, agregue la siguiente declaración necesaria a su política de claves de KMS y reemplace *`account-id`*, *`region`* y *`trailName`* por los valores apropiados para su configuración. Puede agregar identificadores de cuenta adicionales a la sección `EncryptionContext` para permitir que esas cuentas utilicen CloudTrail para emplear su clave de KMS a fin de cifrar archivos de registros.

Como práctica recomendada de seguridad, agregue una clave de condición `aws:SourceArn` a la política de clave de KMS para un registro de seguimiento. La clave de condición global de IAM

`aws:SourceArn` ayuda a garantizar que CloudTrail utilice la clave KMS solo para una traza o trazas específicas.

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
         "StringLike": {
             "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
         }
    }
}
```

La política de una clave de KMS utilizada para cifrar los registros del almacén de datos de eventos de CloudTrail Lake no puede usar las claves de condición `aws:SourceArn` y `aws:SourceAccount`. A continuación, se muestra un ejemplo de política de una clave de KMS para un almacén de datos de eventos.

```
{
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

La siguiente instrucción de política de ejemplo ilustra cómo otra cuenta puede utilizar su clave de KMS para cifrar archivos de registros de CloudTrail.

Escenario

- Su clave de KMS está en la cuenta *111111111111*.
- Usted y la cuenta *222222222222* cifrarán los archivos de registro.

En la política, agrega una o varias cuentas que se cifran con la clave en EncryptionContext de CloudTrail. Esto impide a CloudTrail utilizar la clave para cifrar registros solo para las cuentas que especifique. Cuando concede permiso a la raíz de la cuenta *222222222222* para cifrar registros, delega el permiso al administrador de la cuenta para cifrar los permisos necesarios a otros usuarios de esa cuenta. Para ello, el administrador de la cuenta cambia las políticas asociadas a esos usuarios de IAM.

Como práctica recomendada de seguridad, agregue una clave de condición `aws:SourceArn` a la política de claves de KMS. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que CloudTrail utilice la clave de KMS solo para los registros de seguimiento específicos. Esta condición no se admite en las políticas de claves de KMS para los almacenes de datos de eventos.

Instrucción de la política de claves de KMS:

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
```

```
    }
  }
}
```

Para obtener más información sobre cómo editar una política de claves de KMS para utilizarla con CloudTrail, consulte Edición de una política de claves en la Guía para desarrolladores de AWS Key Management Service.

Concesión de permisos de descifrado

Antes de agregar su clave de KMS a la configuración de CloudTrail, es importante que conceda permisos de descifrado a todos los usuarios que los necesiten. Los usuarios que tienen permisos de cifrado, pero no permisos de descifrado no pueden leer los registros cifrados. Si está utilizando un bucket de S3 existente con una Clave de bucket de S3, los permisos `kms:Decrypt` son necesarios para crear o actualizar un registro de seguimiento con el cifrado SSE-KMS habilitado.

Habilitar los permisos de descifrado de registros de CloudTrail

Los usuarios de su clave deben tener permisos explícitos para leer los archivos de registros que CloudTrail ha cifrado. Para habilitar a los usuarios para que puedan leer archivos de registros cifrados, agregue la siguiente instrucción necesaria a su política de claves de KMS y modifique la sección `Principal` para agregar una línea para cada entidad principal a la que desee permitir descifrar con su clave de KMS.

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

El siguiente es un ejemplo de política que se requiere para permitir que la entidad principal del servicio CloudTrail descifre los registros de seguimiento.

```
{
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

La política de descifrado de una clave de KMS que se utiliza con un almacén de datos de eventos de CloudTrail Lake es similar a la siguiente. Los ARN de usuario o rol especificados como valores para `Principal` necesitan permisos de descifrado para crear o actualizar almacenes de datos de eventos, ejecutar consultas u obtener los resultados de las consultas.

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

El siguiente es un ejemplo de política que se requiere para permitir que la entidad principal del servicio CloudTrail descifre los registros del almacén de datos de eventos.

```
{
      "Sid": "Allow CloudTrail to decrypt an event data store",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Permitir a los usuarios de su cuenta descifrar los registros de seguimiento con su clave de KMS

Ejemplo

Esta instrucción de política ilustra cómo permitir que un usuario o un rol de su cuenta use su clave para leer registros cifrados en el bucket de S3 de su cuenta.

Example Escenario

- Su clave de KMS, el bucket de S3 y el usuario de IAM Bob están en la cuenta *111111111111*.
- Concede al usuario de IAM, Bob, permiso para descifrar los registros de CloudTrail en el bucket de S3.

En la política de claves, habilita los permisos de descifrado de registros de CloudTrail para el usuario de IAM, Bob.

Instrucción de la política de claves de KMS:

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Permitir a los usuarios de otras cuentas descifrar los registros de seguimiento con su clave de KMS

Puede permitir que los usuarios de otras cuentas utilicen su clave de KMS para descifrar registros de seguimiento, pero no los registros del almacén de datos de eventos. Los cambios necesarios en su política de claves dependen de si el bucket de S3 se encuentra en su cuenta o en otra cuenta.

Permitir a los usuarios de un bucket de otra cuenta descifrar archivos de registro

Ejemplo

Esta instrucción de política ilustra cómo permitir que un usuario o un rol de IAM de otra cuenta use su clave para leer archivos de registro cifrados de un bucket de S3 de la otra cuenta.

Escenario

- Su clave de KMS está en la cuenta *111111111111*.
- El usuario de IAM Alice y el bucket de S3 se encuentran en la cuenta *222222222222*.

En este caso, concede permiso a CloudTrail para descifrar los registros de la cuenta *222222222222* y concede permiso a la política del usuario de IAM Alice para utilizar su clave *KeyA*, que se encuentra en la cuenta *111111111111*.

Instrucción de la política de claves de KMS:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Instrucción de política de la usuaria de IAM Alice:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
```

```
}
```

Permitir a los usuarios de otra cuenta descifrar los registros de seguimiento de su bucket

Example

Esta política ilustra cómo otra cuenta puede utilizar su clave para leer archivos de registro cifrados de su bucket de S3.

Example Escenario

- Su clave de KMS y el bucket de S3 se encuentran en la cuenta *111111111111*.
- El usuario que lee registros del bucket está en la cuenta *222222222222*.

Para permitir este escenario, habilite los permisos de cifrado para el rol de IAM CloudTrailReadRole de su cuenta y, a continuación, conceda a la otra cuenta permiso para asumir ese rol.

Instrucción de la política de claves de KMS:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Instrucción de política de entidad de confianza CloudTrailReadRole:

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
```

```
    "Sid": "Allow CloudTrail access",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::222222222222:root"
    },
    "Action": "sts:AssumeRole"
   }
  ]
 }
```

Para obtener más información sobre cómo editar la política de una clave de KMS para utilizarla con CloudTrail, consulte Editing a Key Policy (Edición de la política de una clave) en la Guía para desarrolladores de AWS Key Management Service.

Habilitar CloudTrail para describir las propiedades de la clave de KMS

CloudTrail requiere la capacidad para describir las propiedades de la clave de KMS. Para habilitar esta funcionalidad, agregue la siguiente instrucción necesaria tal cual está a su política de claves de KMS. Esta instrucción no concede a CloudTrail ningún permiso distinto de los permisos que usted especifique.

Como práctica recomendada de seguridad, agregue una clave de condición `aws:SourceArn` a la política de claves de KMS. La clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que CloudTrail utilice la clave KMS solo para una traza o trazas específicas.

```
{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Para obtener más información sobre cómo editar políticas de claves de KMS, consulte Edición de una política de claves en la Guía para desarrolladores de AWS Key Management Service.

Política de claves de KMS predeterminada creada en la consola de CloudTrail

Si crea una AWS KMS key en la consola de CloudTrail, se crean automáticamente las siguientes políticas. La política concede estos permisos:

- Concede a la Cuenta de AWS (raíz) permisos para la clave de KMS.
- Permite a CloudTrail cifrar archivos de registros con la clave de KMS y describir la clave de KMS.
- Permite que todos los usuarios de las cuentas especificadas descifren archivos de registro.
- Permite que todos los usuarios de la cuenta especificada creen un alias de KMS para la clave de KMS.
- Habilita el descifrado de registros entre cuentas para el ID de la cuenta que creó el registro de seguimiento.

Temas

- Política de clave de KMS predeterminada para almacenes de datos de eventos de CloudTrail Lake
- Política de clave de KMS predeterminada para registros de seguimiento

Política de clave de KMS predeterminada para almacenes de datos de eventos de CloudTrail Lake

La siguiente es la política predeterminada que se crea para una AWS KMS key que usa con un almacén de datos de eventos en CloudTrail Lake.

```
{
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores. Created
 ${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
```

```
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

Política de clave de KMS predeterminada para registros de seguimiento

La siguiente es la política predeterminada que se crea para una AWS KMS key que usa con un registro de seguimiento.

> **Note**
>
> La política incluye una instrucción por la que se permite descifrar archivos de registro entre cuentas con la clave de KMS.

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:root",
                    "arn:aws:iam::account-id:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
```

```
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
```

```
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        }
    ]
}
```

Actualización de un recurso para que utilice su clave de KMS

En la consola de AWS CloudTrail, actualice un registro de seguimiento o un almacén de datos de eventos para que utilicen una clave de AWS Key Management Service. Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. Para obtener más información, consulte Precios de AWS Key Management Service.

Temas

- Actualizar un registro de seguimiento para que utilice una clave de KMS
- Actualizar un almacén de datos de eventos para que utilice una clave de KMS

Actualizar un registro de seguimiento para que utilice una clave de KMS

Para actualizar un registro de seguimiento para utilizar la AWS KMS key que ha modificado para CloudTrail, siga los pasos que se describen a continuación en la consola de CloudTrail.

> **Note**
>
> La actualización de un registro de seguimiento mediante el siguiente procedimiento cifra los archivos de log, pero no los archivos de resumen, con SSE-KMS. Los archivos de resumen se cifran con claves de cifrado administradas por Amazon S3 (SSE-S3).
> Si está utilizando un bucket de S3 existente con una clave de bucket de S3, CloudTrail debe tener permiso en la política de claves para utilizar las acciones `GenerateDataKey` y `DescribeKey` de AWS KMS. Si `cloudtrail.amazonaws.com` no tiene estos permisos en la política de claves, no se puede crear ni actualizar un registro de seguimiento.

Para actualizar un registro de seguimiento utilizando la AWS CLI, consulte Habilitar y deshabilitar el cifrado de archivos de registros de CloudTrail con la AWS CLI.

Para actualizar un registro de seguimiento a fin de utilizar su clave de KMS

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. Elija Trails (Registros de seguimiento) y, a continuación, elija un nombre de registro de seguimiento.
3. En General details (Detalles generales), elijaEdit (Editar).
4. En Log file SSE-KMS encryption (Cifrado SSE-KMS de archivos de registro), elija Enabled (Habilitado) si desea cifrar sus archivos de registro con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los registros se cifrarán mediante el cifrado SSE-S3. Para obtener más información sobre el cifrado SSE-KMS, consulte Uso del cifrado del lado del servidor con AWS Key Management Service (SSE-KMS). Para obtener más información sobre el cifrado SSE-S3, consulte Uso de cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3).

   Elija Existing (Existente) para actualizar el registro de seguimiento con su AWS KMS key. Elija una clave de KMS que esté en la misma región que el bucket de S3 que recibe sus archivos de registros. Para verificar la región a la que pertenece un bucket de S3, consulte sus propiedades en la consola de S3.

   > **Note**
   >
   > También puede escribir el ARN de una clave de otra cuenta. Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS. La política de claves debe permitir que CloudTrail utilice la clave para cifrar los archivos de registros y que los usuarios especificados lean archivos de registros en formato no cifrado. Para obtener más información sobre cómo editar manualmente la política de claves, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

   En Alias de AWS KMS, especifique el alias para el que cambió la política para utilizarla con CloudTrail en el formato `alias/MiAlias`. Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS.

   Puede escribir el nombre del alias, el ARN o el ID de clave único global. Si la clave de KMS pertenece a otra cuenta, compruebe que la política de claves tenga los permisos que le permiten utilizarla. El valor puede tener uno de los siguientes formatos:

- Nombre del alias: `alias/MyAliasName`
- ARN del alias: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- ARN de la clave: `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de la clave único global: `12345678-1234-1234-1234-123456789012`

5. Elija Update trail (Actualizar registro de seguimiento).

> **Note**
>
> Si la clave de KMS que eligió está deshabilitada o pendiente de eliminación, no podrá guardar el registro de seguimiento con dicha clave de KMS. Puede habilitar la clave de KMS o elegir otra. Para obtener más información, consulte Estado de la clave: efecto en su clave de KMS en la Guía para desarrolladoresAWS Key Management Service.

Actualizar un almacén de datos de eventos para que utilice una clave de KMS

Para actualizar un almacén de datos de eventos para que utilice la AWS KMS key que se modificó para CloudTrail, siga los pasos que se describen a continuación en la consola de CloudTrail.

Para actualizar un almacén de datos de eventos con la AWS CLI, consulte Actualizar un almacén de datos de eventos con la AWS CLI.

> **Important**
>
> Si deshabilita o elimina la clave de KMS, o elimina los permisos de CloudTrail en la clave, evitará que CloudTrail incorpore eventos en el almacén de datos de eventos y que los usuarios consulten los datos del almacén que se cifró con la clave. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar. Antes de deshabilitar o eliminar una clave de KMS que se esté utilizando con un almacén de datos de eventos, elimínelo o haga una copia de seguridad de este.

Para actualizar un almacén de datos de eventos para que utilice su clave de KMS

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

2. En el panel de navegación, elija Event data stores (Almacenes de datos de eventos) en Lake. Elija un almacén de datos de eventos para actualizarlo.
3. En General details (Detalles generales), elijaEdit (Editar).
4. Si la opción Cifrado aún no está habilitada, seleccione Utilizar mi propia AWS KMS key para cifrar los archivos de registro con su propia clave de KMS.

   Elija Existing (Existente) para actualizar el almacén de datos de eventos con su clave de KMS. Seleccione una clave de KMS que esté en la misma región que el almacén de datos de eventos. No se admite el uso de una clave de otra cuenta.

   En Introduzca el alias de AWS KMS, especifique el alias para el que cambió la política para utilizarla con CloudTrail en el formato `alias/MiAlias`. Para obtener más información, consulte Actualización de un recurso para que utilice su clave de KMS.

   Puede elegir un alias o utilizar el ID global único de la clave. El valor puede tener uno de los siguientes formatos:

   - Nombre del alias: `alias/MyAliasName`
   - ARN del alias: `arn:aws:kms:region:123456789012:alias/MyAliasName`
   - ARN de la clave: `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
   - ID de la clave único global: `12345678-1234-1234-1234-123456789012`
5. Elija Save changes (Guardar cambios).

> **Note**
>
> Si la clave de KMS que eligió está deshabilitada o pendiente de eliminación, no podrá guardar la configuración del almacén de datos de eventos con dicha clave de KMS. Puede habilitar la clave de KMS o elegir una diferente. Para obtener más información, consulte Estado de la clave: efecto en su clave de KMS en la Guía para desarrolladoresAWS Key Management Service.

Habilitar y deshabilitar el cifrado de archivos de registros de CloudTrail con la AWS CLI

En este tema, se describe cómo habilitar y deshabilitar el cifrado SSE-KMS de archivos de registros para CloudTrail mediante la AWS CLI. Para obtener información general, consulte Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS).

Temas

- Habilitar el cifrado de los archivos de registros de CloudTrail mediante la AWS CLI
- Deshabilitar el cifrado de los archivos de registros de CloudTrail mediante la AWS CLI

Habilitar el cifrado de los archivos de registros de CloudTrail mediante la AWS CLI

- Habilitar el cifrado de archivos de registro para un registro de seguimiento
- Habilitar el cifrado de archivos de registro para un almacén de datos de eventos

Habilitar el cifrado de archivos de registro para un registro de seguimiento

1. Cree una clave con la AWS CLI. La clave que cree debe estar en la misma región que el bucket de S3 que recibe sus archivos de registros de CloudTrail. En este paso, utilice el comando de AWS KMS create-key.
2. Obtenga la política de claves existente para poder modificarla al utilizarla con CloudTrail. Puede recuperar la política de claves con el comando de AWS KMS get-key-policy.
3. Agregue las secciones necesarias a la política de claves para que CloudTrail pueda cifrar los archivos de registros y los usuarios puedan descifrarlos. Asegúrese de que todos los usuarios que van a leer los archivos de registro tengan permisos para descifrarlos. No modifique las secciones existentes de la política. Para obtener información acerca de las secciones de políticas que se deben incluir, consulte Configurar políticas de clave de AWS KMS para CloudTrail.
4. Adjunte el archivo de política JSON modificado a la clave ejecutando el comando de AWS KMS put-key-policy.
5. Ejecute el comando CloudTrail `create-trail` o `update-trail` con el parámetro `--kms-key-id`. Este comando habilita el cifrado de registros.

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

El parámetro `--kms-key-id` especifica la clave cuya política ha modificado para CloudTrail. Puede estar en alguno de los siguientes formatos:

- Nombre del alias Ejemplo: `alias/MyAliasName`
- ARN del alias Ejemplo: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- ARN de clave Ejemplo: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de la clave único global Ejemplo: `12345678-1234-1234-1234-123456789012`

A continuación, se muestra un ejemplo de respuesta:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "my-bucket-name"
}
```

La presencia del elemento `KmsKeyId` indica que se ha habilitado el cifrado de los archivos de registro. Los archivos de registro cifrados aparecerán en su bucket en 5 minutos aproximadamente.

Habilitar el cifrado de archivos de registro para un almacén de datos de eventos

1. Cree una clave con la AWS CLI. La clave que cree debe estar en la misma región que el almacén de datos de eventos. Para este paso, ejecute el comando de AWS KMS create-key.
2. Obtenga la política de claves existente para editarla y poder utilizarla con CloudTrail. Puede obtener la política de claves ejecutando el comando de AWS KMS get-key-policy.
3. Agregue las secciones necesarias a la política de claves para que CloudTrail pueda cifrar los archivos de registros y los usuarios puedan descifrarlos. Asegúrese de que todos los

usuarios que van a leer los archivos de registro tengan permisos para descifrarlos. No modifique las secciones existentes de la política. Para obtener información acerca de las secciones de políticas que se deben incluir, consulte Configurar políticas de clave de AWS KMS para CloudTrail.

4. Adjunte el archivo de política JSON modificado a la clave ejecutando el comando de AWS KMS put-key-policy.
5. Ejecute el comando `create-event-data-store` o `update-event-data-store` de CloudTrail y agregue el parámetro `--kms-key-id`. Este comando habilita el cifrado de registros.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

El parámetro `--kms-key-id` especifica la clave cuya política ha modificado para CloudTrail. Puede estar en uno de los siguientes cuatro formatos:

- Nombre del alias Ejemplo: `alias/MyAliasName`
- ARN del alias Ejemplo: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- ARN de clave Ejemplo: `arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID de la clave único global Ejemplo: `12345678-1234-1234-1234-123456789012`

A continuación, se muestra un ejemplo de respuesta:

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
```

```
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

La presencia del elemento `KmsKeyId` indica que se ha habilitado el cifrado de los archivos de registro. Los archivos de registro cifrados aparecerán en su almacén de datos de eventos en 5 minutos aproximadamente.

Deshabilitar el cifrado de los archivos de registros de CloudTrail mediante la AWS CLI

Para detener el cifrado de los registros en un registro de seguimiento, ejecute el comando `update-trail` y pase una cadena vacía al parámetro `kms-key-id`:

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

A continuación, se muestra un ejemplo de respuesta:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

La ausencia del valor `KmsKeyId` indica que el cifrado de los archivos de registro ya no está habilitado.

> **Important**
>
> No se puede detener el cifrado de archivos de registro en un almacén de datos de eventos.

Referencia de eventos de registro de CloudTrail

Un registro de CloudTrail es un registro en formato JSON. El registro contiene información acerca de las solicitudes de recursos de su cuenta como, por ejemplo, quién hizo la solicitud, los servicios utilizados, las acciones realizadas y los parámetros de la acción. Los datos de los eventos se encierran dentro de una matriz `Records`.

En el siguiente ejemplo, se muestra un registro único de un evento. En este caso, un usuario de IAM llamado `Mary_Major` ejecutó el comando aws cloudtrail start-logging para llamar a la acción `StartLogging` de CloudTrail a fin de iniciar el proceso de registro en un registro de seguimiento denominado `myTrail`.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
```

```
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

En el siguiente ejemplo, un usuario de IAM llamado `Paulo_Santos` ejecutó el comando aws cloudtrail start-event-data-store-ingestion para llamar a la acción `StartEventDataStoreIngestion` a fin de iniciar la ingesta en un almacén de datos de eventos.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
```

```
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Hay dos eventos registrados para mostrar actividad inusual en CloudTrail Insights: un evento inicial y un evento final. En el siguiente ejemplo se muestra un registro único de un evento de Insights que se produjo cuando se llamó un número inusual de veces a la API `CompleteLifecycleAction` de Auto Scaling de aplicaciones. Para los eventos de Insights, el valor de `eventCategory` es `Insight`. Un bloque `insightDetails` identifica el estado del evento, la fuente, el nombre, el tipo de información y el contexto, incluidas las estadísticas y atribuciones. Para obtener más información sobre el bloque `insightDetails`, consulte Elemento `insightDetails` CloudTrail Insights.

```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
```

```
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
```

```
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
                    }]
                }]
            }
        },
        "eventCategory": "Insight"
    }
```

En los siguientes temas se enumeran los campos de datos que CloudTrail captura para cada llamada a la API de AWS y para cada evento de inicio de sesión.

Temas

- CloudTrail contenido del registro
- CloudTrail Elemento UserIdentity
- Elemento insightDetails CloudTrail Insights
- Eventos no generados por la API capturados por CloudTrail

CloudTrail contenido del registro

El cuerpo del registro contiene campos que le ayudan a determinar la acción solicitada, así como cuándo y dónde se realizó la solicitud. Cuando el valor de Opcional es Verdadero, el campo solo está presente cuando se aplica al servicio, la API o el tipo de evento. Un valor Opcional de False (Falso) significa que el campo siempre está presente o que su presencia no depende del servicio, la API o el tipo de evento. Un ejemplo es `.responseElements`, que está presente en los eventos de acciones que realizan cambios (acciones de creación, actualización o eliminación).

CloudTrail trunca un campo si su contenido supera el tamaño máximo del campo. Si un campo está truncado, `omitted` está presente con un valor de `true`.

`eventTime`

La fecha y la hora en que se completó la solicitud, en hora universal coordinada (UTC). La marca temporal de un evento proviene del host local que proporciona el punto de enlace de API de servicio en el que se realizó la llamada a la API. Por ejemplo, un evento de CreateBucket API que se ejecute en la región EE.UU. Oeste (Oregón) obtendría su marca horaria a partir de la hora de

un AWS host que ejecute el punto de conexión Amazon S3,`s3.us-west-2.amazonaws.com`. En general, AWS los servicios utilizan el Network Time Protocol (NTP) para sincronizar los relojes del sistema.

Desde: 1.0

Opcional: Falso

`eventVersion`

La versión del formato del evento de registro. La versión actual es la 1.10.

El valor de `eventVersion` es una versión principal y secundaria con el formato *`major_version`*.*`minor_version`*. Por ejemplo, puede tener un valor `eventVersion` de `1.09`, donde `1` es la versión principal y `09` es la versión secundaria.

CloudTrail incrementa la versión principal si se realiza un cambio en la estructura de eventos que no es compatible con versiones anteriores. Esto incluye eliminar un campo JSON que ya existe o cambiar la forma en que se representa el contenido de un campo (por ejemplo, un formato de fecha). CloudTrail incrementa la versión secundaria si un cambio añade nuevos campos a la estructura del evento. Esto puede ocurrir si se proporciona información nueva para algunos o todos los eventos existentes o si la información nueva solo se proporciona para los tipos de eventos nuevos. Las aplicaciones deben ignorar los campos nuevos para mantener la compatibilidad con versiones secundarias de la estructura de eventos.

Si CloudTrail introduce nuevos tipos de eventos, pero la estructura del evento no cambia por lo demás, la versión del evento no cambia.

Para asegurarse de que las aplicaciones pueden analizar la estructura de eventos, le recomendamos que haga una comparación de igualdad con el número de la versión principal. Para asegurarte de que existen los campos esperados por la aplicación, también te recomendamos que realices una greater-than-or-equal comparación entre valores en la versión secundaria. No hay ceros a la izquierda en la versión secundaria. Puede interpretar tanto la *`major_version`* y la *`minor_version`* como números, y realizar operaciones de comparación.

Desde: 1.0

Opcional: Falso

`userIdentity`

Información sobre la identidad de IAM que hizo una solicitud. Para obtener más información, consulte CloudTrail Elemento UserIdentity.

Desde: 1.0

Opcional: Falso

`eventSource`

El servicio de para el que se realizó la solicitud. Este nombre suele ser una forma abreviada del nombre del servicio sin espacios más `.amazonaws.com`. Por ejemplo:

- AWS CloudFormation es`cloudformation.amazonaws.com`.
- Amazon EC2 es `ec2.amazonaws.com`.
- Amazon Simple Workflow Service es `swf.amazonaws.com`.

Esta convención tiene algunas excepciones. Por ejemplo, `eventSource` para Amazon CloudWatch es`monitoring.amazonaws.com`.

Desde: 1.0

Opcional: Falso

`eventName`

La acción solicitada, que es una de las acciones de la API para ese servicio.

Desde: 1.0

Opcional: Falso

`awsRegion`

El al Región de AWS que se hizo la solicitud, como`us-east-2`. Consulte CloudTrail regiones compatibles.

Desde: 1.0

Opcional: Falso

`sourceIPAddress`

La dirección IP desde la que se realizó la solicitud. Para las acciones que se originan desde la consola del servicio, la dirección registrada es para el recurso del cliente subyacente, no para el servidor web de la consola. En el caso de los servicios en AWS, solo se muestra el nombre DNS.

> **Note**
>
> En el caso de eventos originados por AWS, este campo es normalmente `AWS Internal/#`, donde `#` es un número usado para fines internos.

Desde: 1.0

Opcional: Falso

`userAgent`

El agente a través del cual se realizó la solicitud AWS Management Console, como un AWS servicio, los AWS SDK o el AWS CLI. Este campo tiene un tamaño máximo de 1 KB; el contenido que supere ese límite se trunca. A continuación se incluyen valores de ejemplo:

- `lambda.amazonaws.com`: la solicitud se realizó con AWS Lambda.
- `aws-sdk-java`: la solicitud se realizó con AWS SDK for Java.
- `aws-sdk-ruby`: la solicitud se realizó con AWS SDK for Ruby.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— La solicitud se realizó con el AWS CLI instalado en Linux.

> **Note**
>
> En el caso de eventos originados por AWS, este campo es normalmente `AWS Internal/#`, donde `#` es un número usado para fines internos.

Desde: 1.0

Opcional: Verdadero

`errorCode`

El error del AWS servicio si la solicitud devuelve un error. Para ver un ejemplo que muestra este campo, consulte Ejemplo de código de error y registro de mensajes. Este campo tiene un tamaño máximo de 1 KB; el contenido que supere ese límite se trunca.

Desde: 1.0

Opcional: Verdadero

`errorMessage`

Si la solicitud devuelve un error, la descripción del error. Este mensaje incluye mensajes sobre errores de autorización. CloudTrail captura el mensaje registrado por el servicio en su gestión de excepciones. Para ver un ejemplo, consulte Ejemplo de código de error y registro de mensajes. Este campo tiene un tamaño máximo de 1 KB; el contenido que supere ese límite se trunca.

> **Note**
>
> Algunos AWS servicios proporcionan los campos `errorCode` y `errorMessage` como campos de nivel superior en caso de que se trate. Otros servicios de AWS proporcionan información del error como parte de `responseElements`.

Desde: 1.0

Opcional: Verdadero

`requestParameters`

Los parámetros, si hay alguno, que se enviaron con la solicitud. Estos parámetros se documentan en la documentación de referencia de la API del AWS servicio correspondiente. Este campo tiene un tamaño máximo de 100 KB; el contenido que supere ese límite se trunca.

Desde: 1.0

Opcional: Falso

`responseElements`

El elemento de respuesta de las acciones que realizaron cambios (acciones de creación, actualización o eliminación). Si una acción no cambia el estado (por ejemplo, una solicitud para obtener o mostrar objetos), este elemento se omite. Estas acciones se documentan en la documentación de referencia de la API del AWS servicio correspondiente. Este campo tiene un tamaño máximo de 100 KB; el contenido que supere ese límite se trunca.

El `responseElements` valor es útil para ayudarte a rastrear una solicitud AWS Support. Ambos `x-amz-request-id` y `x-amz-id-2` contienen información que ayuda a rastrear una solicitud con AWS Support. Estos valores son los mismos que los que devuelve el servicio en respuesta a la solicitud que inicia los eventos, por lo que se pueden utilizar para emparejar el evento con la solicitud.

Desde: 1.0

Opcional: Falso

`additionalEventData`

Datos adicionales sobre el evento que no forman parte de la solicitud o la respuesta. Este campo tiene un tamaño máximo de 28 KB; el contenido que supere ese límite se trunca.

Desde: 1.0

Opcional: Verdadero

`requestID`

El valor que identifica la solicitud. El servicio al que se llama genera este valor. Este campo tiene un tamaño máximo de 1 KB; el contenido que supere ese límite se trunca.

Desde: 1.01

Opcional: Verdadero

`eventID`

GUID generado por CloudTrail para identificar de forma única cada evento. Puede utilizar este valor para identificar un evento individual. Por ejemplo, puede utilizar el ID como clave

principal para recuperar datos de archivos de registro de una base de datos que permita realizar búsquedas.

Desde: 1.01

Opcional: Falso

eventType

Identifica el tipo de evento que generó el registro del evento. Puede ser uno de los siguientes valores:

- `AwsApiCall`: se llamó a una API.
- `AwsServiceEvent`: el servicio generó un evento relacionado con su registro de seguimiento. Por ejemplo, esto puede ocurrir cuando otra cuenta realiza una llamada con un recurso de su propiedad.
- `AwsConsoleAction`: Se realizó una acción en la consola que no era una llamada a la API.
- `AwsConsoleSignIn`— Un usuario de tu cuenta (root, IAM, federado, SAML o SwitchRole) ha iniciado sesión en. AWS Management Console
- `AwsCloudTrailInsight`— Si los eventos de Insights están habilitados para el seguimiento, CloudTrail genera eventos de Insights cuando CloudTrail detecta una actividad operativa inusual, como picos en el aprovisionamiento de recursos o ráfagas de acciones (IAM). AWS Identity and Access Management

  Los eventos de `AwsCloudTrailInsight` no utilizan los siguientes campos:

  - `eventName`
  - `eventSource`
  - `sourceIPAddress`
  - `userAgent`
  - `userIdentity`

Desde: 1.02

Opcional: Falso

apiVersion

Identifica la versión de la API asociada con el valor de `AwsApiCall` `eventType`.

Desde: 1.01

Opcional: Verdadero

managementEvent

Un valor booleano que identifica si el evento es un evento de administración. `managementEvent` se muestra en un registro de eventos si `eventVersion` es 1.06 o superior y el tipo de evento es uno de los siguientes:

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

Desde: 1.06

Opcional: Verdadero

readOnly

Identifica si esta operación es una operación de solo lectura. Puede ser uno de los valores siguientes:

- `true`: la operación es de solo lectura (por ejemplo, `DescribeTrails`).
- `false`: la operación es de solo escritura (por ejemplo, `DeleteTrail`).

Desde: 1.01

Opcional: Verdadero

resources

Una lista de los recursos a los que ha obtenido acceso el evento. El campo puede contener la siguiente información:

- ARN del recurso
- El ID de cuenta del propietario del recurso

- El identificador de tipo de recurso en el formato: `AWS::aws-service-name::data-type-name`

Por ejemplo, cuando se registra un evento `AssumeRole`, el campo `resources` puede tener un aspecto similar al siguiente:

- ARN: `arn:aws:iam::123456789012:role/myRole`
- ID de cuenta: `123456789012`
- Identificador de tipo de recurso: `AWS::IAM::Role`

Para ver, por ejemplo, los registros con el *`resources`* campo, consulte Evento de AWS STS API en el archivo de CloudTrail registro en la Guía del usuario de IAM o Registro de llamadas a la AWS KMS API en la Guía para desarrolladores.AWS Key Management Service

Desde: 1.01

Opcional: Verdadero

`recipientAccountId`

Representa el ID de cuenta que recibió este evento. El `recipientAccountID` puede ser diferente de CloudTrail Elemento UserIdentity `accountId`. Esto puede ocurrir en el acceso de recursos entre cuentas. Por ejemplo, si una clave de KMS, también conocida como AWS KMS key, fue utilizada por una cuenta aparte para llamar a la API Encrypt, los valores de `accountId` y `recipientAccountID` serán los mismos para el evento enviado a la cuenta que realizó la llamada, pero serán diferentes para el evento que se envía a la cuenta propietaria de la clave de KMS.

Desde: 1.02

Opcional: Verdadero

`serviceEventDetails`

Identifica el evento del servicio, incluido lo que activó el evento y el resultado. Para obtener más información, consulte Eventos de servicio de AWS. Este campo tiene un tamaño máximo de 100 KB; el contenido que supere ese límite se trunca.

Desde: 1.05

Opcional: Verdadero

`sharedEventID`

El GUID se genera CloudTrail para identificar de forma exclusiva CloudTrail los eventos de la misma AWS acción que se envían a cuentas diferentes AWS .

Por ejemplo, cuando una cuenta usa una AWS KMS keyque pertenece a otra cuenta, la cuenta que usó la clave KMS y la cuenta propietaria de la clave KMS reciben CloudTrail eventos separados para la misma acción. Cada CloudTrail evento entregado para esta AWS acción comparte lo mismo`sharedEventID`, pero también tiene un `eventID` y único`recipientAccountID`.

Para obtener más información, consulte Ejemplo de sharedEventID.

> **Note**
>
> El `sharedEventID` campo solo está presente cuando CloudTrail los eventos se envían a varias cuentas. Si la persona que llama y el propietario son de la misma AWS cuenta, CloudTrail envía solo un evento y el `sharedEventID` campo no está presente.

Desde: 1.03

Opcional: Verdadero

`vpcEndpointId`

Identifica el punto de enlace de la VPC en el que se realizaron las solicitudes desde una VPC a otro servicio de AWS , tal como Amazon S3.

Desde: 1.04

Opcional: Verdadero

`eventCategory`

Muestra la categoría de eventos que se utiliza en las llamadas a `LookupEvents`.

- Para los eventos de administración, el valor es `Management`.
- Para los eventos de datos de, el valor es `Data`.

- Para los eventos de Insights, el valor es `Insight`.

Desde: 1.07

Opcional: Falso

`addendum`

Si se ha retrasado la entrega de un evento o queda disponible información adicional sobre un evento existente después de registrar el evento, un campo anexado muestra información sobre el motivo del retraso del evento. Si falta información de un evento existente, el campo anexado incluye la información que falta y un motivo. El contenido incluye lo siguiente:

- **`reason`**: el motivo por el que faltaba el evento o algunos de sus contenidos. Los valores pueden ser cualquiera de los siguientes.
  - **`DELIVERY_DELAY`**: se produjo un retraso en la entrega de eventos. Esto puede deberse a un tráfico de red elevado, a problemas de conectividad o a un problema CloudTrail de servicio.
  - **`UPDATED_DATA`**: faltó un campo en el registro de eventos o había un valor incorrecto.
  - **`SERVICE_OUTAGE`**— Un servicio que registra los eventos CloudTrail relacionados con una interrupción y no puede registrarlos CloudTrail. Esto es excepcionalmente raro.
- **`updatedFields`**: los campos del registro de eventos que se actualizan con la información agregada. Esto solo se proporciona si el motivo es `UPDATED_DATA`.
- **`originalRequestID`**: el ID único original de la solicitud. Esto solo se proporciona si el motivo es `UPDATED_DATA`.
- **`originalEventID`**: el ID del evento original. Esto solo se proporciona si el motivo es `UPDATED_DATA`.

Desde: 1.08

Opcional: Verdadero

`sessionCredentialFromConsole`

Muestra si un evento se originó o no en una AWS Management Console sesión. Este campo no se muestra a menos que el valor sea `true`, lo que significa que el cliente que se utilizó para realizar la llamada a la API era un proxy o un cliente externo. Si se ha utilizado un cliente proxy, el campo del evento `tlsDetails` no se muestra.

Desde: 1.08

Opcional: Verdadero

`edgeDeviceDetails`

Muestra información sobre los dispositivos de borde que son destinos de una solicitud. En la actualidad, los dispositivos `S3 Outposts` incluyen este campo. Este campo tiene un tamaño máximo de 28 KB; el contenido que supere ese límite se trunca.

Desde: 1.08

Opcional: Verdadero

`tlsDetails`

Muestra información sobre la versión de Transport Layer Security (TLS), los conjuntos de cifrado y el nombre de dominio completo (FQDN) del nombre de host proporcionado por el cliente y utilizado en la llamada a la API de servicio, que suele ser el FQDN del punto final del servicio. CloudTrailsigue registrando detalles de TLS parciales si falta la información esperada o está vacía. Por ejemplo, si la versión de TLS y el conjunto de cifrado están presentes, pero el `HOST` encabezado está vacío, los detalles de TLS disponibles se seguirán registrando en ese caso. CloudTrail Para obtener más información sobre los servicios en los que se registran los detalles de TLS, consulte. CloudTrail Detalles de los servicios que admiten TLS en CloudTrail

- **`tlsVersion`**: la versión TLS de una solicitud.
- **`cipherSuite`**: el conjunto de cifrado (combinación de algoritmos de seguridad utilizados) de una solicitud.
- **`clientProvidedHostHeader`**: nombre de host proporcionado por el cliente que se utiliza en la llamada a la API del servicio, que suele ser el FQDN del punto de conexión del servicio.

> **Note**
>
> Hay algunos casos en los que el campo `tlsDetails` no está presente en un registro de eventos.
>
> - El `tlsDetails` campo no está presente si la llamada a la API la realizó una persona Servicio de AWS en su nombre. El campo `invokedBy` del elemento `userIdentity` identifica al Servicio de AWS que hizo la llamada a la API.
> - Si `sessionCredentialFromConsole` está presente con un valor de true, `tlsDetails` estará presente en un registro de evento solo si se utilizó un cliente externo para hacer la llamada a la API.

Desde: 1.08

Opcional: Verdadero

Campos de registro de eventos de Insights

Los siguientes son atributos que se muestran en la estructura JSON de un evento de Insights que difieren de los de un evento de administración o de datos.

`sharedEventId`

La A `sharedEventID` para los eventos de CloudTrail Insights difiere de la `sharedEventID` correspondiente a los tipos de CloudTrail eventos de administración y datos. En los eventos de Insights, a `sharedEventID` es un GUID generado por CloudTrail Insights para identificar de forma exclusiva un evento de Insights. `sharedEventID`es común entre el inicio y el final de los eventos de Insights y ayuda a conectar ambos eventos para identificar de forma única actividades inusuales. `sharedEventID` puede considerarse como el ID general de evento de Insights.

Desde: 1.07

Opcional: Falso

`insightDetails`

Solo eventos de Insights. Muestra información sobre los desencadenantes subyacentes de un evento de Insights, tal como la fuente del evento, el agente del usuario, las estadísticas, el nombre de la API y si se trata de un evento de Insights inicial o final. Para obtener más información sobre el contenido del bloque `insightDetails`, consulte Elemento `insightDetails` CloudTrail Insights

Desde: 1.07

Opcional: Falso

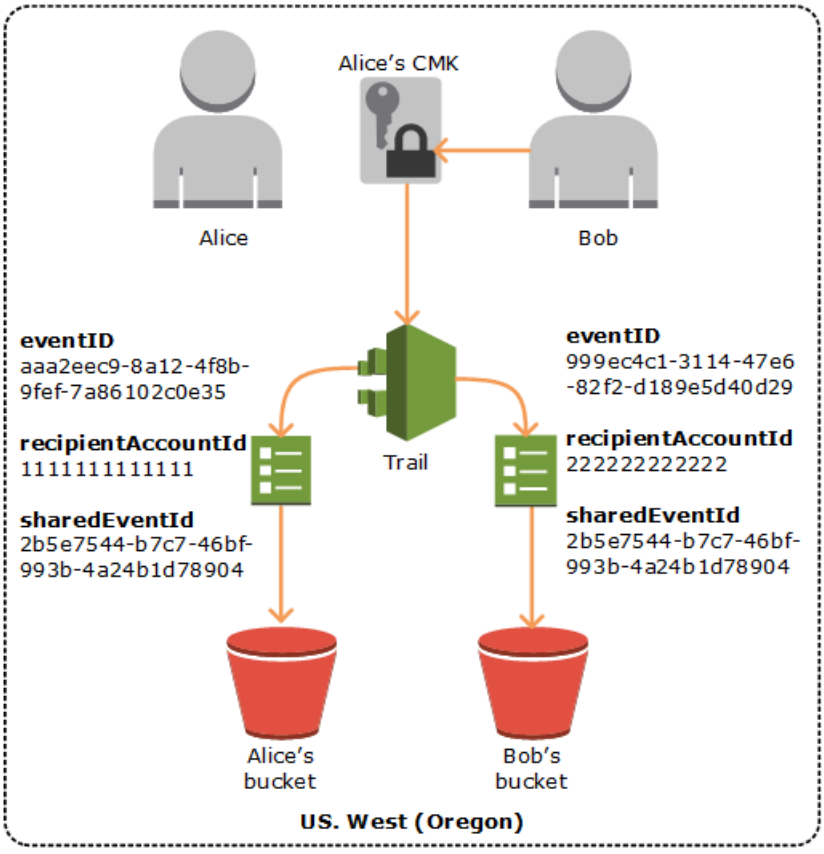
Ejemplo de sharedEventID

A continuación se muestra un ejemplo que describe cómo se generan CloudTrail dos eventos para la misma acción:

1. Alice tiene una AWS cuenta (1111) y crea una AWS KMS key. Es la propietaria de esta clave de KMS.

2. Bob tiene una AWS cuenta (222222222222). Alice concede a Bob permiso para utilizar la clave de KMS.
3. Cada cuenta tiene un registro de seguimiento y un bucket independiente.
4. Bob utiliza la clave de KMS para llamar a la API `Encrypt`.
5. CloudTrail envía dos eventos separados.

   - Un evento se envía a Bob. El evento muestra que Bob utilizó la clave de KMS.
   - Un evento se envía a Alice. El evento muestra que Bob utilizó la clave de KMS.
   - Los eventos tienen el mismo `sharedEventID`, pero el `eventID` y `recipientAccountID` son únicos.



ID de eventos compartidos en CloudTrail Insights

La A `sharedEventID` para los eventos de CloudTrail Insights difiere de la `sharedEventID` para los tipos de CloudTrail eventos de administración y datos. En los eventos de Insights, a `sharedEventID` es un GUID generado por CloudTrail Insights para identificar de forma exclusiva un par de eventos de Insights de inicio y fin. `sharedEventID`es común entre el inicio y el final de

un evento de Insights y ayuda a crear una correlación entre ambos eventos para identificar de forma única una actividad inusual.

`sharedEventID` puede considerarse como el ID general de evento de Insights.

Detalles de los servicios que admiten TLS en CloudTrail

A partir del 28 de junio de 2023, es AWS necesario que la configuración de Transport Layer Security (TLS) para todos los puntos finales de la API de AWS servicio tenga una versión mínima de TLS 1.2. Para obtener más información, consulte la entrada del blog, TLS 1.2, que se convertirá en el nivel mínimo de protocolo TLS para todos los puntos de enlace de la API. AWS La `tlsDetails` estructura de cada CloudTrail registro contiene la versión TLS, el conjunto de cifrado y el nombre de host proporcionado por el cliente y utilizado en la llamada a la API del servicio, que suele ser el nombre de dominio completo (FQDN) del punto final del servicio. A continuación, puede usar los datos de los registros para identificar el software cliente que utiliza una versión antigua de TLS y actualizarlo en consecuencia. Actualmente, casi la mitad de los AWS servicios proporcionan la información de TLS sobre el terreno. CloudTrail `tlsDetails` En la siguiente tabla se muestran AWS los servicios que muestran información de TLS en CloudTrail los registros.

> **Note**
>
> El campo `tlsDetails` es opcional. Hay algunos casos en los que el campo `tlsDetails` no está presente en un registro de eventos.

Servicios que admiten detalles de TLS
Alexa for Business
AWS Activar
AWS AppConfig
AWS App Mesh
AWS App Runner
Amazon AppStream 2.0

Servicios que admiten detalles de TLS
AWS Auto Scaling
AWS Backup
AWS Backup Gateway
AWS Billing
AWS Certificate Manager
AWS Cloud9
Amazon Cloud Directory
AWS CloudFormation
Amazon CloudFront
AWS Cloud Map
Amazon CloudSearch
AWS CloudTrail
Amazon CloudWatch
Información sobre CloudWatch aplicaciones de Amazon
CloudWatch Eventos de Amazon
Amazon CloudWatch Logs
AWS CodeArtifact
AWS CodeBuild
AWS CodeCommit
AWS CodeDeploy

Servicios que admiten detalles de TLS
AWS CodePipeline
AWS CodeStar
AWS CodeStar Conexiones
Amazon Comprehend
Amazon Comprehend Medical
AWS Compute Optimizer
Amazon Connect Voice ID
AWS Control Tower
AWS Cost and Usage Report
AWS Cost Explorer
AWS Database Migration Service (DMS)
AWS Data Pipeline
AWS DataSync
AWS DeepRacer
AWS Device Farm
AWS Diodo
AWS Direct Connect
AWS Directory Service
Amazon DynamoDB
Amazon DynamoDB Accelerator (DAX) (Acelerador de Amazon DynamoDB (DAX)).

Servicios que admiten detalles de TLS
Amazon Elastic Block Store (EBS)
Amazon Elastic Compute Cloud (EC2)
Conexión de la instancia de Amazon EC2
Amazon Elastic Container Registry (ECR)
Amazon Elastic Container Registry (ECR) Public
Amazon Elastic Container Service (ECS)
Amazon ElastiCache
Amazon Elastic File System (EFS)
Amazon Elastic Transcoder
AWS Elastic Load Balancing (ELB)
AWS Elastic Load Balancing (ELBV2)
AWS Elemental MediaStore
Amazon EMR
Amazon EventBridge
AWS Firewall Manager
Amazon Forecast
Amazon Fraud Detector
Amazon FSx
Amazon GameLift
AWS Global Accelerator

Servicios que admiten detalles de TLS
AWS Glue (Lake Formation)
AWS HealthLake
AWS Identity and Access Management (IAM)
AWS Tienda de identidades
Amazon Inspector
AWS IoT Analytics
AWS IoT Core
AWS IoT Events
AWS IoT Secure Tunneling
AWS IoT SiteWise
AWS IoT Wireless
Amazon Kendra
AWS Key Management Service (KMS)
Amazon Kinesis
Amazon Managed Service para Apache Flink
Amazon Data Firehose
Amazon Kinesis Data Streams
Amazon Kinesis Video Streams
AWS Lambda
AWS License Manager

Servicios que admiten detalles de TLS
Amazon Lightsail
Amazon Lookout for Equipment
Amazon Machine Learning
Amazon Managed Service para Prometheus
AWS Managed Services
AWS Marketplace Commerce Analytics
AWS Marketplace Descubrimiento
AWS Marketplace Entitlement Service
AWS Marketplace Metering Service
Amazon Mechanical Turk
Amazon MemoryDB para Redis
AWS Migration Hub
AWS Network Firewall
OpenSearch Servicio Amazon
AWS OpsWorks CM
AWS Organizations
Amazon Polly
Lista de precios de AWS
AWS Private Certificate Authority
AWS Proton

Servicios que admiten detalles de TLS
Amazon QuickSight
Amazon Redshift
Amazon Rekognition
Amazon Relational Database Service (RDS)
API de datos de Amazon Relational Database Service (RDS)
AWS Resource Groups Etiquetado
Amazon Route 53
Amazon Route 53 Dominios
Amazon Route 53 Resolver
Amazon SageMaker
Amazon SageMaker Edge
AWS Secrets Manager
AWS Security Token Service (STS)
AWS Service Catalog
AWS Service Quotas
AWS Shield
Amazon SimpleDB
Amazon Simple Email Service (SES)
Amazon Simple Notification Service (SNS)
Amazon Simple Queue Service (SQS)

Servicios que admiten detalles de TLS
Amazon Simple Storage Service (S3)
Amazon S3 Glacier
Amazon Simple Workflow Service (SWF)
AWS Snowball
AWS Step Functions
AWS Storage Gateway
AWS Support
AWS Systems Manager
Amazon Textract
Amazon Timestream
Amazon Transcribe Streaming Service
AWS Transfer Family
Amazon Translate
AWS Trusted Advisor
AWS WAF
Amazon WorkDocs
Amazon WorkMail
Flujo de WorkMail mensajes de Amazon
Amazon WorkSpaces
AWS X-Ray

CloudTrail Elemento UserIdentity

AWS Identity and Access Management (IAM) proporciona diferentes tipos de identidades. El elemento `userIdentity` contiene información sobre el tipo de identidad de IAM que ha realizado la solicitud y las credenciales que se han utilizado. Si se utilizaron credenciales temporales, el elemento muestra cómo se obtuvieron las credenciales.

Contenido

- Ejemplos
- Campos
- Valores para AWS STS las API con SAML y federación de identidades web
- AWS STS identidad de origen

Ejemplos

`userIdentity` con credenciales de usuario de IAM

El siguiente ejemplo muestra el elemento `userIdentity` de una solicitud sencilla realizada con las credenciales de la usuaria de IAM llamada `Alice`.

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

`userIdentity` con credenciales de seguridad temporales

El siguiente ejemplo muestra un elemento `userIdentity` de una solicitud realizada con credenciales de seguridad temporales obtenidas mediante la adopción de un rol de IAM. El elemento contiene detalles adicionales sobre el rol que se asumió para obtener las credenciales.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
```

```
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
    }
}
```

`userIdentity` de una solicitud hecha en nombre de un usuario de IAM Identity Center

En el siguiente ejemplo, se muestra un elemento `userIdentity` de una solicitud hecha en nombre de un usuario de IAM Identity Center.

```
"userIdentity": {
 "type": "IdentityCenterUser",
 "accountId": "123456789012",
 "onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
 },
 "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

Campos

Los siguientes campos pueden aparecer en un elemento `userIdentity`.

`type`

El tipo de la identidad. Se admiten los siguientes valores:

- `Root`— La solicitud se realizó con sus Cuenta de AWS credenciales. Si el tipo de `userIdentity` es `Root` y configura un alias para su cuenta, el campo `userName` contiene el alias de la cuenta. Para obtener más información, consulte Su ID de Cuenta de AWS y su alias.

- `IAMUser`: la solicitud se realizó con las credenciales de un usuario de IAM.
- `AssumedRole`: la solicitud se realizó con credenciales de seguridad temporales obtenidas con un rol a través de una llamada a la API de AWS Security Token Service (AWS STS) `AssumeRole`. Para ello se pueden utilizar roles de Amazon EC2 y acceso a la API entre cuentas.
- `Role`: la solicitud se realizó con una identidad de IAM persistente que tiene permisos específicos. El emisor de las sesiones de rol es siempre el rol. Para obtener más información sobre los roles, consulte Términos y conceptos sobre los roles en la Guía del usuario de IAM.
- `FederatedUser`— La solicitud se realizó con credenciales de seguridad temporales obtenidas de una llamada a la AWS STS `GetFederationToken`API. El elemento `sessionIssuer` indica si se llamó a la API con credenciales de usuario raíz o de usuario de IAM.

  Para obtener más información acerca de las credenciales de seguridad temporales, consulte Credenciales de seguridad temporales en la guía del usuario de IAM.
- `Directory`: la solicitud se realizó a un servicio de directorio y el tipo es desconocido. Los servicios de directorio incluyen los siguientes: Amazon WorkDocs y Amazon QuickSight.
- `AWSAccount`— La solicitud fue realizada por otro Cuenta de AWS
- `AWSService`— La solicitud fue realizada por un hombre Cuenta de AWS que pertenece a un Servicio de AWS. Por ejemplo, AWS Elastic Beanstalk asume una función de IAM en su cuenta para llamar a otra Servicios de AWS en su nombre.
- `IdentityCenterUser`: la solicitud se hizo en nombre de un usuario de IAM Identity Center.
- `Unknown`— La solicitud se realizó con un tipo de identidad que no CloudTrail se puede determinar.

Opcional: Falso

`AWSAccount` y `AWSService` aparecen como `type` en sus archivos de registros cuando se utiliza el acceso entre cuentas mediante un rol de IAM de su propiedad.

Ejemplo: acceso entre cuentas iniciado por otra cuenta de AWS .

1. Usted es propietario de un rol de IAM en su cuenta.
2. Otra AWS cuenta cambia a esa función para asumir la función de tu cuenta.
3. Como es propietario del rol de IAM, recibe un registro que muestra que la otra cuenta adoptó el rol. El valor de `type` es `AWSAccount`. Para ver un ejemplo de entrada de registro, consulta el evento de la AWS STS API en el archivo de CloudTrail registro.

Ejemplo: acceso entre cuentas iniciado por un servicio AWS

1. Usted es propietario de un rol de IAM en su cuenta.
2. Una AWS cuenta propiedad de un AWS servicio asume esa función.
3. Como es propietario del rol de IAM, recibe un registro que muestra el servicio de AWS que adoptó el rol. El valor de `type` es `AWSService`.

`userName`

El nombre descriptivo de la identidad que realizó la llamada. El valor que aparece en `userName` se basa en el valor de `type`. En la tabla siguiente se muestra la relación entre `type` y `userName`:

`type`	**`userName`**	Descripción
`Root` (sin alias definido)	No presente	Si no has configurado un alias para ti Cuenta de AWS, el `userName` campo no aparece. Para obtener más información sobre los alias de las cuentas, consulta Tu Cuenta de AWS ID y su alias. Tenga en cuenta que el campo `userName` no puede contener `Root` porque `Root` es un tipo de identidad, no un nombre de usuario.
`Root` (con alias definido)	El alias de la cuenta	Para obtener más información sobre los Cuenta de AWS alias, consulta Tu Cuenta de AWS ID y su alias.
`IAMUser`	El nombre de usuario del usuario de IAM	
`AssumedRole`	No presente	En el caso del tipo `AssumedRole` , puede encontrar el campo `userName` de `sessionContext` , como parte del elemento **`sessionIssuer`** . Para ver una entrada de ejemplo, consulte Ejemplos.

type	userName	Descripción
Role	Definido por el usuario	Las secciones sessionContext y sessionIssuer contienen información sobre la identidad que emitió la sesión para el rol.
FederatedUser	No presente	Las secciones sessionContext y sessionIssuer contienen información sobre la identidad que emitió la sesión para el usuario federado.
Directory	Puede estar presente	Por ejemplo, el valor puede ser el alias de cuenta o la dirección de correo electrónico del ID de Cuenta de AWS asociado.
AWSService	No presente	
AWSAccount	No presente	
IdentityCenterUser	No presente	La sección onBehalfOf contiene información sobre el ID de usuario de IAM Identity Center y el ARN del almacén de identidades para los que se hizo la llamada. Para obtener más información acerca de IAM Identity Center, consulte la Guía del usuario de AWS IAM Identity Center .
Unknown	Puede estar presente	Por ejemplo, el valor puede ser el alias de cuenta o la dirección de correo electrónico del ID de Cuenta de AWS asociado.

> **Note**
>
> El campo userName contiene la cadena HIDDEN_DUE_TO_SECURITY_REASONS cuando el evento registrado es un error de inicio de sesión en la consola ocasionado al ingresar un nombre de usuario incorrecto. CloudTrail no graba el contenido en este caso porque el texto podría contener información confidencial, como en los ejemplos siguientes:
>
> - Un usuario escribe por error una contraseña en el campo de nombre de usuario.

- Un usuario hace clic en el enlace de la página de inicio de sesión de una AWS cuenta, pero después escribe el número de cuenta de otra.
- Un usuario escribe por error el nombre de una cuenta de correo electrónico personal, un identificador de inicio de sesión en un banco u otro identificador privado.

Opcional: Verdadero

`principalId`

Un identificador único para la entidad que ha efectuado la llamada. Para las solicitudes realizadas con credenciales de seguridad temporales, este valor incluye el nombre de la sesión que se pasa a la llamada API `AssumeRole`, `AssumeRoleWithWebIdentity` o `GetFederationToken`.

Opcional: Verdadero

`arn`

El nombre de recurso de Amazon (ARN) de la entidad principal que realizó la llamada. La última sección del arn contiene el usuario o el rol que realizó la llamada.

Opcional: Verdadero

`accountId`

La cuenta que posee la entidad que concedió permisos para la solicitud. Si la solicitud se hizo con credenciales de seguridad temporales, esta es la cuenta perteneciente al usuario o rol de IAM que se utilizó para obtener las credenciales.

Si la solicitud se hizo con un token de acceso autorizado de IAM Identity Center, esta es la cuenta propietaria de la instancia de IAM Identity Center.

Opcional: Verdadero

`accessKeyId`

El ID de clave de acceso de que se utilizó para firmar la solicitud. Si la solicitud se realizó con credenciales de seguridad temporales, este es el ID de clave de acceso de las credenciales temporales. Por razones de seguridad, puede ser que el `accessKeyId` no esté presente, o puede mostrarse como una cadena vacía.

Opcional: Verdadero

`sessionContext`

Si la solicitud se hizo con credenciales de seguridad temporales, `sessionContext` proporciona información sobre la sesión que se creó para esas credenciales. Las sesiones se crean cuando se llama a alguna API que devuelve credenciales temporales. Los usuarios también crean sesiones cuando trabajan en la consola y hacen solicitudes a través de la API que incluyen la autenticación multifactor. Este elemento tiene los siguientes atributos:

- `creationDate`: la fecha y la hora en que se emitieron las credenciales de seguridad temporales. Representadas con la notación básica ISO 8601.
- `mfaAuthenticated`: el valor es `true` si el usuario raíz o el usuario de IAM que usaron sus credenciales para la solicitud también se autenticó con un dispositivo MFA; de lo contrario, el valor es `false`.
- `sourceIdentity`: consulte AWS STS identidad de origen en este tema. El campo `sourceIdentity` se produce en eventos cuando los usuarios adoptan un rol de IAM para llevar a cabo una acción. `sourceIdentity` identifica la identidad de usuario original que hace la solicitud, ya sea que la identidad de ese usuario sea un usuario de IAM, un rol de IAM, un usuario autenticado con federación basada en SAML o un usuario autenticado mediante la federación de identidades web conforme con OpenID Connect (OIDC). Para obtener más información sobre la configuración AWS STS para recopilar la información de identidad de origen, consulte Supervisar y controlar las acciones que se toman con los roles asumidos en la Guía del usuario de IAM.
- `ec2RoleDelivery`: el valor es `1.0` si el servicio de metadatos de instancias de Amazon EC2 versión 1 (IMDSv1) proporcionó las credenciales. El valor es `2.0` si las credenciales se proporcionaron mediante el nuevo esquema IMDS.

  AWS Las credenciales proporcionadas por el Amazon EC2 Instance Metadata Service (IMDS) incluyen una clave de contexto ec2: RoleDelivery IAM. Esta clave de contexto facilita la aplicación del nuevo esquema en resource-by-resource función de una service-by-service o varias, ya que utiliza la clave de contexto como condición en las políticas de IAM, las políticas de recursos o las políticas de control de servicios. AWS Organizations Para obtener más información, consulte Datos de usuario y metadatos de instancia en la Guía del usuario de instancias de Linux de Amazon EC2.

Opcional: Verdadero

`invokedBy`

El nombre de la Servicio de AWS persona que realizó la solicitud, cuando la solicitud la realiza un Servicio de AWS Auto Scaling de Amazon EC2 o. AWS Elastic Beanstalk Este campo solo está presente cuando una solicitud la realiza un Servicio de AWS. Esto incluye las solicitudes realizadas por los servicios que utilizan sesiones de acceso directo (FAS), Servicio de AWS los directores, las funciones vinculadas al servicio o las funciones de servicio utilizadas por un. Servicio de AWS

Opcional: Verdadero

`sessionIssuer`

Si un usuario hizo una solicitud con credenciales de seguridad temporales, `sessionIssuer` proporciona información acerca de cómo el usuario obtuvo las credenciales. Por ejemplo, si obtuvo las credenciales de seguridad temporales asumiendo un rol, este elemento proporciona información acerca del rol asumido. Si obtuvo las credenciales con las credenciales de un usuario raíz o un usuario de IAM para llamar a AWS STS en `GetFederationToken`, el elemento proporciona información sobre la cuenta raíz o el usuario de IAM. Este elemento tiene los siguientes atributos:

- `type`: el origen de las credenciales de seguridad temporales, como `Root`, `IAMUsero Role`.
- `userName`: el nombre descriptivo del usuario o el rol que emitió la sesión. El valor que aparece depende del valor `type` de la identidad `sessionIssuer`. En la tabla siguiente se muestra la relación entre `sessionIssuer type` y `userName`:

`sessionIssuer` type	**`userName`**	Descripción
`Root` (sin alias definido)	No presente	Si no ha creado un alias para su cuenta, no aparece el campo `userName`. Para obtener más información sobre los Cuenta de AWS alias, consulta Tu Cuenta de AWS ID y su alias. Tenga en cuenta que el campo `userName` no puede contener `Root` porque `Root` es un tipo de identidad, no un nombre de usuario.

sessionIssuer type	**userName**	Descripción
`Root` (con alias definido)	El alias de la cuenta	Para obtener más información sobre los Cuenta de AWS alias, consulta Tu ID de AWS cuenta y su alias.
`IAMUser`	El nombre de usuario del usuario de IAM	Esto también se aplica cuando un usuario federado utiliza una sesión emitida por `IAMUser`.
`Role`	El nombre del rol	Un rol que asume un usuario de IAM o un usuario federado de identidad web en una sesión de rol. Servicio de AWS

- `principalId`: el ID interno de la entidad que se utilizó para obtener las credenciales.
- `arn`: el ARN de la fuente (cuenta, usuario de IAM o rol) que se utilizó para obtener credenciales de seguridad temporales.
- `accountId`: la cuenta que posee la entidad que se utilizó para obtener las credenciales.

Opcional: Verdadero

`onBehalfOf`

Si la solicitud la hizo una persona que llamó a IAM Identity Center, `onBehalfOf` proporciona información sobre el ID de usuario de IAM Identity Center y el ARN del almacén de identidades para el que se hizo la llamada. Este elemento tiene los siguientes atributos:

- `userId`: el ID del usuario de IAM Identity Center en nombre del que se hizo la llamada.
- `identityStoreArn`: el ARN del almacén de identidades de IAM Identity Center en nombre del que se hizo la llamada.

Opcional: Verdadero

`credentialId`

El ID de la credencial de la solicitud. Solo se establece cuando la persona que llama usa un token de portador, como un token de acceso autorizado de IAM Identity Center.

Opcional: Verdadero

`webIdFederationData`

Si la solicitud se hizo con credenciales de seguridad temporales obtenidas por federación de identidades web, `webIdFederationData` muestra información sobre el proveedor de identidades.

Este elemento tiene los siguientes atributos:

- `federatedProvider`: el nombre principal del proveedor de identidad (por ejemplo, `www.amazon.com` para Login with Amazon o `accounts.google.com` para Google).
- `attributes`: el ID de aplicación y el ID de usuario tal como los indicó el proveedor (por ejemplo, `www.amazon.com:app_id` y `www.amazon.com:user_id` para Login with Amazon).

> **Note**
>
> La omisión de este campo o la presencia de este campo con un valor vacío significa que no hay información sobre el proveedor de identidad.

Opcional: Verdadero

Valores para AWS STS las API con SAML y federación de identidades web

AWS CloudTrail admite las llamadas a la API logging AWS Security Token Service (AWS STS) realizadas con el lenguaje de marcado de aserciones de seguridad (SAML) y la federación de identidades web. Cuando un usuario realiza una llamada a las `AssumeRoleWithWebIdentity`API `AssumeRoleWithSAML`y, CloudTrail graba la llamada y envía el evento a su bucket de Amazon S3.

El elemento `userIdentity` de estas API contiene los siguientes valores.

`type`

El tipo de identidad.

- `SAMLUser`: la solicitud se realizó con una aserción SAML.
- `WebIdentityUser`: la solicitud la realizó un proveedor de federación de identidades web.

`principalId`

Un identificador único para la entidad que ha efectuado la llamada.

- Para `SAMLUser`, este identificador es una combinación de las claves `saml:namequalifier` y `saml:sub`.
- Para `WebIdentityUser`, es una combinación del emisor, el ID de aplicación y el ID de usuario.

`userName`

El nombre de la identidad que realizó la llamada.

- Para `SAMLUser`, esta es la clave de `saml:sub`.
- Para `WebIdentityUser`, este es el ID de usuario.

`identityProvider`

El nombre principal del proveedor de identidad externo. Este campo aparece únicamente para los tipos `SAMLUser` o `WebIdentityUser`.

- Para `SAMLUser`, es la clave de `saml:namequalifier` de la aserción de SAML.
- Para `WebIdentityUser`, es el nombre de emisor del proveedor de federación de identidades web. Puede ser un proveedor que haya configurado, como los siguientes:
  - `cognito-identity.amazon.com` para Amazon Cognito
  - `www.amazon.com` para Login with Amazon
  - `accounts.google.com` para Google
  - `graph.facebook.com` para Facebook

A continuación se incluye un elemento `userIdentity` de ejemplo para la acción `AssumeRoleWithWebIdentity`.

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

Para ver, por ejemplo, registros del aspecto `SAMLUser` y los `WebIdentityUser` tipos del `userIdentity` elemento, consulte Registrar llamadas de IAM y AWS STS API con AWS CloudTrail.

AWS STS identidad de origen

Un administrador de IAM puede AWS Security Token Service configurarlo para exigir que los usuarios especifiquen su identidad cuando utilicen credenciales temporales para asumir funciones. El campo `sourceIdentity` está presente en eventos donde los usuarios adoptan un rol de IAM o llevan a cabo acciones con el rol adoptado.

El campo `sourceIdentity` identifica la identidad de usuario original que realiza la solicitud, ya sea que la identidad de ese usuario se trate de un usuario de IAM, un rol de IAM, un usuario autenticado mediante la federación basada en SAML o un usuario autenticado mediante la identidad federada web conforme con OpenID Connect (OIDC). Una vez que el administrador de IAM realiza la configuración AWS STS, CloudTrail registra la `sourceIdentity` información en los siguientes eventos y ubicaciones dentro del registro de eventos:

- Las AWS STS `AssumeRoleAssumeRoleWithSAML`, o las `AssumeRoleWithWebIdentity` llamadas que realiza la identidad de un usuario cuando asume un rol. `sourceIdentity`se encuentra en el `requestParameters` bloque de AWS STS llamadas.
- Las AWS STS `AssumeRoleAssumeRoleWithSAML`, o las `AssumeRoleWithWebIdentity` llamadas que realiza la identidad de un usuario si utiliza un rol para asumir otro rol, lo que se conoce como encadenamiento de roles. `sourceIdentity`se encuentra en el `requestParameters` bloque de AWS STS llamadas.
- Las llamadas a la API del AWS servicio que realiza la identidad del usuario al asumir un rol y utilizar las credenciales temporales asignadas por AWS STS. En los eventos API de servicio, `sourceIdentity` se encuentra en el bloque `sessionContext`. Por ejemplo, si una identidad de usuario crea un nuevo bucket de S3, se produce `sourceIdentity` en el bloque `sessionContext` del evento `CreateBucket`.

Para obtener más información sobre cómo configurar AWS STS la recopilación de la información de identidad de origen, consulte Supervisar y controlar las acciones que se toman con los roles asumidos en la Guía del usuario de IAM. Para obtener más información sobre AWS STS los eventos que se registran CloudTrail, consulte Registrar las llamadas de IAM y AWS STS API AWS CloudTrail en la Guía del usuario de IAM.

Los siguientes son fragmentos de ejemplo de eventos que muestran el campo `sourceIdentity`.

Ejemplo de sección de **`requestParameters`**

En el siguiente fragmento de eventos de ejemplo, un usuario realiza una AWS STS `AssumeRole` solicitud y establece una identidad de origen, representada aquí por. *`source-identity-value-set`* El usuario adopta un rol representado por el ARN `arn:aws:iam::123456789012:role/Assumed_Role` del rol. El campo `sourceIdentity` está en el bloque `requestParameters` del evento.

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
    },
```

Ejemplo de sección de **`responseElements`**

En el siguiente fragmento de evento de ejemplo, un usuario realiza una AWS STS `AssumeRole` solicitud para asumir un rol denominado`Developer_Role`, y establece una identidad de origen,. `Admin` El usuario adopta un rol representado por el ARN `arn:aws:iam::111122223333:role/Developer_Role` del rol. El campo `sourceIdentity` se muestra en los bloques `requestParameters` y `responseElements` del evento. Las credenciales temporales utilizadas para adoptar el rol, la cadena de token de sesión y el ID del rol adoptado, el nombre de sesión y el ARN de sesión se muestran en el bloque `responseElements`, junto con la identidad de la fuente.

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
        "credentials": {
```

```
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                            EXAMPLE_SESSION_TOKEN
                            XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

Ejemplo de sección de **`sessionContext`**

En el siguiente fragmento de evento de ejemplo, un usuario asume un rol denominado `DevRole` para llamar a una API de servicio. AWS El usuario establece una identidad de origen, representada aquí por. *`source-identity-value-set`* El campo `sourceIdentity` está en el bloque `sessionContext`, dentro del bloque `userIdentity` del evento.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
```

```
    }
  }
}
```

Elemento **insightDetails** CloudTrail Insights

Los registros de eventos de Insights de AWS CloudTrail incluyen campos que son diferentes de otros eventos de CloudTrail en su estructura JSON, a veces llamados carga. Un eventos de CloudTrail Insights incluye un bloque `insightDetails` que contiene información sobre los desencadenantes subyacentes de un evento de Insights, tal como la fuente del evento, las identidades de usuario, los agentes de usuario, los promedios históricos o los valores de referencia, estadísticas, nombre de la API y si se trata de un evento de Insights inicial o final. El bloque `insightDetails` contiene la siguiente información.

- **`state`**: si el evento es el evento inicial o final de Insights. El valor puede ser `Start` o `End`.

  Desde: 1.07

  Opcional: Falso

- **`eventSource`**: el punto de enlace del servicio de AWS que fue la fuente de la actividad inusual, como `ec2.amazonaws.com`.

  Desde: 1.07

  Opcional: Falso

- **`eventName`**: el nombre del evento de Insights, normalmente el nombre de la API que fue la fuente de la actividad inusual.

  Desde: 1.07

  Opcional: Falso

- **`insightType`**: el tipo de evento de Insights. Este valor puede ser `ApiCallRateInsight`, `ApiErrorRateInsight` o ambos.

  Desde: 1.07

  Opcional: Falso

- **`insightContext`** -

Información sobre las herramientas de AWS (llamadas agentes de usuario), usuarios y roles de IAM (llamados identidades de usuario) y códigos de error asociados a los eventos que CloudTrail analizó para generar el evento de Insights. Este elemento también incluye estadísticas que muestran cómo se compara la actividad inusual en un evento de Insights con la actividad de referencia o normal.

Desde: 1.07

Opcional: Falso

- **`statistics`**: incluye datos sobre la tasa promedio de referencia, o típica de llamadas o errores a la API en cuestión, que realiza una cuenta, medida durante el periodo de referencia, la tasa promedio de llamadas que desencadenaron el evento de Insights durante el primer minuto del evento de Insights, la duración, en minutos, del evento de Insights y la duración, en minutos, del periodo de medición de referencia.

  Desde: 1.07

  Opcional: Falso

  - **`baseline`**: la cantidad promedio de llamadas a la API o errores por minuto durante el periodo de referencia en la API en cuestión del evento de Insights para la cuenta, calculada durante los siete días anteriores al inicio del evento de Insights.

    Desde: 1.07

    Opcional: Falso

  - **`insight`** -

    Para un evento inicial de Insights, este valor es el número medio de llamadas a la API o errores por minuto durante el inicio de la actividad inusual. Para un evento final de Insights, este valor es el promedio de llamadas por minuto a la API durante la actividad inusual.

    Desde: 1.07

    Opcional: Falso

  - **`insightDuration`**: la duración, en minutos, de un evento de Insights (el periodo de tiempo desde el inicio hasta el final de la actividad inusual en la API en cuestión). `insightDuration` ocurre tanto en eventos iniciales como finales de Insights.

Desde: 1.07

Opcional: Falso

- **`baselineDuration`**: la duración, en minutos, del periodo de referencia (el periodo de tiempo en el que la actividad normal se mide en la API en cuestión). `baselineDuration` comprende, como mínimo, los siete días (10 080 minutos) que preceden a un evento de Insights. Este campo está presente tanto en eventos iniciales como finales de Insights. La hora de finalización de la medición de `baselineDuration` es siempre el comienzo de un evento de Insights.

  Desde: 1.07

  Opcional: Falso

- **`attributions`**: este bloque incluye información sobre las identidades de usuario, agentes de usuario y códigos de error correlacionados con la actividad inusual y de referencia. Un máximo de cinco identidades de usuario, cinco agentes de usuario y cinco códigos de error se capturan en un bloque `attributions` de eventos de Insights, ordenados por un promedio del recuento de actividad, en orden descendente de mayor a menor.

  Desde: 1.07

  Opcional: Verdadero

  - **`attribute`**: contiene el tipo de atributo. Los valores pueden ser `userIdentityArn`, `userAgent` o `errorCode`.
    - **`userIdentityArn`**: un bloque que muestra hasta los cinco usuarios principales de AWS o roles de IAM que contribuyeron a las llamadas a la API o los errores durante la actividad inusual y los periodos de referencia. También consulte `userIdentity` en CloudTrail contenido del registro.

      Desde: 1.07

      Opcional: Falso

      - **`insight`**: un bloque que muestra hasta los cinco ARN de identidad de usuario principales que contribuyeron a las llamadas a la API realizadas durante el periodo de actividad inusual, en orden descendente desde el número mayor de llamadas a la API hasta el menor. También muestra el promedio de llamadas a la API realizadas por las identidades de usuario durante el periodo de actividad inusual.

Desde: 1.07

Opcional: Falso

- **`value`**: el ARN de una de las cinco identidades de usuario principales que contribuyeron a las llamadas a la API realizadas durante el periodo de actividad inusual.

  Desde: 1.07

  Opcional: Falso

- **`average`**: el número de llamadas a la API o errores por minuto durante el periodo de actividad inusual para la identidad de usuario en el campo `value`.

  Desde: 1.07

  Opcional: Falso

- **`baseline`**: un bloque que muestra hasta los cinco ARN de identidad de usuario principales que más contribuyeron a las llamadas a la API o a los errores realizados durante el periodo de actividad normal. También muestra el promedio de llamadas a la API o errores realizados por las identidades de usuario durante el periodo de actividad normal.

  Desde: 1.07

  Opcional: Falso

  - **`value`**: el ARN de una de las cinco identidades de usuario principales que contribuyeron a las llamadas a la API o los errores realizados durante el periodo de actividad normal.

    Desde: 1.07

    Opcional: Falso

  - **`average`**: el promedio histórico de llamadas a la API o errores por minuto durante los siete días anteriores a la hora de inicio de la actividad de Insights para la identidad del usuario en el campo `value`.

    Desde: 1.07

    Opcional: Falso

- **`userAgent`**: un bloque que muestra hasta las cinco herramientas principales de AWS mediante las cuales la identidad del usuario contribuyó a las llamadas a la API durante la actividad inusual y los periodos de referencia. Estas herramientas incluyen la AWS Management Console, la AWS CLI o los SDK de AWS. También consulte `userAgent` en CloudTrail contenido del registro.

  Desde: 1.07

  Opcional: Falso

- **`insight`**: un bloque que muestra hasta los cinco agentes de usuarios principales que contribuyeron a las llamadas a la API realizadas durante el periodo de actividad inusual, en orden descendente desde el mayor número de llamadas a la API hasta el menor. También muestra el promedio de llamadas a la API o errores registrados por los agentes de usuario durante el periodo de actividad inusual.

  Desde: 1.07

  Opcional: Falso

  - **`value`**: uno de los cinco agentes de usuario principales que contribuyeron a las llamadas a la API realizadas durante el periodo de actividad inusual.

    Desde: 1.07

    Opcional: Falso

  - **`average`**: el número de llamadas a la API o errores registrados por minuto durante el periodo de actividad inusual para el agente de usuario en el campo `value`.

    Desde: 1.07

    Opcional: Falso

- **`baseline`**: un bloque que muestra hasta los cinco agentes de usuario principales que más contribuyeron a las llamadas a la API realizadas durante el periodo de actividad normal. También muestra el promedio de llamadas a la API o errores registrados por los agentes de usuario durante el periodo de actividad normal.

  Desde: 1.07

  Opcional: Falso

- **`value`**: uno de los cinco agentes de usuario principales que contribuyeron a las llamadas a la API o los errores registrados durante el periodo de actividad normal.

  Desde: 1.07

  Opcional: Falso

- **`average`**: el promedio histórico de llamadas a la API o errores por minuto durante los siete días anteriores a la hora de inicio de la actividad de Insights para el agente de usuario en el campo `value`.

  Desde: 1.07

  Opcional: Falso

- **`errorCode`**: un bloque que muestra hasta los cinco códigos de error principales que se produjeron en las llamadas a la API durante la actividad inusual y los periodos de referencia, en orden descendente desde el mayor número de llamadas a la API hasta el menor. También consulte `errorCode` en CloudTrail contenido del registro.

  Desde: 1.07

  Opcional: Falso

  - **`insight`**: un bloque que muestra hasta los cinco códigos de error principales que se produjeron en las llamadas a la API realizadas durante el periodo de actividad inusual, en orden descendente desde el mayor número de llamadas asociadas a la API hasta el menor. También muestra el número promedio de llamadas a la API en las que se produjeron los errores durante el periodo de actividad inusual.

    Desde: 1.07

    Opcional: Falso

    - **`value`**: uno de los cinco códigos de error principales que se produjo en las llamadas a la API realizadas durante el periodo de actividad inusual, tal como `AccessDeniedException`.

      Si ninguna de las llamadas que desencadenaron el evento de Insights produjo errores, este valor es `null`.

      Desde: 1.07

Opcional: Falso

- **`average`**: el número de llamadas a la API por minuto durante el periodo de actividad inusual para el código de error en el campo `value`.

  Si el valor del código de error es `null` y no hay otros códigos de error en el bloque `insight`, el valor del `average` es el mismo que el del bloque `statistics` para el evento de Insights en general.

  Desde: 1.07

  Opcional: Falso

- **`baseline`**: un bloque que muestra hasta los cinco códigos de error principales que se produjeron en las llamadas a la API realizadas durante el periodo de actividad normal. También muestra el promedio de llamadas a la API realizadas por los agentes de usuario durante el periodo de actividad normal.

  Desde: 1.07

  Opcional: Falso

  - **`value`**: uno de los cinco códigos de error principales que se produjo en las llamadas a la API realizadas durante el periodo normal de actividad, tal como `AccessDeniedException`.

    Desde: 1.07

    Opcional: Falso

  - **`average`**: el promedio histórico de llamadas a la API o errores por minuto durante los siete días anteriores a la hora de inicio de la actividad de Insights para el código de error en el campo `value`.

    Desde: 1.07

    Opcional: Falso

Ejemplo de bloque **`insightDetails`**

A continuación se muestra un ejemplo de un bloque `insightDetails` de evento de Insights para un evento de Insights que se produjo cuando se llamó una cantidad inusual de veces a la

API `CompleteLifecycleAction` de Application Auto Scaling. Para ver un ejemplo de un evento completo de Insights, consulte Referencia de eventos de registro de CloudTrail.

Este ejemplo proviene de un evento inicial de Insights, indicado por `"state": "Start"`. Las identidades de usuario principales, `CodeDeployRole1`, `CodeDeployRole2` y `CodeDeployRole3`, que llamaron a las API asociadas al evento de Insights, se muestran en el bloque `attributions`, junto con sus tasas promedio de llamadas a la API para este evento de Insights, y el valor de referencia para el rol `CodeDeployRole1`. El bloque `attributions` también muestra que el agente de usuario es `codedeploy.amazonaws.com`, lo que significa que las identidades de usuario principales utilizaron la consola AWS CodeDeploy para ejecutar las llamadas a la API.

Debido a que no hay códigos de error asociados a los eventos que se analizaron para generar el evento de Insights (el valor es`null`), el promedio de `insight` para el código de error es el mismo que el promedio general de `insight` para todo el evento de Insights, que se muestra en el bloque `statistics`.

```
          "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
```

```
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                    "average": 0.2
                  }
                ],
                "baseline": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
```

```
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        }
```

Eventos no generados por la API capturados por CloudTrail

Además de registrar llamadas a la API de AWS, CloudTrail captura otros eventos relacionados que podrían afectar la seguridad o conformidad de su cuenta de AWS o ayudar a solucionar problemas operativos.

Temas

- Eventos de servicio de AWS
- AWS Management Console eventos de inicio de sesión

Eventos de servicio de AWS

CloudTrail permite registrar eventos de servicios no generados por la API. Estos eventos se crean mediante los servicios de AWS, pero no se desencadenan directamente por una solicitud a una API pública de AWS. Para estos eventos, el campo `eventType` tiene el valor `AwsServiceEvent`.

A continuación, se muestra un escenario de ejemplo de un evento de servicio de AWS que se genera cuando una clave administrada por el cliente se rota automáticamente en AWS Key Management Service (AWS KMS). Para obtener más información sobre la rotación de claves de KMS, consulte Rotación de claves de KMS.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
```

```
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```


AWS Management Console eventos de inicio de sesión

CloudTrail registra los intentos de inicio de sesión en AWS Management Console los foros de AWS discusión y en el AWS Support Center. Todos los eventos de inicio de sesión de usuarios de IAM y usuarios raíz, así como todos los eventos de inicio de sesión de usuarios federados, generan registros en los archivos de registro. CloudTrail Para obtener más información acerca de cómo buscar y visualizar registros, consulte Búsqueda de los archivos de CloudTrail registro y Descarga de los archivos de registros de CloudTrail.

> **Note**
>
> La región registrada en un `ConsoleLogin` evento varía en función del tipo de usuario y de si utilizas un terminal global o regional para iniciar sesión.
>
> - Si inicias sesión como usuario root, CloudTrail graba el evento en us-east-1.
> - Si inicia sesión con un usuario de IAM y utiliza el punto final global, CloudTrail registra la región del `ConsoleLogin` evento de la siguiente manera:
>   - Si hay una cookie de alias de cuenta en el navegador, CloudTrail registra el `ConsoleLogin` evento en una de las siguientes regiones: us-east-2, eu-north-1 o ap-

southeast-2. Esto se debe a que el proxy de la consola redirige al usuario en función de la latencia desde la ubicación de inicio de sesión del usuario.

- Si no hay una cookie de alias de cuenta en el navegador, CloudTrail registra el `ConsoleLogin` evento en us-east-1. Esto se debe a que el proxy de la consola redirige de nuevo al inicio de sesión global.

- Si inicia sesión con un usuario de IAM y utiliza un punto final regional, CloudTrail registra el `ConsoleLogin` evento en la región correspondiente al punto final. Para obtener más información sobre los AWS Sign-In puntos finales, consulte AWS Sign-In puntos finales y cuotas.

Temas

- Ejemplos de registros de eventos de usuarios de IAM
- Ejemplos de registros de eventos para usuarios raíz
- Ejemplos de registros de eventos para usuarios federados

Ejemplos de registros de eventos de usuarios de IAM

Los siguientes ejemplos muestran registros de eventos de diferentes escenarios de inicio de sesión de usuario de IAM.

Temas

- Usuario de IAM, inicio de sesión correcto sin MFA
- Usuario de IAM, inicio de sesión correcto con MFA
- Usuario de IAM, inicio de sesión incorrecto
- Usuario de IAM, verificaciones de MFA del proceso de inicio de sesión (un solo tipo de dispositivo de MFA)
- Usuario de IAM, verificaciones de MFA del proceso de inicio de sesión (varios tipos de dispositivos de MFA)

Usuario de IAM, inicio de sesión correcto sin MFA

El siguiente registro muestra que un usuario denominado inició sesión `Anaya` correctamente en el AWS Management Console sin utilizar la autenticación multifactor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


Usuario de IAM, inicio de sesión correcto con MFA

El siguiente registro muestra que un usuario de IAM llamado inició sesión `Anaya` correctamente en el sistema AWS Management Console mediante autenticación multifactor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Usuario de IAM, inicio de sesión incorrecto

En el siguiente registro, se muestra que un usuario de IAM llamado `Paulo` intentó iniciar sesión sin éxito.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
```

```
}
```

Usuario de IAM, verificaciones de MFA del proceso de inicio de sesión (un solo tipo de dispositivo de MFA)

A continuación, se muestra que el proceso de inicio de sesión verificó si se requiere autenticación multifactor (MFA) para un usuario de IAM durante el inicio de sesión. En este ejemplo, el valor de `mfaType` es `U2F MFA`, lo que indica que el usuario de IAM habilitó un único dispositivo de MFA o varios dispositivos de MFA del mismo tipo (`U2F MFA`).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
```

```
    }
}
```

Usuario de IAM, verificaciones de MFA del proceso de inicio de sesión (varios tipos de dispositivos de MFA)

A continuación, se muestra que el proceso de inicio de sesión verificó si se requiere autenticación multifactor (MFA) para un usuario de IAM durante el inicio de sesión. En este ejemplo, el valor de `mfaType` es `Multiple MFA Devices`, lo que indica que el usuario de IAM habilitó varios tipos de dispositivos de MFA.

```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "IAMUser",
       "principalId": "EXAMPLE6E4XEGITWATV6R",
       "accountId": "123456789012",
       "accessKeyId": "",
       "userName": "Mary"
   },
   "eventTime": "2023-07-19T23:10:09Z",
   "eventSource": "signin.amazonaws.com",
   "eventName": "CheckMfa",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "192.0.2.0",
   "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0",
   "requestParameters": null,
   "responseElements": {
       "CheckMfa": "Success"
   },
   "additionalEventData": {
       "MfaType": "Multiple MFA Devices"
   },
   "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
   "readOnly": false,
   "eventType": "AwsConsoleSignIn",
   "managementEvent": true,
   "recipientAccountId": "123456789012",
   "eventCategory": "Management",
   "tlsDetails": {
       "tlsVersion": "TLSv1.3",
       "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Ejemplos de registros de eventos para usuarios raíz

En los siguientes ejemplos se muestran registros de eventos para varios escenarios de inicio de sesión del usuario `root`. Al iniciar sesión con el usuario root, CloudTrail registra el evento en us-east-1. `ConsoleLogin`

Temas

- Usuario raíz, inicio de sesión correcto sin MFA
- Usuario raíz, inicio de sesión correcto con MFA
- Usuario raíz, inicio de sesión incorrecto
- Usuario raíz, MFA cambiado
- Usuario raíz, contraseña cambiada

Usuario raíz, inicio de sesión correcto sin MFA

A continuación, se muestra un evento de inicio de sesión correcto para un usuario raíz sin autenticación multifactor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
```

```
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Usuario raíz, inicio de sesión correcto con MFA

A continuación, se muestra un evento de inicio de sesión correcto para un usuario raíz con autenticación multifactor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


Usuario raíz, inicio de sesión incorrecto

A continuación, se muestra un evento de inicio de sesión correcto para un usuario raíz que no utiliza MFA.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


Usuario raíz, MFA cambiado

A continuación se muestra un evento de ejemplo para un usuario raíz que cambia la configuración de autenticación multifactor (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Usuario raíz, contraseña cambiada

A continuación se muestra un evento de ejemplo para un usuario raíz que cambia su contraseña.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
}
```

Ejemplos de registros de eventos para usuarios federados

En los siguientes ejemplos se muestran registros de eventos de usuarios federados. Los usuarios federados reciben credenciales de seguridad temporales para acceder a los AWS recursos mediante una solicitud. `AssumeRole`

A continuación se muestra un evento de ejemplo de una solicitud de cifrado de federación. El identificador de clave de acceso original se proporciona en el campo `accessKeyId` del elemento `userIdentity`. El campo `accessKeyId` de `responseElements` contiene un nuevo identificador de clave de acceso si el valor de `sessionDuration` solicitado se incluye en la solicitud de cifrado; de lo contrario, contiene el valor del identificador de clave de acceso original.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
```

```
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
```

```
    }
}
```

A continuación, se muestra un evento de inicio de sesión de un usuario federado; sin autenticación multifactor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
```

```
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Historial del documento

En la siguiente tabla se describen los cambios importantes en la documentación de AWS CloudTrail. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

- Versión de la API: 01-11-2013
- Última actualización de la documentación: 2 de abril de 2020

Cambio	Descripción	Fecha
Se agregó compatibilidad para los servicios	Esta versión es compatible con Deadline Cloud. AWS Para obtener más información, consulte Servicio de AWS los temas de CloudTrail.	2 de abril de 2024
Funcionalidad agregada	La versión del AWS CloudTrai l evento ahora es la 1.10. Para obtener más informaci ón, consulte el contenido del CloudTrail registro.	26 de marzo de 2024
Se agregó compatibilidad para los servicios	Esta versión admite AWS Billing Conductor. Para obtener más información, consulta Servicio de AWS los temas sobre cómo registrar CloudTrail las llamadas a la AWS Billing Conductor API y su uso AWS CloudTrail.	12 de marzo de 2024
Funcionalidad agregada	Ahora puede registrar CloudTrail los eventos de datos en los AWS X-Ray rastreos y los nodos AWS	7 de marzo de 2024

	Systems Manager gestionados mediante selectores de eventos avanzados. Para obtener más información, consulte Eventos de datos.	
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en los dominios de Amazon Simple Workflow Service (Amazon SWF) mediante selectores de eventos avanzados. Para obtener más información, consulte Eventos de datos.	14 de febrero de 2024
Funcionalidad agregada	CloudTrail agregó la `ListInsightsMetricData` API. La `ListInsightsMetricData` API devuelve los datos de las métricas de Insights para las rutas que han activado Insights. Para obtener más información, consulta ListInsightsMetricDatala referencia de la AWS CloudTrail API.	6 de febrero de 2024
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos para AWS IoT y AWS AppConfig mediante selectores de eventos avanzados. AWS IoT SiteWise Para obtener más información, consulte Eventos de datos.	4 de enero de 2024

Funcionalidad agregada	Ahora puede registrar eventos CloudTrail de datos AWS IoT Greengrass mediante selectores de eventos avanzados. Para obtener más información, consulte Eventos de datos.	22 de diciembre de 2023
Compatibilidad con nuevas regiones	CloudTrail amplió el apoyo a una nueva región, la región de Canadá Oeste (Calgary) . Para obtener más informaci ón, consulta las regiones CloudTrail compatibles.	20 de diciembre de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos para Amazon Keyspaces (para Apache Cassandra), AWS IoT TwinMaker Amazon RDS y AWS Supply Chain mediante selectores de eventos avanzados. Para obtener más información, consulte Eventos de datos.	20 de diciembre de 2023
Política AWS gestionada actualizada	Se actualizó la política administrada CloudTrai lServiceRolePolicy para permitir las siguientes acciones en el almacén de datos de eventos de una organización cuando la federación está deshabili tada: `glue:DeleteTable` y `lakeformation:Dere gisterResource` .	26 de noviembre de 2023

Funcionalidad agregada	Ahora puede federar un banco de datos de eventos de CloudTrail Lake para ver los metadatos asociados al banco de datos de eventos en el catálogo de AWS Glue datos y ejecutar consultas SQL sobre los datos de eventos con Amazon Athena. Los metadatos de la tabla almacenados en el catálogo de AWS Glue datos permiten al motor de consultas de Athena saber cómo buscar, leer y procesar los datos que desea consultar. Para obtener más información, consulte Federación de un almacén de datos de eventos.	26 de noviembre de 2023
Funcionalidad agregada	Ahora puede registrar eventos CloudTrail de datos AWS Cloud Map mediante selectore s de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	16 de noviembre de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en los mensajes de Amazon SQS mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	16 de noviembre de 2023

Funcionalidad agregada	CloudTrail Lake ahora ofrece dos opciones de precios para los almacenes de datos de eventos: un precio de retención prorrogable por un año y un precio de retención por siete años. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Antes de esta versión, todos los almacenes de datos de eventos utilizaban la opción de precios de retención de siete años. Puede cambiar un almacén de datos de eventos de usar la opción de precio de retención de siete años a usar el precio de retención prorrogable de un año mediante la CloudTrail consola o la operación de API. AWS CLIUpdateEventDataStore Para obtener más información sobre las opciones de precios, consulte Precios de AWS CloudTrail y opciones de precios del almacén de datos de eventos.	15 de noviembre de 2023

Funcionalidad agregada	Ahora puede recopilar los eventos de Insights en Lake. CloudTrail AWS CloudTrail Gracias al análisis continuo de los eventos de CloudTrai l gestión, Insights ayuda a AWS los usuarios a identific ar y responder a las actividad es inusuales asociadas a las llamadas a las API y a las tasas de error de las API. Para recopilar los eventos de Insights en CloudTrail Lake, necesita un almacén de datos de eventos de origen que registre los eventos de administración y habilite Insights, y un banco de datos de eventos de destino que recopile los eventos de Insights en función de una actividad inusual de eventos de administración en el almacén de datos de eventos de origen. Para obtener más información, consulte Crear un banco de datos de eventos para los eventos de CloudTrai l Insights y Registrar los eventos de Insights.	9 de noviembre de 2023

Se agregó compatibilidad para los servicios	Esta versión admite AWS Launch Wizard. Para obtener más información, consulte Servicio de AWS los temas sobre el uso de las llamadas a la AWS Launch Wizard API CloudTrail y el registro de llamadas a la API AWS CloudTrail.	8 de noviembre de 2023
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Bedrock. Para obtener más información, consulte Servicio de AWS los temas CloudTrail y registre las llamadas a la API de Amazon Bedrock mediante AWS CloudTrail.	23 de octubre de 2023
Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos en CodeWhisperer las personalizaciones de Amazon mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	18 de octubre de 2023

Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en bases de datos y tablas de Amazon Timestream mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	28 de septiembre de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en temas de Amazon SNS y puntos de enlace de la plataform a mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	28 de septiembre de 2023
Documentación actualizada	Se agregó una tabla para mostrar las tareas que pueden realizar la cuenta de administr ación, las cuentas de administr ador delegado y las cuentas de los miembros de una AWS Organizations organizac ión. CloudTrail Para obtener más información, consulte Organization delegated administrator (Administrador delegado de la organización).	25 de septiembre de 2023

Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Marketplace los acuerdos. Para obtener más información, consulte Servicio de AWS los temas sobre cómo registrar CloudTrail las llamadas a la API de acuerdos y su uso AWS CloudTrail.	1 de septiembre de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en las transmisiones de vídeo de Amazon Kinesis y en los SageMaker puntos de enlace de Amazon mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	31 de agosto de 2023
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Application Transformation Service. AWS Application Transformation Service es un servicio de backend utilizado por servicios como AWS Microservice Extractor para .NET. Para obtener más información, consulte los servicios e CloudTrail integraciones compatibles.	26 de agosto de 2023

Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en AWS Private CA Connector for Active Directory mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	24 de agosto de 2023
Documentación actualizada	Se agregaron nuevos tutoriales de CloudTrail Lake para mostrar cómo crear almacenes de datos de eventos, ver los paneles de CloudTrail Lake, copiar eventos de senderos en un almacén de datos de eventos, ver y ejecutar consultas de muestra y guardar los resultados de las AWS Management Console consultas en un bucket de Amazon S3 mediante. Para obtener más información, consulte los tutoriales de Lake CloudTrail	16 de agosto de 2023
Compatibilidad con nuevas regiones	CloudTrail amplió el apoyo a una nueva región, la región de Israel (Tel Aviv). Para obtener más información, consulta las regiones CloudTrail compatibles.	1 de agosto de 2023

Se agregó compatibilidad para los servicios	Esta versión admite AWS HealthImaging. Para obtener más información, consulta los servicios e integraciones CloudTrail compatibles y el registro de llamadas a la AWS HealthImaging API mediante AWS CloudTrail.	26 de julio de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en los almacenes AWS HealthIma ging de datos mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	26 de julio de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en los canales AWS Systems Manager de control y las redes Amazon Managed Blockchai n mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	21 de junio de 2023

Funcionalidad agregada	Ahora puede verificar los resultados de las consultas guardadas en CloudTrail Lake mediante el aws cloudtrail verify-query-results comando. Para obtener más información, consulte Validar los resultados de consultas guardados con la AWS CLI.	21 de junio de 2023
Se agregó compatibilidad para los servicios	Esta versión es compatibl e con Amazon Verified Permissions. Para obtener más información, consulta los servicios e integraciones CloudTrail compatibles y el registro de llamadas a la API de permisos verificados de Amazon mediante AWS CloudTrail.	13 de junio de 2023
Funcionalidad agregada	Ahora puede usar los paneles de CloudTrail Lake para visualizar los eventos en un almacén de datos de eventos. Para obtener más información, consulte Ver los paneles de Lake.	13 de junio de 2023

Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos en los almacenes de políticas de permisos verificados de Amazon mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	13 de junio de 2023
Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos en un CodeWhisperer perfil de Amazon mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	6 de junio de 2023
Funcionalidad agregada	Ahora puedes iniciar y detener la ingesta de eventos en los almacenes de datos de CloudTrail eventos. Para obtener información sobre cómo detener la ingesta de eventos mediante la consola, consulte Evitar que un almacén de datos de eventos ingiera eventos. Para obtener información sobre cómo detener la ingesta de eventos mediante el AWS CLI, consulte Detener la ingestión en un banco de datos de eventos.	2 de junio de 2023

Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en un espacio de trabajo de registro de escritura anticipada de Amazon EMR mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	31 de mayo de 2023
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Security Lake. Para obtener más informaci ón, consulte los servicios e integraciones CloudTrail compatibles y el registro de llamadas a la API de Amazon Security Lake mediante AWS CloudTrail.	30 de mayo de 2023
Documentación actualizada	Se actualizó CloudTrail el tema del elemento UserIdent ity para incluir un ejemplo y descripciones de campos para una solicitud realizada en nombre de un usuario del Centro de Identidad de IAM. Para obtener más información, consulte Elemento userIdentity de CloudTrail .	23 de mayo de 2023

Documentación actualizada	Esta actualización es compatible con la siguiente versión de parche para la biblioteca de CloudTrail procesamiento: -1.6.1.jar. aws-cloudtrail-processing-library Para obtener más información, consulte Uso de la biblioteca de CloudTrail procesamiento y la biblioteca de CloudTrail procesamiento en. GitHub	23 de mayo de 2023
Funcionalidad agregada	CloudTrail Lake ahora es compatible con todas las funciones y operadores de Presto. Para obtener más información, consulte Restricciones SQL de CloudTrail Lake.	9 de mayo de 2023
Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos en un GuardDuty detector de Amazon mediante selectores de eventos avanzados. Para obtener más información, consulta Registrar eventos de datos y Registrar llamadas a la GuardDuty API de Amazon con AWS CloudTrail.	30 de marzo de 2023

Documentación actualizada	Se ha agregado una nueva sección sobre la creación de etiquetas de asignación de costos definidas por el usuario para los almacenes de datos de eventos. Para obtener más información, consulte Crear etiquetas de asignación de costes definidas por el usuario para los almacenes de datos de eventos de CloudTrail Lake.	24 de marzo de 2023
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Telco Network Builder (AWS TNB). Para obtener más información, consulte los servicios e integraciones CloudTrail compatibles y el registro de llamadas a la API de AWS Telco Network Builder mediante. AWS CloudTrail	21 de febrero de 2023
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en los grupos de identidades de Amazon Cognito mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	15 de febrero de 2023

Documentación actualizada	Se agregó una nueva sección sobre los recursos de aprendizaje disponibles para CloudTrail Lake. Para obtener más información, consulte Learning resources (Recursos de aprendizaje).	9 de febrero de 2023
Funcionalidad agregada	Ahora puede crear integraciones de CloudTrail Lake con fuentes de AWS eventos externas a. Puede registrar y almacenar datos de actividad de los usuarios desde cualquier origen en sus entornos híbridos, como aplicaciones internas o de SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores. Para obtener más información, consulte Crear una integración con un origen de eventos externo a AWS.	31 de enero de 2023
Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos sobre la CloudTrail `PutAuditEvents` actividad en un canal de CloudTrail Lake mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	31 de enero de 2023

Compatibilidad con nuevas regiones	CloudTrail amplió el apoyo a una nueva región, la región de Asia Pacífico (Melbourne). Para obtener más informaci ón, consulta las regiones CloudTrail compatibles.	24 de enero de 2023
Documentación actualizada	Se agregó una nueva sección sobre la administración de la coherencia de los datos en CloudTrail, consulte Administr ar la consistencia de los datos en CloudTrail.	18 de enero de 2023
Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos en las tiendas de SageMaker características de Amazon mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	27 de diciembre de 2022
Se agregó compatibilidad para los servicios	Esta versión es compatibl e con AWS Marketplace Discovery. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	15 de diciembre de 2022

Funcionalidad agregada	Ahora puedes registrar eventos de CloudTrail datos en los componentes de prueba del experimento de Amazon SageMaker Metrics mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	15 de diciembre de 2022
Funcionalidad agregada	Ahora puede crear un almacén de datos de eventos para incluir los elementos de AWS Config configuración y utilizar el almacén de datos de eventos para investigar los cambios no conformes en sus entornos de producción. Para obtener más informaci ón, consulte Crear un banco de datos de eventos para los elementos AWS Config de configuración.	28 de noviembre de 2022
Compatibilidad con nuevas regiones	CloudTrail amplió el apoyo a una nueva región, la región de Asia Pacífico (Hyderabad). Para obtener más informaci ón, consulta las regiones CloudTrail compatibles.	22 de noviembre de 2022

Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en Amazon FinSpace entornos mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	18 de noviembre de 2022
Compatibilidad con nuevas regiones	CloudTrail amplió el soporte a una nueva región, la región de Europa (España). Para obtener más informaci ón, consulta las regiones CloudTrail compatibles.	16 de noviembre de 2022
Compatibilidad con nuevas regiones	CloudTrail amplió el apoyo a una nueva región, la región de Europa (Zúrich). Para obtener más información, consulta las regiones CloudTrail compatibl es.	9 de noviembre de 2022
Funcionalidad agregada	La cuenta de administración de una AWS Organizations organización ahora puede añadir un administrador delegado para gestionar los almacenes de datos de CloudTrail rutas y eventos de la organización. Para obtener más información, consulte Organization delegated administrator (Administrador delegado de la organización).	7 de noviembre de 2022

Funcionalidad agregada	Ahora puede habilitar el AWS Key Management Service cifrado de un almacén de datos de eventos de CloudTrail Lake. Para obtener más información, consulte Create an event data store (Creación de un almacén de datos de eventos).	7 de noviembre de 2022
Funcionalidad agregada	Ahora puede guardar los resultados de las consultas de CloudTrail Lake en un bucket de Amazon S3 al ejecutar una consulta. Para obtener más información sobre cómo ejecutar una consulta, consulte Ejecutar una consulta y guardar los resultados de la consulta. Para obtener más información sobre la descarga de los resultados de consultas, consulte Obtener y descargar los resultados de consultas guardados.	21 de octubre de 2022
Funcionalidad agregada	Ahora puede copiar los eventos de los CloudTrail senderos a un almacén de datos de eventos de CloudTrail Lake. Para obtener más información, consulte Copiar eventos de senderos en CloudTrail Lake.	19 de septiembre de 2022

Documentación actualizada	Se agregó una lista de CloudWatch métricas de Amazon compatibles con CloudTrail Lake. Para obtener más informaci ón, consulta CloudWatch Métricas compatibles.	16 de septiembre de 2022
Funcionalidad agregada	Ahora puede ver los canales CloudTrail vinculados al servicio mediante. AWS CLI Para obtener más informaci ón, consulte Visualización de canales vinculados al servicio mediante el CloudTrail . AWS CLI	9 de septiembre de 2022
Compatibilidad con nuevas regiones	CloudTrail amplió el soporte a una nueva región, la región de Oriente Medio (EAU). Para obtener más informaci ón, consulta las regiones CloudTrail compatibles.	30 de agosto de 2022
Documentación actualizada	Se agregó una lista de servicios que proporcionan información sobre el TLS a CloudTrail. Para obtener más información, consulte los servicios que admiten los detalles de TLS en. CloudTrail	19 de julio de 2022

Funcionalidad modificada	CloudTrail ha cambiado el nombre de la política gestionada `AWSCloudTrailReadOnlyAccess` a `AWSCloudTrail_ReadOnlyAccess`. Se han reducido los permisos de esta política. De forma predeterminada, la política ya no concede permiso para publicar todos los buckets, AWS Lambda funciones o AWS KMS alias de Amazon S3. Para obtener más información, consulte Acceso de solo lectura.	6 de junio de 2022
Funcionalidad modificada	Como práctica recomendada de seguridad, ahora puede agregar un `aws:SourceArn` o una clave de condición `aws:SourceAccount` a un bloqueo de comprobación ACL `s3:GetBucketAcl` en las políticas de bucket de Amazon S3. Para obtener más información, consulte Configurar las políticas de bucket de Amazon S3 para CloudTrail.	11 de mayo de 2022

Funcionalidad modificada	A partir del 24 de febrero de 2022, AWS CloudTrail empecé a cambiar los valores de los `sourceIPAddress` campos `userAgent` y, en cualquier caso, si se originaban en una AWS Management Console sesión en la que se utilizaba un cliente proxy. Para estos eventos, CloudTrail reemplaza los valores de los `sourceIPAddress` campos `userAgent` y por `AWS Internal`. CloudTrailrealizó este cambio para estandarizar la forma en que se registra la información para las acciones de servicio en todos los AWS servicios. Para obtener más información, consulte el contenido del CloudTrail registro.	12 de abril de 2022
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon GameSparks. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	24 de marzo de 2022
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS App Mesh Envoy Management Service. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	18 de marzo de 2022

Documentación actualizada	Se han agregado nuevos ejemplos de consultas para CloudTrail Lake, una nueva función que le permite ejecutar consultas SQL detalladas y de varios campos en sus eventos. Además, se ha agregado un nuevo campo, `BytesScanned`, a los resultados de los metadatos de las consultas de las operaciones `DescribeQuery` y `GetQueryResults`. Para obtener más información, consulte Trabajar con Lake. CloudTrail	4 de marzo de 2022

Funcionalidad modificada	CloudTrail ahora elimina el ID de cuenta del propietario del bucket de Amazon S3 en el `resources` bloque de un evento de datos si se cumplen las dos condiciones siguientes: la llamada a la API del evento de datos proviene de una AWS cuenta diferente a la del propietario del bucket de Amazon S3 y la persona que llama a la API ha recibido un `AccessDenied` error que solo afecta a la cuenta de la persona que llama. Para obtener más información, consulte Eliminación de los ID de las cuentas de los propietarios de los buckets para eventos de datos llamados por otras cuentas.	3 de marzo de 2022

Documentación actualizada	Esta actualización es compatible con la siguiente versión de la biblioteca de CloudTrail procesamiento: se agregó soporte para implementar un administrador S3 personalizado, registro de eventos para registrar excepciones relacionadas con el análisis de archivos, soporte para analizar un `errorCode` campo opcional y se actualizó la expresión regular de análisis de ID de cuenta para aceptar valores no numéricos. `insightDetails` Para obtener más información, consulte Uso de la biblioteca de procesamiento y la biblioteca de CloudTrail procesamiento en. CloudTrail GitHub	28 de enero de 2022

Funcionalidad agregada	CloudTrail presenta CloudTrail Lake, una nueva función que le permite ejecutar consultas SQL detalladas de varios campos en sus eventos. Los eventos se agregan en almacenes de datos de eventos, que son colecciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Para obtener más información, consulte Trabajar con Lake. CloudTrail	5 de enero de 2022
Compatibilidad con nuevas regiones	CloudTrail amplió el apoyo a una nueva región, la región de Asia Pacífico (Yakarta). Para obtener más información, consulta las regiones CloudTrail compatibles.	13 de diciembre de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon WorkSpaces Web. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	3 de diciembre de 2021

Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en AWS Glue tablas creadas por Lake Formation mediante selectore s de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	30 de noviembre de 2021
Funcionalidad modificada	Como práctica recomenda da de seguridad, ahora puede añadir una clave de `aws:SourceAccount` condición `aws:SourceArn` o clave a las políticas AWS KMS clave y a las políticas de bucket de Amazon S3. Para obtener más información, consulte Configurar políticas AWS KMS clave CloudTrail y Configurar políticas de bucket de Amazon S3 para CloudTrai l.	15 de noviembre de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatibl e con AWS Resilience Hub. Consulte Servicios e integraci ones admitidos con AWS CloudTrail.	10 de noviembre de 2021

Funcionalidad agregada	Hay disponible un nuevo tipo de evento de CloudTrail Insights: eventos de Insights con tasa de error. Un evento de índice de errores de Insights captura una actividad inusual en un error que se produce en las API llamadas de su cuenta. Para obtener más información, consulte Registro de eventos de datos para registros de seguimiento.	10 de noviembre de 2021
Funcionalidad agregada	Ahora puede registrar eventos de CloudTrail datos en transmisiones de DynamoDB mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	22 de septiembre de 2021
Funcionalidad agregada	Ahora puede registrar eventos de datos en puntos de acceso de Amazon S3. Puede registrar eventos de datos de puntos de acceso de Amazon S3 mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	24 de agosto de 2021

Funcionalidad modificada	Cuando configura una ruta para enviar notificaciones a Amazon SNS, CloudTrail agrega una declaración de política a su política de acceso a temas de SNS que permite enviar contenido CloudTrail a un tema de SNS. Como práctica recomendada de seguridad, le recomendamos que añada una clave de `aws:SourceAccount` condición `aws:SourceArn` o clave a la CloudTrail declaración de política. Para obtener más información, consulte la política temática de Amazon SNS para. CloudTrail	16 de agosto de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con el controlador de recuperación de aplicaciones Amazon Route 53. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	27 de julio de 2021

Funcionalidad agregada	Ahora puede registrar eventos de datos en las API directas de Amazon EBS que se ejecutan en instantáneas de EBS. Puede registrar eventos de datos en la API directa de Amazon EBS mediante selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	27 de julio de 2021
Funcionalidad modificada	Cuando CloudTrail procesa eventos de datos, conserva los números en su formato original, ya sea un entero (`int`) o un`float`. En los eventos que tienen números enteros en los campos de un evento de datos, CloudTrai l históricamente procesaba estos números como flotantes . Ahora, CloudTrail mantiene el formato original de los números enteros en los eventos de datos. Para obtener más información, consulte Uso de la biblioteca CloudTrail de procesamiento.	13 de julio de 2021

Funcionalidad agregada	Ahora puede excluir de sus registros de seguimiento los eventos de administración de la API de datos de Amazon RDS. Para obtener más información, consulte Registro de eventos de administración para registros de seguimiento.	1 de julio de 2021
Se agregó compatibilidad para los servicios	Esta versión admite AWS BugBust. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	24 de junio de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Managed Grafana y Amazon Managed Service for Prometheus. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	2 de junio de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS App Runner. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	18 de mayo de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Systems Manager Incident Manager. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	10 de mayo de 2021

Documentación actualizada	Esta actualización describe los requisitos de registro de eventos de datos para los paquetes de AWS Config conformidad, especialmente para los marcos de cumplimiento como HIPAA o FedRAMP. Para obtener más información, consulte Registro de eventos de datos.	7 de mayo de 2021
Se agregó compatibilidad para los servicios	Esta versión admite Service Quotas y API directas de Amazon EBS. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	13 de abril de 2021
Funcionalidad agregada	Una vez que un administrador de IAM realiza la configuración AWS STS, CloudTrail registra la `sourceIdentity` información en los eventos cuando los usuarios asumen una función de IAM o realizan cualquier acción con la función asumida. Para obtener más información, consulte Elemento userIdentity de CloudTrail .	13 de abril de 2021

Documentación actualizada	Esta actualización documenta los límites, en kilobytes (KB), del contenido de algunos campos de registro de eventos. CloudTrail Para obtener más información, consulte el contenido del CloudTrail registro.	8 de abril de 2021
Funcionalidad agregada	Una vez que un administrador de IAM realiza la configuración AWS STS, CloudTrail registra la `sourceIdentity` información en los eventos cuando los usuarios asumen una función de IAM o realizan cualquier acción con la función asumida. Para obtener más información, consulte Elemento userIdentity de CloudTrail .	6 de abril de 2021
Funcionalidad agregada	Ahora puede registrar eventos de datos en tablas de Amazon DynamoDB. Puede registrar eventos de datos de DynamoDB mediante selectores de eventos o selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	23 de marzo de 2021

Se agregó compatibilidad para los servicios	Esta versión admite Amazon Managed Workflows for Apache Airflow Consulte Servicios e integraciones admitidos con AWS CloudTrail.	22 de marzo de 2021
Funcionalidad agregada	Ahora puede registrar eventos de datos en puntos de acceso S3 Object Lambda si ha elegido utilizar selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	18 de marzo de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Fault Injection Simulator. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	15 de marzo de 2021
Funcionalidad agregada	Ahora puede registrar eventos de datos en nodos Ethereum en Amazon Managed Blockchain si ha elegido utilizar selectores de eventos avanzados. Para obtener más información, consulte Registro de eventos de datos.	1 de marzo de 2021

Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Managed Blockchain y la versión preliminar de Ethereum for Managed Blockchain. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	4 de febrero de 2021
Se agregó compatibilidad para los servicios	Esta versión admite AWS Amplify. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	3 de febrero de 2021
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Lookout for Metrics. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	1 de febrero de 2021
Documentación actualizada	Esta actualización es compatible con la siguiente versión de parche para la biblioteca de CloudTrail procesamiento: actualice las referencias del archivo.jar en la guía del usuario para usar la versión más reciente, aws-cloudtrail-processing-library -1.4.0.jar. Para obtener más información, consulte Uso de la biblioteca de CloudTrail procesamiento y la CloudTrail biblioteca de procesamiento en. GitHub	12 de enero de 2021

Funcionalidad agregada	Ahora puede registrar eventos de datos en Amazon S3 en AWS Outposts. Para obtener más información, consulte Registro de eventos de datos.	21 de diciembre de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Lookout for Equipment AWS Well-Architected Tool y Amazon Location Service. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	16 de diciembre de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con la versión AWS IoT Greengrass 2. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	15 de diciembre de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon EMR en EKS. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	10 de diciembre de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Audit Manager y Amazon HealthLake. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	8 de diciembre de 2020

Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Lookout for Vision. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	1 de diciembre de 2020
Funcionalidad agregada	La versión del AWS CloudTrail evento ahora es la 1.08. La versión 1.08 introduce nuevos campos para. CloudTrail Para obtener más información, consulte el contenido de los CloudTrail registros.	24 de noviembre de 2020
Funcionalidad agregada	AWS CloudTrail presenta selectores de eventos avanzados para eventos de datos. Los selectores de eventos avanzados permiten un control más preciso de los eventos de datos que se registran en el registro de seguimiento. Puede incluir o excluir eventos de datos para AWS recursos específicos y seleccionar API específicas en esos recursos para registrarlos en su registro. Para obtener más información, consulte Registro de eventos de datos.	24 de noviembre de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Network Firewall. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	17 de noviembre de 2020

Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Trusted Advisor. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	22 de octubre de 2020
Documentación actualizada	Se han agregado dos nuevos ejemplos de registros de eventos para eventos de inicio de sesión de usuario raíz. Para obtener más información, consulte AWS Eventos de inicio de sesión en la consola de .	13 de octubre de 2020
Funcionalidad modificada	Se han reducido los permisos de la política `AWSCloudTrail_FullAccess` . Esta política ya no le permite eliminar temas de Amazon SNS ni buckets de Amazon S3 y la acción `getObject` se ha eliminado. Para obtener más información, consulte Otorgar permisos personalizados a los CloudTrail usuarios.	29 de septiembre de 2020

Documentación actualizada	Esta actualización es compatible con la siguiente versión de parches para la biblioteca de CloudTrail procesamiento: actualice las referencias al archivo.jar en la guía del usuario para que usen la versión más reciente, aws-cloudtrail-processing-library -1.3.0.jar. Para obtener más información, consulte Uso de la biblioteca de CloudTrail procesamiento y la CloudTrail biblioteca de procesamiento en. GitHub	28 de agosto de 2020
Se agregó compatibilidad para los servicios	Esta versión admite AWS Outposts. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	28 de agosto de 2020

Funcionalidad agregada	AWS CloudTrail Insights presenta campos de atribución para los eventos de CloudTrai l Insights. Los campos de atribuciones muestran las principales identidades de usuario, agentes de usuario y códigos de error asociados a la actividad anormal que desencadena eventos de Insights. Para la comparaci ón, los campos de atribucio nes también muestran las principales identidades de usuario, agentes de usuario y códigos de error asociados a la actividad normal o de referencia. Para obtener más información, consulte Registro de eventos de datos para registros de seguimiento.	13 de agosto de 2020
Funcionalidad agregada	La AWS CloudTrail consola tiene un nuevo aspecto diseñado para que sea más fácil de usar. La guía del AWS CloudTrail usuario se ha actualizado con cambios en los procedimientos para realizar las tareas en la consola, como la creación de rutas, la actualización de las rutas y la descarga del historial de eventos.	13 de agosto de 2020

Se agregó compatibilidad para los servicios	Esta versión admite Amazon Interactive Video Service. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	15 de julio de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Honeycode. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	24 de junio de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Macie. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	19 de mayo de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Kendra. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	13 de mayo de 2020
Se agregó compatibilidad para los servicios	Esta versión admite AWS IoT SiteWise. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	29 de abril de 2020
Se agregó compatibilidad con regiones	Esta versión es compatible con una región más: Europa (Milán). Consulte Regiones compatibles de AWS CloudTrail.	28 de abril de 2020

Servicio y compatibilidad regional agregados	Esta versión es compatible con Amazon AppFlow. Consulte Servicios e integraciones admitidos con AWS CloudTrail. También se ha agregado soporte a la región de África (Ciudad del Cabo). Consulte Regiones compatibles de AWS CloudTrail.	22 de abril de 2020
Funcionalidad agregada	AWS KMS Las acciones de gran volumen`Encrypt`, como`Decrypt`, y ahora `GenerateDataKey` se registran como eventos de lectura. Si optas por registrar todos los AWS KMS eventos de tu ruta y también por registrar los eventos de gestión de Write, tu ruta registrará AWS KMS las acciones relevantes`Disable`, como: `Delete` y`ScheduleKey` .	7 de abril de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon CodeGuru Reviewer. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	7 de febrero de 2020
Se agregó compatibilidad para los servicios	Esta versión es compatible con el servicio Amazon Managed Apache Cassandra. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	17 de enero de 2020

Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Connect. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	13 de diciembre de 2019
Documentación actualizada	Esta actualización es compatible con la siguiente versión de parche para la biblioteca de CloudTrail procesamiento: actualice las referencias del archivo.jar en la guía del usuario para usar la versión más reciente, aws-cloudtrail-processing-library -1.2.0.jar. Para obtener más información, consulte Uso de la biblioteca de CloudTrail procesamiento y la CloudTrail biblioteca de procesamiento en. GitHub	21 de noviembre de 2019
Funcionalidad agregada	Esta versión es compatible con AWS CloudTrail Insights, que le ayuda a detectar actividades inusuales en su cuenta. Consulte Registro de eventos de información para registros de seguimiento.	20 de noviembre de 2019
Funcionalidad agregada	En esta versión se añade una opción para filtrar AWS Key Management Service los eventos y eliminarlos de un rastro. Consulte Creación de un registro de seguimiento.	20 de noviembre de 2019

Se agregó compatibilidad para los servicios	Esta versión admite AWS CodeStar las notificaciones. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	7 de noviembre de 2019
Funcionalidad agregada	Esta versión permite añadir etiquetas al crear una ruta de acceso CloudTrail, tanto si se utiliza la CloudTrail consola como la API. Esta versión agrega dos nuevas API, `GetTrail` y `ListTrails` .	1 de noviembre de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS App Mesh. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	17 de octubre de 2019
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Translate. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	17 de octubre de 2019
Actualización de la documentación	El tema Servicios no compatibles se ha restaurado y actualizado para incluir solo los AWS servicios que actualmente no registran eventos. CloudTrail Consulte CloudTrail Servicios no compatibles.	7 de octubre de 2019

Actualización de la documentación	La documentación se ha actualizado con cambios en la política de `AWSCloudTrailFullAccess` . Se ha actualizado una política de ejemplo que muestra permisos equivalentes a `AWSCloudTrailFullAccess` para restringir los recursos sobre los que puede actuar la acción de `iam:PassRole` a aquellos que coinciden con la siguiente declaración de condición: `"iam:PassedToService": "cloudtrail.amazonaws.com"` . Consulte AWS CloudTrail Políticas de ejemplo basadas en la identidad.	24 de septiembre de 2019
Actualización de la documentación	La documentación se ha actualizado con un nuevo tema, Gestión de CloudTrail costes, para ayudarle a obtener los datos de CloudTrail registro que necesita sin salirse del presupuesto.	3 de septiembre de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS Control Tower. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	13 de agosto de 2019

Se agregó compatibilidad con regiones	Esta versión es compatible con una región más: Medio Oriente (Baréin). Consulte Regiones compatibles de AWS CloudTrail.	29 de julio de 2019
Actualización de la documentación	La documentación se ha actualizado con información sobre la seguridad de CloudTrail. Consulte Seguridad en AWS CloudTrail.	3 de julio de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS Ground Station. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	6 de junio de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS IoT Things Graph. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	4 de junio de 2019
Se agregó compatibilidad para los servicios	Esta versión admite Amazon AppStream 2.0. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	25 de abril de 2019
Se agregó compatibilidad con regiones	Esta versión es compatible con una región más: Asia Pacífico (Hong Kong). Consulte Regiones compatibles de AWS CloudTrail.	24 de abril de 2019

Se agregó compatibilidad para los servicios	Esta versión es compatible con el Amazon Managed Service para Apache Flink. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	22 de marzo de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS Backup. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	4 de febrero de 2019
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon WorkLink. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	23 de enero de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS Cloud9. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	21 de enero de 2019
Se agregó compatibilidad para los servicios	Esta versión admite AWS Elemental MediaLive. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	19 de enero de 2019
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Comprehend. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	18 de enero de 2019

Se agregó compatibilidad para los servicios	Esta versión admite AWS Elemental MediaPackage. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	21 de diciembre de 2018
Se agregó compatibilidad con regiones	Esta versión es compatible con una región más: UE (Estocolmo). Consulte Regiones compatibles de AWS CloudTrail.	11 de diciembre de 2018
Actualización de la documentación	La documentación se ha actualizado con información sobre los servicios admitidos y no admitidos. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	3 de diciembre de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Resource Access Manager (AWS RAM). Consulte Servicios e integraciones admitidos con AWS CloudTrail.	20 de noviembre de 2018
Funcionalidad actualizada	Esta versión permite crear un registro CloudTrail que registre los eventos de todas AWS las cuentas de una organización en AWS Organizations. Consulte Creación de un registro de seguimiento para una organización.	19 de noviembre de 2018

Se agregó compatibilidad para los servicios	Esta versión es compatible con la API de SMS y voz de Amazon Pinpoint. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	16 de noviembre de 2018
Se agregó compatibilidad para los servicios	Esta versión admite AWS IoT Greengrass. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	29 de octubre de 2018
Documentación actualizada	Esta actualización es compatible con la siguiente versión del parche para la biblioteca de CloudTrail procesamiento: actualice las referencias al archivo.jar en la guía del usuario para usar la versión más reciente, aws-cloudtrail-processing-library -1.1.3.jar. Para obtener más información, consulte Uso de la biblioteca de CloudTrail procesamiento y la CloudTrail biblioteca de procesamiento en. GitHub	18 de octubre de 2018
Funcionalidad agregada	Esta versión admite el uso de filtros adicionales en Event history. Consulte Visualización de CloudTrail eventos en la CloudTrail consola.	18 de octubre de 2018

Funcionalidad agregada	Esta versión es compatible con Amazon Virtual Private Cloud (Amazon VPC) para establecer una conexión privada entre su VPC y AWS CloudTrail. Consulte Uso AWS CloudTrail con puntos finales de VPC de interfaz.	9 de agosto de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Data Lifecycle Manager. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	24 de julio de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon MQ. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	19 de julio de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Mobile CLI. Consulte Servicios e integraciones admitidos con AWS CloudTrail.	29 de junio de 2018
AWS CloudTrail la notificación del historial de documentación está disponible a través de la fuente RSS	Ahora puede recibir notificaciones sobre las actualizaciones de la AWS CloudTrail documentación suscribiéndose a una fuente RSS.	29 de junio de 2018

Actualizaciones anteriores

En la siguiente tabla se describe el historial de publicación de la documentación AWS CloudTrail anterior al 29 de junio de 2018.

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con información sobre rendimiento de Amazon RDS. Para obtener más información, consulte Integraciones y servicios CloudTrail compatibles.	21 de junio de 2018
Funcionalidad agregada	Esta versión permite registrar todos los eventos CloudTrail de administración en el historial de eventos. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.	14 de junio de 2018
Se agregó compatibilidad para los servicios	Esta versión admite AWS Billing and Cost Management. Consulte CloudTrail servicios e integraciones compatibles.	7 de junio de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consulte CloudTrail servicios e integraciones compatibles.	5 de junio de 2018
Documentación actualizada	Esta actualización es compatible con la siguiente versión de parches para la biblioteca CloudTrail de procesamiento: • Actualice las referencias del archivo.jar en la guía del usuario para utilizar la versión más reciente, aws-cloudtrail-processing-library -1.1.2.jar. Para obtener más información, consulte Uso de la biblioteca de procesamiento de CloudTrail y la Biblioteca de procesamiento enCloudTrail . GitHub	16 de mayo de 2018

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión admite AWS Billing and Cost Management. Consulte CloudTrail servicios e integraciones compatibles.	7 de junio de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Elastic Container Service for Kubernetes (Amazon EKS). Consulte CloudTrail servicios e integraciones compatibles.	5 de junio de 2018
Documentación actualizada	Esta actualización es compatible con la siguiente versión de parches para la biblioteca CloudTrail de procesamiento: • Actualice las referencias del archivo.jar en la guía del usuario para utilizar la versión más reciente, aws-cloudtrail-processing-library -1.1.2.jar. Para obtener más información, consulte Uso de la biblioteca de procesamiento de CloudTrail y la Biblioteca de procesamiento enCloudTrail . GitHub	16 de mayo de 2018
Se agregó compatibilidad para los servicios	Esta versión admite AWS X-Ray. Consulte CloudTrail servicios e integraciones compatibles.	25 de abril de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS IoT Analytics. Consulte CloudTrail servicios e integraciones compatibles.	23 de abril de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con Secrets Manager. Consulte CloudTrail servicios e integraciones compatibles.	10 de abril de 2018

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Rekognition. Consulte CloudTrail servicios e integraciones compatibles.	6 de abril de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con la Autoridad de Certificación AWS Privada (PCA). Consulte CloudTrail servicios e integraciones compatibles.	4 de abril de 2018
Funcionalidad agregada	Esta versión permite facilitar la búsqueda de archivos de CloudTrail registro con Amazon Athena. Puede crear automáticamente tablas para consultar registros directamente desde la CloudTrail consola y utilizar esas tablas para ejecutar consultas en Athena. Para obtener más información, consulte Creación CloudTrail servicios e integraciones compatibles de una tabla de CloudTrail registros en la CloudTrail consola.	15 de marzo de 2018
Se agregó compatibilidad para los servicios	Esta versión admite AWS AppSync. Consulte CloudTrail servicios e integraciones compatibles.	13 de febrero de 2018
Se han agregado regiones compatibles	Esta versión es compatible con una región más: Asia-Pacífico (Osaka) (ap-northeast-3). Consulte CloudTrail regiones compatibles.	12 de febrero de 2018
Se agregó compatibilidad para los servicios	Esta versión admite AWS Shield. Consulte CloudTrail servicios e integraciones compatibles.	12 de febrero de 2018
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon SageMaker. Consulte CloudTrail servicios e integraciones compatibles.	11 de enero de 2018

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión admite AWS Batch. Consulte CloudTrail servicios e integraciones compatibles.	10 de enero de 2018
Funcionalidad agregada	Esta versión permite ampliar la cantidad de actividad de la cuenta que está disponible en el historial de CloudTrail eventos a 90 días. También puedes personalizar la visualización de las columnas para mejorar la visualización de tus CloudTrail eventos. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.	12 de diciembre de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon WorkMail. Consulte CloudTrail servicios e integraciones compatibles.	12 de diciembre de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con Alexa for Business AWS Elemental MediaConvert, y AWS Elemental MediaStore. Consulte CloudTrail servicios e integraciones compatibles.	1 de diciembre de 2017
Se agregó funcionalidad y documentación	Esta versión admite el registro de eventos de datos para AWS Lambda funciones. Para obtener más información, consulte Registro de eventos de datos.	30 de noviembre de 2017
Se agregó funcionalidad y documentación	Esta versión admite el registro de eventos de datos para AWS Lambda las funciones. Para obtener más información, consulte Registro de eventos de datos.	30 de noviembre de 2017

Cambio	Descripción	Fecha de lanzamiento
Se agregó funcionalidad y documentación	Esta versión admite las siguientes actualizaciones de la biblioteca CloudTrail de procesamiento: • Agregue compatibilidad con la identificación mediante valores booleanos de eventos de administración. • Actualice la versión del CloudTrail evento a la 1.06. Para obtener más información, consulte Uso de la biblioteca de procesamiento de CloudTrail y la Biblioteca CloudTrail de procesamiento en GitHub.	30 de noviembre de 2017
Se agregó compatibilidad para los servicios	Esta versión admite AWS Glue. Consulte CloudTrail servicios e integraciones compatibles.	7 de noviembre de 2017
Nueva documentación	Esta versión agrega un nuevo tema, Cuotas en AWS CloudTrail.	19 de octubre de 2017
Documentación actualizada	Esta versión actualiza la documentación de las API compatibles en el historial de CloudTrail eventos de Amazon Athena, AWS CodeBuild Amazon Elastic Container Registry y. AWS Migration Hub	13 de octubre de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Chime. Consulte CloudTrail servicios e integraciones compatibles.	27 de septiembre de 2017
Se agregó funcionalidad y documentación	Esta versión admite la configuración del registro de eventos de datos para todos los buckets de Amazon S3 de su AWS cuenta. Consulte Registro de eventos de datos.	20 de septiembre de 2017

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Lex. Consulte CloudTrail servicios e integraciones compatibles.	15 de agosto de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Migration Hub. Consulte CloudTrail servicios e integraciones compatibles.	14 de agosto de 2017
Se agregó funcionalidad y documentación	Esta versión permite CloudTrail habilitarla de forma predeterminada en todas las AWS cuentas. Los últimos siete días de actividad de la cuenta están disponibles en el historial de CloudTrail eventos y los eventos más recientes aparecen en el panel de control de la consola. La característica anteriormente conocida como API activity history (Historial de la actividad de la API) se ha reemplazado por el Event history (Historial de eventos). Para obtener más información, consulte Cómo CloudTrail funciona.	14 de agosto de 2017
Se agregó funcionalidad y documentación	Esta versión permite descargar eventos de la CloudTrail consola en la página del historial de actividades de la API. Puede descargar eventos en formato JSON o CSV. Para obtener más información, consulte Descarga de eventos.	27 de julio de 2017

Cambio	Descripción	Fecha de lanzamiento
Funcionalidad agregada	Esta versión admite el registro de las operaciones de la API en el nivel de objeto de Amazon S3 en dos regiones adicionales, Europa (Londres) y Canadá (centro). Para obtener más información, consulte Trabajar con archivos de registros de CloudTrail.	19 de julio de 2017
Se agregó compatibilidad para los servicios	Esta versión permite buscar las API de Amazon CloudWatch Events en la función de historial de actividad de las CloudTrail API.	27 de junio de 2017
Se agregó funcionalidad y documentación	Esta versión admite API adicionales en la función de historial de actividad de la CloudTrail API para los siguientes servicios: • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	27 de junio de 2017
Se agregó compatibilidad para los servicios	Esta versión admite AWS CodeStar. Consulte CloudTrail servicios e integraciones compatibles.	14 de junio de 2017

Cambio	Descripción	Fecha de lanzamiento

Se agregó funcionalidad y documentación	Esta versión admite las siguientes actualizaciones de la biblioteca CloudTrail de procesamiento:
	• Añada compatibilidad con distintos formatos para los mensajes de SQS de la misma cola de SQS a fin de identificar CloudTrail los archivos de registro. Se admiten los siguientes formatos:
	  • Notificaciones que se CloudTrail envían a un tema de SNS
	  • Notificaciones que Amazon S3 envía a un tema SNS
	  • Notificaciones que Amazon S3 envía directamente a una cola SQS
	• Agrega compatibilidad para la propiedad `deleteMessageUponFailure` , que se puede utilizar para eliminar mensajes que no se pueden procesar.
	
	Para obtener más información, consulte Uso de la biblioteca de procesamiento de CloudTrail y la Biblioteca CloudTrail de procesamiento en GitHub.
		1 de junio de 2017

Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Athena. Consulte CloudTrail servicios e integraciones compatibles.	19 de mayo de 2017

Cambio	Descripción	Fecha de lanzamiento
Funcionalidad agregada	Esta versión admite el envío de eventos de datos a Amazon CloudWatch Logs. Para obtener más información sobre cómo configurar el registro de seguimiento para registrar eventos de datos, consulte Eventos de datos. Para obtener más información sobre el envío de eventos a CloudWatch Logs, consulteMonitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.	9 de mayo de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con el servicio AWS Marketplace de medición. Consulte CloudTrail servicios e integraciones compatibles.	2 de mayo de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon QuickSight. Consulte CloudTrail servicios e integraciones compatibles.	28 de abril de 2017
Se agregó funcionalidad y documentación	Esta versión permite usar la consola actualizada para crear registros de seguimiento nuevos. A partir de ahora puede configurar registros de seguimiento nuevos para registrar eventos de administración y de datos. Para obtener más información, consulte Creación de un registro de seguimiento.	11 de abril de 2017

Cambio	Descripción	Fecha de lanzamiento
Se agrear documentación	Si no CloudTrail envía registros a su bucket de S3 ni envía notificaciones de redes sociales desde algunas regiones de su cuenta, es posible que deba actualizar las políticas. Para obtener más información sobre cómo actualizar la política del bucket de S3, consulte Errores comunes en la configuración de la política de Amazon S3. Para obtener más información sobre cómo actualizar la política de temas de SNS, consulte CloudTrail no envía notificaciones para una región.	31 de marzo de 2017
Se agregó compatibilidad para los servicios	Esta versión admite AWS Organizations. Consulte CloudTrail servicios e integraciones compatibles.	27 de febrero de 2017
Se agregó funcionalidad y documentación	Esta versión permite usar la consola actualizada para configurar registros de seguimiento para registrar eventos de administración y de datos. Para obtener más información, consulte Trabajar con archivos de registros de CloudTrail.	10 de febrero de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Cloud Directory. Consulte CloudTrail servicios e integraciones compatibles.	26 de enero de 2017
Se agregó funcionalidad y documentación	Esta versión permite buscar AWS CodeCommit las API de Amazon GameLift y AWS Managed Services en el historial de actividad de las CloudTrail API.	26 de enero de 2017

Cambio	Descripción	Fecha de lanzamiento
Funcionalidad agregada	Esta versión admite la integración con AWS Health Dashboard. Puedes utilizarla AWS Health Dashboard para identificar si tus rutas no pueden entregar los registros a un tema de SNS o a un bucket de S3. Esto puede ocurrir cuando hay un problema con la política del bucket de S3 o del tema de SNS. AWS Health Dashboard le informa sobre los senderos afectados y le recomienda formas de corregir la política. Para más información, consulte la Guía del usuario de AWS Health.	24 de enero de 2017
Se agregó funcionalidad y documentación	Esta versión admite el filtrado por fuente de eventos en la CloudTrail consola. La fuente de eventos muestra el AWS servicio al que se realizó la solicitud. Para obtener más información, consulte Visualización CloudTrail de eventos de administración recientes en la CloudTrail consola.	12 de enero de 2017
Se agregó compatibilidad para los servicios	Esta versión admite AWS CodeCommit. Consulte CloudTrail servicios e integraciones compatibles.	11 de enero de 2017
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Lightsail . Consulte CloudTrail servicios e integraciones compatibles.	23 de diciembre de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS Managed Services. Consulte CloudTrail servicios e integraciones compatibles.	21 de diciembre de 2016

Cambio	Descripción	Fecha de lanzamiento
Se han agregado regiones compatibles	Esta versión es compatible con la región Europa (Londres). Consulte CloudTrail regiones compatibles.	13 de diciembre de 2016
Se han agregado regiones compatibles	Esta versión es compatible con la región Canadá (Central). Consulte CloudTrail regiones compatibles.	8 de diciembre de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con AWS CodeBuild SeeCloudTrail servicios e integraciones compatibles. Esta versión admite AWS Health. Consulte CloudTrail servicios e integraciones compatibles. Esta versión admite AWS Step Functions. Consulte CloudTrail servicios e integraciones compatibles.	1 de diciembre de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Polly. Consulte CloudTrail servicios e integraciones compatibles.	30 de noviembre de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS OpsWorks for Chef Automate. Consulte CloudTrail servicios e integraciones compatibles.	23 de noviembre de 2016

Cambio	Descripción	Fecha de lanzamiento
Se agregó funcionalidad y documentación	Esta versión permite configurar el registro de seguimiento para registrar eventos de solo lectura, solo escritura o todos los eventos. CloudTrail admite el registro de operaciones de API a nivel de objeto de Amazon S3`GetObject` , como`PutObject` , y`DeleteObject` . Puede configurar los registros de seguimiento para registrar operaciones de API de nivel de objeto. Para obtener más información, consulte Trabajar con archivos de registros de CloudTrail.	21 de noviembre de 2016
Se agregó funcionalidad y documentación	Esta versión admite más valores para el campo `type` en el elemento `userIdentity` : `AWSAccount` y `AWSService` . Para obtener más información, consulte Campos para `userIdentity` .	16 de noviembre de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Application Auto Scaling. Consulte CloudTrail servicios e integraciones compatibles.	31 de octubre de 2016
Se han agregado regiones compatibles	Esta versión es compatible con la región EE. UU. Este (Ohio). Consulte CloudTrail regiones compatibles.	17 de octubre de 2016
Se agregó funcionalidad y documentación	Esta versión admite el registro de eventos de AWS servicio que no son de API. Para obtener más información, consulte Eventos de servicio de AWS.	23 de septiembre de 2016

Cambio	Descripción	Fecha de lanzamiento
Se agregó funcionalidad y documentación	Esta versión admite el uso de la CloudTrail consola para ver los tipos de recursos compatibles AWS Config con. Para obtener más información, consulte Ver los recursos a los que se hace referencia AWS Config.	7 de julio de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS Service Catalog. Consulte CloudTrail servicios e integraciones compatibles.	6 de julio de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Elastic File System (Amazon EFS). Consulte CloudTrail servicios e integraciones compatibles.	28 de junio de 2016
Se han agregado regiones compatibles	Esta versión admite una región más: ap-south-1 (Asia-Pacífico [Bombay]). Consulte CloudTrail regiones compatibles.	27 de junio de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS Application Discovery Service. Consulte CloudTrail servicios e integraciones compatibles.	12 de mayo de 2016
Se agregó compatibilidad para los servicios	Esta versión admite CloudWatch los registros de la región de Sudamérica (São Paulo). Para obtener más información, consulte Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.	6 de mayo de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS WAF. Consulte CloudTrail servicios e integraciones compatibles.	28 de abril de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS Support. Consulte CloudTrail servicios e integraciones compatibles.	21 de abril de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Inspector . Consulte CloudTrail servicios e integraciones compatibles.	20 de abril de 2016

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión admite AWS IoT. Consulte CloudTrail servicios e integraciones compatibles.	11 de abril de 2016
Se agregó funcionalidad y documentación	Esta versión admite las llamadas a la API logging AWS Security Token Service (AWS STS) realizadas con el lenguaje de marcado de aserciones de seguridad (SAML) y la federación de identidades web. Para obtener más información, consulte Valores para AWS STS las API con SAML y federación de identidades web.	28 de marzo de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS Certificate Manager. Consulte CloudTrail servicios e integraciones compatibles.	25 de marzo de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Data Firehose. Consulte CloudTrail servicios e integraciones compatibles.	17 de marzo de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon CloudWatch Logs. Consulte CloudTrail servicios e integraciones compatibles.	10 de marzo de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Cognito. Consulte CloudTrail servicios e integraciones compatibles.	18 de febrero de 2016
Se agregó compatibilidad para los servicios	Esta versión admite AWS Database Migration Service. Consulte CloudTrail servicios e integraciones compatibles.	4 de febrero de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon GameLift (Amazon GameLift). Consulte CloudTrail servicios e integraciones compatibles.	27 de enero de 2016

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon CloudWatch Events. Consulte CloudTrail servicios e integraciones compatibles.	16 de enero de 2016
Se han agregado regiones compatibles	Esta versión es compatible con una región más: ap-northeast-2 (Asia-Pacífico [Seúl]). Consulte CloudTrail regiones compatibles.	6 de enero de 2016
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Elastic Container Registry (Amazon ECR). Consulte CloudTrail servicios e integraciones compatibles.	21 de diciembre de 2015
Se agregó funcionalidad y documentación	Esta versión admite la activación en CloudTrail todas las regiones y admite múltiples rutas por región. Para obtener más información, consulte ¿Cómo se CloudTrail comporta a nivel regional y global?.	17 de diciembre de 2015
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Machine Learning. Consulte CloudTrail servicios e integraciones compatibles.	10 de diciembre de 2015
Se agregó funcionalidad y documentación	Esta versión es compatible con el cifrado de los archivos de registro, la validación de la integridad de los archivos de registro y el etiquetado. Para obtener más información, consulte Cifrado de archivos de CloudTrail registro con AWS KMS claves (SSE-KMS) , Validar la integridad de los archivos de registros de CloudTrail y Actualización de un registro de seguimiento.	1 de octubre de 2015
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon OpenSearch Service. Consulte CloudTrail servicios e integraciones compatibles.	1 de octubre de 2015

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión admite eventos en nivel de bucket de Amazon S3. Consulte CloudTrail servicios e integraciones compatibles.	1 de septiembre de 2015
Se agregó compatibilidad para los servicios	Esta versión admite AWS Device Farm. Consulte CloudTrail servicios e integraciones compatibles.	13 de julio de 2015
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon API Gateway. Consulte CloudTrail servicios e integraciones compatibles.	9 de julio de 2015
Se agregó compatibilidad para los servicios	Esta versión admite CodePipeline. Consulte CloudTrail servicios e integraciones compatibles.	9 de julio de 2015
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon DynamoDB. Consulte CloudTrail servicios e integraciones compatibles.	28 de mayo de 2015
Se agregó compatibilidad para los servicios	Esta versión admite CloudWatch los registros de la región EE.UU. Oeste (Norte de California). Consulte las Notas de la versión de CloudTrail . Para obtener más información sobre la CloudTrail compatibilidad con la supervisión de CloudWatch los registros , consulteMonitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs.	19 de mayo de 2015
Se agregó compatibilidad para los servicios	Esta versión admite AWS Directory Service. Consulte CloudTrail servicios e integraciones compatibles.	14 de mayo de 2015
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Simple Email Service (Amazon SES). Consulte CloudTrail servicios e integraciones compatibles.	7 de mayo de 2015

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Elastic Container Service. ConsulteCloudTrail servicios e integraciones compatibles.	9 de abril de 2015
Se agregó compatibilidad para los servicios	Esta versión admite AWS Lambda. Consulte CloudTrail servicios e integraciones compatibles.	9 de abril de 2015
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon WorkSpaces. Consulte CloudTrail servicios e integraciones compatibles.	9 de abril de 2015
	Esta versión admite la búsqueda de la AWS actividad capturada por CloudTrail (CloudTrail eventos). Puede buscar y filtrar eventos en su cuenta relacionados con actividades de creación, modificación o eliminación. Para buscar estos eventos, puedes usar la CloudTrail consola, el AWS Command Line Interface (AWS CLI) o el AWS SDK. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.	12 de marzo de 2015
Se agregó compatibilidad con servicios y documentación nueva	Esta versión es compatible con Amazon CloudWatch Logs en las regiones de Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio) y Europa (Fráncfort). Para obtener más información, consulte Envío de eventos a CloudWatch Logs.	5 de marzo de 2015
Nueva documentación	Se ha agregado a la página de CloudTrail conceptos una nueva sección que describe la CloudTrail compatibilidad con AWS Security Token Service (AWS STS) puntos finales regionales.	17 de febrero de 2015

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Route 53. Consulte CloudTrail servicios e integraciones compatibles.	11 de febrero de 2015
Se agregó compatibilidad para los servicios	Esta versión admite AWS Config. Consulte CloudTrail servicios e integraciones compatibles.	10 de febrero de 2015
Se agregó compatibilidad para los servicios	Esta versión admite AWS CloudHSM. Consulte CloudTrail servicios e integraciones compatibles.	8 de enero de 2015
Se agregó compatibilidad para los servicios	Esta versión admite AWS CodeDeploy. Consulte CloudTrail servicios e integraciones compatibles.	17 de diciembre de 2014
Se agregó compatibilidad para los servicios	Esta versión admite AWS Storage Gateway. Consulte CloudTrail servicios e integraciones compatibles.	16 de diciembre de 2014
Se han agregado regiones compatibles	Esta versión admite una región adicional: us-gov-west -1 (AWS GovCloud (US-West)). Consulte CloudTrail regiones compatibles.	16 de diciembre de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon S3 Glacier. Consulte CloudTrail servicios e integraciones compatibles.	11 de diciembre de 2014
Se agregó compatibilidad para los servicios	Esta versión admite AWS Data Pipeline. Consulte CloudTrail servicios e integraciones compatibles.	2 de diciembre de 2014
Se agregó compatibilidad para los servicios	Esta versión admite AWS Key Management Service. Consulte CloudTrail servicios e integraciones compatibles.	12 de noviembre de 2014

Cambio	Descripción	Fecha de lanzamiento
Nueva documentación	Se agregó la sección nueva, Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs, a la guía. Describe cómo utilizar Amazon CloudWatch Logs para supervisar los eventos de CloudTrail registro.	10 de noviembre de 2014
Nueva documentación	Se agregó la sección nueva, Uso de la biblioteca de procesamiento de CloudTrail, a la guía. Proporciona información sobre cómo escribir un procesador de CloudTrail registros en Java mediante la biblioteca AWS CloudTrail de procesamiento.	5 de noviembre de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Elastic Transcoder. Consulte CloudTrail servicios e integraciones compatibles.	27 de octubre de 2014
Se han agregado regiones compatibles	Esta versión es compatible con una región más: eu-central-1 (Europa [Fránkfort]). Consulte CloudTrail regiones compatibles.	23 de octubre de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon CloudSearch. Consulte CloudTrail servicios e integraciones compatibles.	16 de octubre de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Simple Notification Service. Consulte CloudTrail servicios e integraciones compatibles.	09 de octubre de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon ElastiCache. Consulte CloudTrail servicios e integraciones compatibles.	15 de septiembre de 2014

Cambio	Descripción	Fecha de lanzamiento
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon WorkDocs. Consulte CloudTrail servicios e integraciones compatibles.	27 de agosto de 2014
Se agregó contenido nuevo	Esta versión incluye un tema que trata sobre el registro de eventos de inicio de sesión. Consulte AWS Management Console eventos de inicio de sesión.	24 de julio de 2014
Se agregó contenido nuevo	El elemento eventVersion de esta versión se ha actualizado a la versión 1.02 y se han agregado tres nuevos campos. Consulte CloudTrail contenido del registro.	18 de julio de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Auto Scaling (consulte CloudTrail servicios e integraciones compatibles).	17 de julio de 2014
Se han agregado regiones compatibles	Esta versión es compatible con tres regiones más: ap-southeast-1 (Asia-Pacífico [Singapur]), ap-northeast-1 (Asia-Pacífico [Tokio]) y sa-east-1 (América del Sur [São Paulo]). Consulte CloudTrail regiones compatibles.	30 de junio de 2014
Compatibilidad adicional con servicio	Esta versión es compatible con Amazon Redshift. Consulte CloudTrail servicios e integraciones compatibles.	10 de junio de 2014
Se agregó compatibilidad para los servicios	Esta versión admite AWS OpsWorks. Consulte CloudTrail servicios e integraciones compatibles.	5 de junio de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon CloudFront. Consulte CloudTrail servicios e integraciones compatibles.	28 de mayo de 2014

Cambio	Descripción	Fecha de lanzamiento
Se han agregado regiones compatibles	Esta versión es compatible con tres regiones más: us-west-1 (Oeste de EE. UU. [Norte de California]), eu-west-1 (Europa [Irlanda]), ap-southeast-2 (Asia-Pacífico [Sídney]). Consulte CloudTrail regiones compatibles.	13 de mayo de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Simple Workflow Service. Consulte CloudTrail servicios e integraciones compatibles.	9 de mayo de 2014
Se agregó contenido nuevo	Esta versión incluye temas sobre el uso compartido de archivos de registro entre cuentas. Consulte Compartir archivos de registro de CloudTrail entre cuentas de AWS.	2 de mayo de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon CloudWatch. Consulte CloudTrail servicios e integraciones compatibles.	28 de abril de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon Kinesis. Consulte CloudTrail servicios e integraciones compatibles.	22 de abril de 2014
Se agregó compatibilidad para los servicios	Esta versión admite AWS Direct Connect. Consulte CloudTrail servicios e integraciones compatibles.	11 de abril de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Amazon EMR. Consulte CloudTrail servicios e integraciones compatibles.	4 de abril de 2014
Se agregó compatibilidad para los servicios	Esta versión es compatible con Elastic Beanstalk. Consulte CloudTrail servicios e integraciones compatibles.	2 de abril de 2014

Cambio	Descripción	Fecha de lanzamiento
Compatibilidad adicional con servicio	Esta versión admite AWS CloudFormation. Consulte CloudTrail servicios e integraciones compatibles.	7 de marzo de 2014
Nueva guía	Esta versión introduce AWS CloudTrail.	13 de noviembre de 2013

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.