



Guía del usuario

# AWS CloudTrail



Version 1.0

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

# AWS CloudTrail: Guía del usuario

Copyright © 2025 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  |
| Acceso a CloudTrail .....                                           | 2  |
| Consola de CloudTrail .....                                         | 3  |
| AWS CLI .....                                                       | 4  |
| API de CloudTrail .....                                             | 4  |
| AWS SDK .....                                                       | 4  |
| Funcionamiento de CloudTrail .....                                  | 4  |
| Historial de eventos de CloudTrail .....                            | 5  |
| CloudTrail Lake y los almacenes de datos de eventos .....           | 5  |
| Paneles de CloudTrail Lake .....                                    | 9  |
| Registros de seguimiento de CloudTrail .....                        | 10 |
| Eventos de CloudTrail Insights .....                                | 16 |
| Canales de CloudTrail .....                                         | 18 |
| Conceptos .....                                                     | 18 |
| Eventos de CloudTrail .....                                         | 19 |
| Historial de eventos .....                                          | 53 |
| Registros de seguimiento .....                                      | 53 |
| Registros de seguimiento de la organización .....                   | 56 |
| CloudTrail Lake y los almacenes de datos de eventos .....           | 58 |
| CloudTrail Insights .....                                           | 58 |
| Etiquetas .....                                                     | 59 |
| AWS Security Token Service y CloudTrail .....                       | 59 |
| Eventos de servicios globales .....                                 | 59 |
| Regiones admitidas .....                                            | 61 |
| Servicios e integraciones compatibles .....                         | 66 |
| Integraciones de servicios de AWS con registros de CloudTrail ..... | 66 |
| Integración de CloudTrail con Amazon EventBridge .....              | 69 |
| Integración de CloudTrail con AWS Organizations .....               | 70 |
| Integración de CloudTrail con AWS Control Tower .....               | 70 |
| Integración de CloudTrail con Amazon Security Lake .....            | 71 |
| Integración de CloudTrail Lake con Amazon Athena .....              | 71 |
| Integración de CloudTrail Lake con AWS Config .....                 | 71 |
| Integración de CloudTrail Lake con AWS Audit Manager .....          | 71 |
| AWSTemas de servicio de para CloudTrail .....                       | 72 |

|                                                                                                                                    |     |
|------------------------------------------------------------------------------------------------------------------------------------|-----|
| Servicios no admitidos .....                                                                                                       | 100 |
| Cuotas en AWS CloudTrail .....                                                                                                     | 100 |
| Cuotas de recursos de CloudTrail .....                                                                                             | 101 |
| Cuotas de transacciones por segundo (TPS) en CloudTrail .....                                                                      | 108 |
| Tutoriales de CloudTrail .....                                                                                                     | 109 |
| Concesión de permisos para utilizar CloudTrail .....                                                                               | 109 |
| Visualización del historial de eventos .....                                                                                       | 111 |
| Creación de un registro de seguimiento para registrar los eventos de administración .....                                          | 113 |
| Ver los archivos de registros .....                                                                                                | 117 |
| Creación de un almacén de datos de eventos para eventos de datos de S3 .....                                                       | 119 |
| Visualización del costo y el uso de CloudTrail .....                                                                               | 127 |
| Se utiliza AWS Budgets para administrar los costos .....                                                                           | 133 |
| Creación de etiquetas de asignación de costos definidas por el usuario para almacenes de datos de eventos de CloudTrail Lake ..... | 133 |
| Administración de los costos de los registros de seguimiento de CloudTrail .....                                                   | 134 |
| Configuración de registros de seguimiento .....                                                                                    | 134 |
| Véase también .....                                                                                                                | 136 |
| Administración de los costos de CloudTrail Lake .....                                                                              | 136 |
| Opciones de precios del almacén de datos de eventos .....                                                                          | 136 |
| Comprensión de los cargos de CloudTrail Lake .....                                                                                 | 138 |
| Recomendaciones sobre cómo reducir los costos .....                                                                                | 140 |
| Véase también .....                                                                                                                | 142 |
| Trabajar con el historial de eventos de CloudTrail .....                                                                           | 143 |
| Limitaciones del Historial de eventos .....                                                                                        | 144 |
| Visualización de eventos de administración recientes con la consola .....                                                          | 145 |
| Navegación entre páginas .....                                                                                                     | 146 |
| Personalización de la pantalla .....                                                                                               | 147 |
| Filtro de eventos de CloudTrail .....                                                                                              | 148 |
| Ver los detalles de un evento .....                                                                                                | 150 |
| Descarga de eventos .....                                                                                                          | 150 |
| Ver los recursos a los que se hace referencia con AWS Config .....                                                                 | 152 |
| Visualización de eventos de administración recientes con la AWS CLI .....                                                          | 153 |
| Requisitos previos .....                                                                                                           | 154 |
| Obtener ayuda de la línea de comandos .....                                                                                        | 155 |
| Buscar eventos .....                                                                                                               | 155 |
| Especificar el número de eventos que se devuelven .....                                                                            | 156 |



|                                                                                                   |     |
|---------------------------------------------------------------------------------------------------|-----|
| Buscar eventos por intervalo de tiempo .....                                                      | 157 |
| Buscar eventos por atributo .....                                                                 | 157 |
| Especificar la siguiente página de resultados .....                                               | 159 |
| Obtener datos de entrada JSON de un archivo .....                                                 | 159 |
| Campos de resultados de búsqueda .....                                                            | 161 |
| Trabajar con CloudTrail Insights .....                                                            | 163 |
| Costos de los eventos de Insights .....                                                           | 164 |
| Entrega de eventos de Insights .....                                                              | 167 |
| Registro de eventos de Insights con la consola de CloudTrail .....                                | 168 |
| Habilitación de CloudTrail Insights en un registro de seguimiento existente con la consola ..     | 168 |
| Habilitación CloudTrail Insights en un almacén de datos de eventos existente con la consola ..... | 169 |
| Registro de eventos de Insights con la AWS CLI .....                                              | 170 |
| Registro de eventos de Insights para un registro de seguimiento mediante la AWS CLI .....         | 170 |
| Registro de eventos de Insights para un almacén de datos de eventos mediante la AWS CLI .....     | 172 |
| Visualización de eventos de Insights para registros de seguimiento .....                          | 176 |
| Cómo visualizar eventos de Insights para registros de seguimiento con la consola .....            | 177 |
| Cómo visualizar eventos de Insights para registros de seguimiento con la AWS CLI .....            | 186 |
| Visualización de eventos de Insights para los almacenes de datos de eventos .....                 | 196 |
| Visualización del panel de Insights de un almacén de datos de eventos .....                       | 197 |
| Visualización de consultas de muestra para los eventos de Insights .....                          | 198 |
| Trabajar con CloudTrail Lake .....                                                                | 200 |
| Almacenes de datos de eventos de CloudTrail Lake .....                                            | 200 |
| Consultas de CloudTrail Lake .....                                                                | 202 |
| Paneles de CloudTrail Lake .....                                                                  | 202 |
| Integraciones de CloudTrail Lake .....                                                            | 203 |
| Recursos adicionales .....                                                                        | 204 |
| Regiones en las que se admite CloudTrail Lake .....                                               | 204 |
| Conceptos y terminología de CloudTrail Lake .....                                                 | 206 |
| Almacenes de datos de eventos .....                                                               | 206 |
| Integraciones .....                                                                               | 208 |
| Consultas .....                                                                                   | 210 |
| Paneles .....                                                                                     | 210 |
| Almacenes de datos de eventos .....                                                               | 211 |

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| Creación, actualización y administración de almacenes de datos de eventos con la consola .....        | 213 |
| Creación, actualización y administración de almacenes de datos de eventos con la AWS CLI .....        | 273 |
| Administración de los ciclos de vida de los almacenes de datos de eventos .....                       | 306 |
| Copiar eventos de registro de seguimiento en un almacén de datos de eventos .....                     | 307 |
| Federar un almacén de datos de eventos .....                                                          | 331 |
| Almacenes de datos de eventos de la organización .....                                                | 343 |
| Integraciones .....                                                                                   | 350 |
| Creación de una integración con un socio de CloudTrail con la consola .....                           | 351 |
| Creación de una integración personalizada con la consola .....                                        | 354 |
| Creación, actualización y administración de las integraciones de CloudTrail Lake con la AWS CLI ..... | 358 |
| Información adicional acerca de los socios de integración .....                                       | 368 |
| Esquema de eventos de integraciones de CloudTrail Lake .....                                          | 369 |
| Paneles .....                                                                                         | 378 |
| Requisitos previos .....                                                                              | 380 |
| Limitaciones .....                                                                                    | 380 |
| Compatibilidad de regiones .....                                                                      | 380 |
| Permisos necesarios .....                                                                             | 381 |
| Consulta de un panel administrado .....                                                               | 385 |
| Habilitación del panel de aspectos destacados .....                                                   | 403 |
| Desactivación del panel de aspectos destacados .....                                                  | 405 |
| Creación de un panel personalizado .....                                                              | 405 |
| Establecer un programa de actualización para un panel personalizado .....                             | 409 |
| Deshabilitar un programa de actualización para un panel personalizado .....                           | 410 |
| Cambiar la protección contra la terminación .....                                                     | 410 |
| Eliminar un panel personalizado .....                                                                 | 411 |
| Crear, actualizar y administrar los paneles con la AWS CLI .....                                      | 412 |
| Consultas .....                                                                                       | 202 |
| Herramientas del editor de consultas .....                                                            | 430 |
| Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural .....             | 431 |
| Visualización de consultas de ejemplo .....                                                           | 438 |
| Creación o edición de una consulta .....                                                              | 442 |
| Ejecutar una consulta y guardar los resultados de la consulta .....                                   | 444 |
| Visualización de los resultados de la consulta .....                                                  | 449 |

|                                                                                                               |     |
|---------------------------------------------------------------------------------------------------------------|-----|
| Resumen de los resultados de las consultas en lenguaje natural .....                                          | 451 |
| Descarga de los resultados de consultas guardados .....                                                       | 453 |
| Validación de los resultados de consultas guardados .....                                                     | 455 |
| Optimización de consultas .....                                                                               | 470 |
| Ejecución y administración de consultas de CloudTrail Lake con la AWS CLI .....                               | 474 |
| Restricciones SQL de CloudTrail Lake .....                                                                    | 480 |
| Funciones, condiciones y operadores join compatibles .....                                                    | 481 |
| Soporte avanzado de consultas en varias tablas .....                                                          | 482 |
| Esquemas SQL compatibles con los almacenes de datos de eventos .....                                          | 483 |
| Esquema compatible para los campos de registro de eventos de CloudTrail .....                                 | 484 |
| Esquema compatible para los campos de registro de eventos de CloudTrail Insights .....                        | 487 |
| Esquema compatible para los campos de registro de elementos de configuración de AWS Config .....              | 489 |
| Esquema compatible para los campos de registro de evidencia de AWS Audit Manager .....                        | 491 |
| Esquema compatible para campos de eventos que no son de AWS .....                                             | 492 |
| Métricas de CloudWatch admitidas .....                                                                        | 493 |
| Trabajar con registros de seguimiento de CloudTrail .....                                                     | 497 |
| Creación de un registro de seguimiento para su Cuenta de AWS .....                                            | 498 |
| Creación y actualización de un registro de seguimiento con la consola .....                                   | 500 |
| Creación, actualización y administración de registros de seguimiento con la AWS CLI .....                     | 535 |
| Creación de varios registros de seguimiento .....                                                             | 569 |
| Creación de un registro de seguimiento para una organización .....                                            | 572 |
| Cambio de registros de seguimiento de cuentas de miembros a registros de seguimiento de la organización ..... | 577 |
| Prepararse a fin de crear un registro de seguimiento para la organización .....                               | 577 |
| Creación de un registro de seguimiento para la organización en la consola .....                               | 581 |
| Creación de un registro de seguimiento para una organización con la AWS CLI .....                             | 593 |
| Solución de problemas .....                                                                                   | 601 |
| Cómo entender los registros de seguimiento de varias regiones y las regiones optativas .....                  | 604 |
| ¿Cuáles son las ventajas de los registro de seguimiento de varias regiones? .....                             | 604 |
| ¿Qué ocurre cuando se crea un registro de seguimiento de varias regiones? .....                               | 605 |
| ¿Qué sucede cuando se habilita una región optativa? .....                                                     | 605 |
| ¿Qué sucede cuando se deshabilita una región optativa? .....                                                  | 606 |
| Copia de eventos de registro de seguimiento en CloudTrail Lake .....                                          | 606 |
| Consideraciones para copiar eventos de registros de seguimiento .....                                         | 608 |
| Permisos necesarios para copiar eventos de registro de seguimiento .....                                      | 610 |

|                                                                                                                          |     |
|--------------------------------------------------------------------------------------------------------------------------|-----|
| Copiar eventos de registros de seguimiento a un almacén de datos de eventos existente con la consola de CloudTrail ..... | 614 |
| Obtención y visualización de archivos de registros de CloudTrail .....                                                   | 617 |
| Búsqueda de los archivos de registros de CloudTrail .....                                                                | 618 |
| Descarga de los archivos de registros de CloudTrail .....                                                                | 620 |
| Configuración de notificaciones de Amazon SNS para CloudTrail .....                                                      | 621 |
| Configuración de CloudTrail para el envío de notificaciones .....                                                        | 622 |
| Uso de AWS CloudTrail con los puntos de enlace de la VPC de la interfaz .....                                            | 624 |
| Regiones .....                                                                                                           | 625 |
| Crear un punto de enlace de la VPC para CloudTrail .....                                                                 | 625 |
| Crear una política de punto de conexión de VPC para CloudTrail .....                                                     | 625 |
| Subredes compartidas .....                                                                                               | 629 |
| Requisitos de nomenclatura .....                                                                                         | 630 |
| Requisitos de nomenclatura para recursos de CloudTrail .....                                                             | 630 |
| Requisitos de nomenclatura para buckets de Amazon S3 .....                                                               | 630 |
| AWS KMSRequisitos de nomenclatura para el alias de .....                                                                 | 631 |
| Cierre de Cuenta de AWS y registros de seguimiento .....                                                                 | 632 |
| Configuración de los ajustes de CloudTrail .....                                                                         | 634 |
| Administrador delegado de la organización .....                                                                          | 634 |
| Permisos necesarios para designar un administrador delegado .....                                                        | 639 |
| Cómo agregar un administrador delegado de CloudTrail .....                                                               | 640 |
| Cómo eliminar un administrador delegado de CloudTrail .....                                                              | 641 |
| Canales vinculados a servicios .....                                                                                     | 642 |
| Visualización de canales vinculados a servicios con la consola .....                                                     | 642 |
| Visualización de canales vinculados a servicios con la AWS CLI .....                                                     | 643 |
| Descripción de los eventos de CloudTrail .....                                                                           | 647 |
| Eventos de administración .....                                                                                          | 648 |
| Eventos de datos .....                                                                                                   | 651 |
| Eventos de datos compatibles con AWS CloudTrail .....                                                                    | 652 |
| Eventos de actividad de la red .....                                                                                     | 682 |
| Eventos de Insights .....                                                                                                | 687 |
| Eventos de administración .....                                                                                          | 690 |
| Eventos de administración .....                                                                                          | 691 |
| Eventos de lectura y escritura .....                                                                                     | 692 |
| Registro de eventos de administración con la Consola de administración de AWS .....                                      | 693 |
| Registro de eventos de administración con la AWS CLI .....                                                               | 698 |

|                                                                                                            |     |
|------------------------------------------------------------------------------------------------------------|-----|
| Registro de eventos de administración con los SDK de AWS .....                                             | 713 |
| Eventos de datos .....                                                                                     | 713 |
| Eventos de datos .....                                                                                     | 715 |
| Eventos de solo lectura y de solo escritura .....                                                          | 748 |
| Registrar eventos de datos con la Consola de administración de AWS .....                                   | 749 |
| Registrar eventos de datos con la AWS Command Line Interface .....                                         | 760 |
| Filtrado de los eventos de datos mediante selectores de eventos avanzados .....                            | 773 |
| Registrar eventos de datos para la conformidad con AWS Config .....                                        | 786 |
| Registro de eventos de datos con los SDK de AWS .....                                                      | 787 |
| Eventos de actividad de la red .....                                                                       | 787 |
| Campos de los selectores de eventos avanzados para eventos de actividad de la red .....                    | 791 |
| Registro de eventos de actividad de la red con la Consola de administración de AWS .....                   | 794 |
| Registro de eventos de actividad de la red con la AWS Command Line Interface .....                         | 798 |
| Registro de eventos con los SDK de AWS .....                                                               | 820 |
| Agregar claves de etiqueta de recurso y claves de condición global de IAM al evento .....                  | 821 |
| Etiquetas de recursos compatibles de Servicios de AWS .....                                                | 823 |
| Servicios de AWS compatibles con las claves de condición global de IAM .....                               | 824 |
| Ejemplos de evento .....                                                                                   | 827 |
| CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red ..... | 829 |
| Orden de truncamiento de campos para un tamaño máximo de evento de 1 MB .....                              | 843 |
| Ejemplo de sharedEventID .....                                                                             | 844 |
| CloudTrail registra el contenido de los eventos de Insights para registros de seguimiento .....            | 845 |
| Ejemplo de bloque insightDetails .....                                                                     | 851 |
| CloudTrail registra el contenido de los eventos de Insights para los almacenes de datos de eventos .....   | 853 |
| Elemento userIdentity de CloudTrail. ....                                                                  | 858 |
| Ejemplos .....                                                                                             | 858 |
| Campos .....                                                                                               | 860 |
| Valores de las API de AWS STS con SAML e identidad federada web .....                                      | 868 |
| AWS STSIdentidad fuente de .....                                                                           | 870 |
| Eventos no generados por la API capturados por CloudTrail .....                                            | 873 |
| Servicio de AWSEventos de .....                                                                            | 873 |
| Consola de administración de AWSEventos de inicio de sesión en la .....                                    | 874 |
| Archivos de registro de CloudTrail .....                                                                   | 891 |
| Recepción de archivos de registro de CloudTrail de varias regiones .....                                   | 893 |

|                                                                                                                                |     |
|--------------------------------------------------------------------------------------------------------------------------------|-----|
| Administración de la consistencia de los datos .....                                                                           | 894 |
| Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs .....                                              | 895 |
| Envío de eventos a Amazon CloudWatch Logs .....                                                                                | 896 |
| Creación de alarmas de CloudWatch para eventos de CloudTrail: ejemplos .....                                                   | 905 |
| Impedir que CloudTrail envíe eventos a CloudWatch Logs .....                                                                   | 913 |
| Grupo de registros de CloudWatch y nomenclatura de secuencias de registros para CloudTrail .....                               | 914 |
| Documento de política de roles para que CloudTrail utilice CloudWatch Logs para el monitoreo. ....                             | 915 |
| Recepción de archivos de registros de CloudTrail desde varias cuentas .....                                                    | 917 |
| Eliminación de los ID de las cuentas de los propietarios de los buckets para eventos de datos llamados por otras cuentas ..... | 918 |
| Configuración de la política de bucket para varias cuentas .....                                                               | 920 |
| Crea registros de seguimiento en cuentas adicionales .....                                                                     | 922 |
| Compartir archivos de registro de CloudTrail entre cuentas de AWS .....                                                        | 924 |
| Comparta archivos de registros entre cuentas asumiendo un rol .....                                                            | 925 |
| Validar la integridad de los archivos de registros de CloudTrail .....                                                         | 935 |
| ¿Por qué utilizarla? .....                                                                                                     | 935 |
| Funcionamiento .....                                                                                                           | 936 |
| Habilitación de la validación de la integridad de los archivos de registros de CloudTrail .....                                | 937 |
| Validación de la integridad de los archivos de registros de CloudTrail con la AWS CLI .....                                    | 938 |
| Estructura de los archivos de resumen de CloudTrail .....                                                                      | 947 |
| Implementaciones personalizadas para validar la integridad de los archivos de registros de CloudTrail .....                    | 955 |
| Ejemplos de archivos de registros de CloudTrail .....                                                                          | 967 |
| Formato de nombre de archivo de registros de CloudTrail .....                                                                  | 968 |
| Ejemplos de archivos de registros .....                                                                                        | 968 |
| Uso de la biblioteca de procesamiento de CloudTrail .....                                                                      | 981 |
| Requisitos mínimos .....                                                                                                       | 982 |
| Procesamiento de registros de CloudTrail .....                                                                                 | 982 |
| Temas avanzados .....                                                                                                          | 988 |
| Recursos adicionales .....                                                                                                     | 994 |
| Seguridad .....                                                                                                                | 995 |
| Protección de los datos .....                                                                                                  | 996 |
| Identity and Access Management .....                                                                                           | 997 |
| Público .....                                                                                                                  | 998 |

|                                                                                                                                                              |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Autenticación con identidades .....                                                                                                                          | 998  |
| Administración de acceso mediante políticas .....                                                                                                            | 1000 |
| Cómo AWS CloudTrail funciona con IAM .....                                                                                                                   | 1001 |
| Ejemplos de políticas basadas en identidades .....                                                                                                           | 1009 |
| Ejemplos de políticas basadas en recursos .....                                                                                                              | 1027 |
| Política de bucket de Amazon S3 para CloudTrail .....                                                                                                        | 1035 |
| Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake .....                                                                        | 1044 |
| Política de temas de Amazon SNS para CloudTrail .....                                                                                                        | 1047 |
| Solución de problemas .....                                                                                                                                  | 1055 |
| Cómo utilizar roles vinculados a servicios .....                                                                                                             | 1059 |
| AWSPolíticas de administradas por .....                                                                                                                      | 1066 |
| Validación de conformidad .....                                                                                                                              | 1069 |
| Resiliencia .....                                                                                                                                            | 1070 |
| Seguridad de la infraestructura .....                                                                                                                        | 1071 |
| Prevención de la sustitución confusa entre servicios .....                                                                                                   | 1071 |
| Prácticas recomendadas de seguridad .....                                                                                                                    | 1072 |
| Prácticas recomendadas de seguridad de CloudTrail Detective .....                                                                                            | 1073 |
| Prácticas recomendadas preventivas de seguridad de CloudTrail .....                                                                                          | 1075 |
| Cifrado de archivos de registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS (SSE-KMS) .....                | 1079 |
| Activación del cifrado de los archivos de registro .....                                                                                                     | 1081 |
| Conceder permisos para crear una clave de KMS .....                                                                                                          | 1082 |
| Configurar políticas de clave de AWS KMS para CloudTrail .....                                                                                               | 1083 |
| Actualización de un recurso para que utilice su clave de KMS con la consola .....                                                                            | 1099 |
| Habilitar y deshabilitar el cifrado de los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail con AWS CLI ..... | 1103 |
| Cómo AWS CloudTrail usa AWS KMS .....                                                                                                                        | 1107 |
| Historial de documentos .....                                                                                                                                | 1113 |
| Actualizaciones anteriores .....                                                                                                                             | 1189 |

# ¿Qué es AWS CloudTrail?

AWS CloudTrail es un Servicio de AWS que ayuda a habilitar la auditoría operativa y de riesgos, la gobernanza y la conformidad 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 Consola de administración de AWS, AWS Command Line Interface y las API y los SDK de AWS.

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 eventos de CloudTrail](#).

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 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 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 obtener más información, consulte [Trabajar con AWS CloudTrail Lake](#).

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 [Administración de los costos de CloudTrail Lake](#).

- 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 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 las tasas de llamada a la 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 a su bucket de 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.

## Acceso a CloudTrail

Puede trabajar con CloudTrail de cualquiera de las siguientes formas.

### Temas

- [Consola de CloudTrail](#)
- [AWS CLI](#)

- [API de CloudTrail](#)
- [AWS SDK](#)

## Consola de CloudTrail

Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.

La consola de CloudTrail ofrece una interfaz de usuario para realizar muchas tareas de CloudTrail como:

- Visualizar los últimos eventos y el historial de eventos para la cuenta de AWS.
- Descarga de un archivo filtrado o completo de los últimos 90 días de eventos administración desde el Historial de eventos.
- Creación y edición de registros de seguimiento de CloudTrail
- Creación y edición de almacenes de datos de eventos de CloudTrail Lake
- Ejecución de consultas en almacenes de datos de eventos
- Configuración de los registros de seguimiento de CloudTrail, incluido:
  - Selección de un bucket de Amazon S3 para registros de seguimiento
  - Establecer un prefijo.
  - Configuración de la entrega en CloudWatch Logs.
  - Uso de claves de AWS KMS para el cifrado de los datos de registro de seguimiento
  - 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 incluye:
  - Integrar los almacenes de datos de eventos con socios de CloudTrail o con sus propias aplicaciones para registrar eventos de orígenes externos a AWS.
  - Federación de los almacenes de datos de eventos para ejecutar consultas desde Amazon Athena.
  - Usar claves de AWS KMS para el cifrado de los datos del almacén de datos de eventos.
  - Agregar y administrar etiquetas para sus almacenes de datos de eventos.

Para obtener más información sobre Consola de administración de AWS, consulte [Consola de administración de AWS](#).

## AWS CLI

La AWS Command Line Interface es una herramienta unificada que puede utilizar para interactuar con CloudTrail desde la línea de comandos. Para obtener más información, consulte la [Guía del usuario de AWS Command Line Interface](#). Para obtener una lista completa de los comandos de la CLI de CloudTrail, consulte [cloudtrail](#) y [cloudtrail-data](#) en la Referencia de comandos de la AWS CLI.

## API de CloudTrail

Además de la consola y la CLI, también puede utilizar las API RESTful de CloudTrail para programar CloudTrail directamente. Para obtener más información, consulte la [Referencia de la API de AWS CloudTrail](#) y la [Referencia de la API CloudTrail-Data](#).

## AWS SDK

Además de la API de CloudTrail, puede utilizar uno de los SDK de AWS. Cada SDK se compone de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas. Los SDK proporcionan una forma conveniente de crear acceso programático a CloudTrail. Por ejemplo, puede usar los SDK para firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. Para obtener más información, consulte la página [Herramientas para crear en AWS](#).

## Funcionamiento de CloudTrail

Al crear su Cuenta de AWS, tendrá acceso automáticamente al Historial de eventos de CloudTrail. 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.

Para mantener un registro continuo de los eventos en su Cuenta de AWS más allá de los 90 días, cree un registro de seguimiento o un almacén de datos de eventos de CloudTrail Lake.

### Temas

- [Historial de eventos de CloudTrail](#)
- [CloudTrail Lake y los almacenes de datos de eventos](#)
- [Paneles de CloudTrail Lake](#)

- [Registros de seguimiento de CloudTrail](#)
- [Eventos de CloudTrail Insights](#)
- [Canales de CloudTrail](#)

## Historial de eventos de CloudTrail

Vaya a la página Historial de eventos para ver los eventos de administración de los últimos 90 días de forma sencilla en la consola de CloudTrail. 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 eventos de CloudTrail](#).

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.

No se cobran cargos de CloudTrail por ver la página Historial de eventos ni por ejecutar el comando `lookup-events`.

## CloudTrail Lake y los almacenes de datos de eventos

Puede crear un almacén de datos de eventos para registrar los [eventos de CloudTrail](#) (eventos de administración, de datos y de actividad de la red), los [eventos de CloudTrail Insights](#), las [pruebas de AWS Audit Manager](#), los [elementos de configuración de AWS Config](#) o los [eventos ajenos a AWS](#).

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.

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. 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 [Descripción de los almacenes de datos de eventos de la organización](#).

De forma predeterminada, CloudTrail cifra todos los eventos que se encuentran en un almacén de datos de eventos. Cuando configure un almacén de datos de eventos, puede optar por utilizar su propia AWS KMS key. Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. Después de asociar un almacén de datos de eventos a una clave de KMS, esta no se podrá eliminar ni cambiar. Para obtener más información, consulte [Cifrado de archivos de registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS \(SSE-KMS\)](#).

En la siguiente tabla se proporciona información sobre las tareas que puede realizar en los almacenes de datos de eventos.

| Tarea                                                 | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Ver y crear paneles</a>                   | Puede usar los paneles de CloudTrail Lake para consultar las tendencias de eventos de los almacenes de datos de eventos de la cuenta. Puede ver los paneles administrados, crear paneles personalizados y habilitar el panel de aspectos destacados para ver los aspectos destacados de los datos de sus eventos que CloudTrail Lake selecciona y administra.                                                                                                                                                                                   |
| <a href="#">Registro de eventos de administración</a> | <p>Configure su almacén de datos de eventos para que registre eventos de solo lectura, de solo escritura o todos los eventos de administración. De forma predeterminada, los almacenes de datos de eventos registran eventos de administración.</p> <p>Puede filtrar los eventos administrados en los siguientes campos del selector de eventos avanzados: <code>eventName</code> , <code>eventSource</code> , <code>eventType</code> , <code>readOnly</code> , <code>sessionCredentialFromConsole</code> y <code>userIdentity.arn</code> .</p> |
| <a href="#">Registrar eventos de datos</a>            | Puede usar <a href="#">selectores de eventos avanzados</a> para crear selectores detallados que registren solo los eventos que le interesen. Por ejemplo, puede filtrar por el campo <code>eventName</code> para incluir o excluir el registro de llamadas a la API específicas, lo que puede ayudar a controlar los costos. Para obtener más                                                                                                                                                                                                   |

| Tarea                                                                     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                           | información, consulte <a href="#">Filtrado de los eventos de datos mediante selectores de eventos avanzados</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <a href="#">Registro de eventos de actividad de la red</a>                | Puede configurar su almacén de datos de eventos para que registre eventos de actividad de la red. Puede utilizar selectores de eventos avanzados para filtrar en función de los campos <code>eventName</code> , <code>errorCode</code> y <code>vpcEndpointId</code> para registrar solo los eventos que le interesen.                                                                                                                                                                                                                                      |
| <a href="#">Registrar eventos de Insights</a>                             | <p>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 obtener más información, consulte <a href="#">Trabajar con CloudTrail Insights</a>.</p> <p>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 <a href="#">Precios de AWS CloudTrail</a>.</p> |
| <a href="#">Copiar eventos de registro de seguimiento</a>                 | Puede copiar los eventos de registro de seguimiento en un almacén de datos de eventos <a href="#">nuevo</a> o <a href="#">existente</a> para crear una instantánea puntual de los eventos registrados en el registro de seguimiento.                                                                                                                                                                                                                                                                                                                       |
| <a href="#">Habilitar la federación en un almacén de datos de eventos</a> | Puede federar un almacén de datos de eventos para ver los metadatos asociados al almacén de datos de eventos en el <a href="#">catálogo de datos de AWS Glue</a> 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.                                                                                                                               |

| Tarea                                                                                     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Detener o iniciar la ingesta de eventos en un almacén de datos de eventos</a> | 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.                                                                                                                                                                                                                                                  |
| <a href="#">Creación de una integración con un origen de eventos externo a AWS</a>        | 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 sobre los socios de integración disponibles, consulte <a href="#">Integraciones con AWS CloudTrail Lake</a> . |
| <a href="#">Visualización de consultas de ejemplo de Lake en la consola de CloudTrail</a> | La consola de CloudTrail brinda una serie de consultas de ejemplo que pueden ayudarlo a empezar a escribir sus propias consultas.                                                                                                                                                                                                                                                                                                             |
| <a href="#">Creación o edición de una consulta</a>                                        | 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.                                                                                                                                                                                                                           |
| <a href="#">Guardado de los resultados de las consultas en un bucket de S</a>             | Al ejecutar una consulta, puede guardar los resultados de la consulta en un bucket de S3.                                                                                                                                                                                                                                                                                                                                                     |
| <a href="#">Descargar los resultados de consultas guardados</a>                           | Puede descargar un archivo CSV que contenga los resultados de las consultas de CloudTrail Lake guardados.                                                                                                                                                                                                                                                                                                                                     |
| <a href="#">Validar los resultados de consultas guardados</a>                             | 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 acerca de CloudTrail Lake, consulte [Trabajar con AWS CloudTrail Lake](#).

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 [Administración de los costos de CloudTrail Lake](#).

## Paneles de CloudTrail Lake

Puede usar los paneles de CloudTrail Lake para consultar las tendencias de eventos de los almacenes de datos de eventos de la cuenta. CloudTrail Lake ofrece los siguientes tipos de paneles:

- **Paneles administrados:** puede ver un panel administrado para ver las tendencias de eventos de un almacén de datos de eventos que recopila eventos de administración, eventos de datos o eventos de Insights. Estos paneles están disponibles automáticamente y CloudTrail Lake los administra. CloudTrail ofrece 14 paneles administrados entre los que elegir. Puede actualizar manualmente los paneles administrados. No puede modificar, agregar ni eliminar los widgets de estos paneles; sin embargo, puede guardar un panel administrado como un panel personalizado si desea modificar los widgets o establecer un programa de actualización.
- **Paneles personalizados:** estos le permiten consultar eventos en cualquier tipo de almacén de datos de eventos. Puede agregar hasta 10 widgets a un panel personalizado. Puede actualizar manualmente un panel personalizado o puede establecer un programa de actualización.
- **Paneles destacados:** habilite el panel de aspectos destacados para ver información general a golpe de vista de la actividad recopilada de AWS por los almacenes de datos de eventos de la cuenta. CloudTrail administra el panel de aspectos destacados e incluye widgets que son pertinentes para la cuenta. Los widgets que se muestran en el panel de aspectos destacados son únicos para cada cuenta. Estos widgets podrían mostrar la actividad anormal o las anomalías detectadas. Por ejemplo, el panel de aspectos destacados podría incluir el Widget de acceso entre cuentas total, que muestra si hay un aumento en la actividad anormal entre cuentas. CloudTrail actualiza el panel de aspectos destacados cada 6 horas. En el panel se muestran los datos de las últimas 24 horas de la última actualización.

Cada panel consta de uno o más widgets y cada uno representa una consulta SQL.

Para obtener más información, consulte [Paneles de CloudTrail Lake](#).



## Registros de seguimiento de CloudTrail

Un registro de seguimiento es una configuración que permite la entrega de eventos a un bucket de Amazon S3 que especifique. También puede enviar y analizar los eventos de un registro de seguimiento con [Registros de Amazon CloudWatch](#) y [Amazon EventBridge](#).

Los registros de seguimiento pueden registrar eventos de administración de CloudTrail, eventos de datos, eventos de actividad de la red y eventos de Insights.

Puede crear registros de seguimiento multirregión y de una sola región para su Cuenta de AWS.

### registros de seguimiento multirregión

Cuando crea un registro de seguimiento de varias regiones, CloudTrail registra los eventos de todas las Regiones de AWS que están [habilitadas](#) en la Cuenta de AWS y envía los archivos de registro de eventos de CloudTrail al bucket de S3 que se especifique. Como práctica recomendada, le recomendamos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas. Todos los registros de seguimiento que se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones. Puede convertir un registro de seguimiento de una sola región en uno de varias regiones mediante la AWS CLI. Para obtener más información, consulte [Cómo entender los registros de seguimiento de varias regiones y las regiones optativas](#), [Creación de un registro de seguimiento con la consola](#) y [Conversión de un registro de seguimiento de una sola región en un registro de seguimiento de varias regiones](#).

### registros de seguimiento de una sola región

Cuando crea un registro de seguimiento de una sola región, CloudTrail solo registra los eventos de esa región. A continuación, entrega los archivos de registros de eventos de CloudTrail al bucket de Amazon S3 que especifique. Solo puede crear un registro de seguimiento de una sola región mediante la AWS CLI. Si crea registros de seguimiento individuales adicionales, puede disponer que dichos registros de seguimiento envíen los archivos de registro de eventos de CloudTrail al mismo bucket de S3 o a buckets separados. Esta es la opción predeterminada al crear un registro de seguimiento mediante la AWS CLI o la API de CloudTrail. Para obtener más información, consulte [Creación, actualización y administración de registros de seguimiento con la AWS CLI](#).

 Note

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

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.

De forma predeterminada, cuando crea un registro de seguimiento en la consola de CloudTrail, los archivos de registro de eventos y de resumen se cifran con una clave de KMS. Si decide no habilitar el cifrado SSE-KMS, los archivos de registros de eventos y de resumen se cifran mediante el cifrado del servidor (SSE) de Amazon S3. Puede almacenar sus archivos de registro en su bucket 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 archivos de registros varias veces por hora, cada 5 minutos aproximadamente. Estos archivos de registros contienen llamadas a la API de servicios en la cuenta que admite CloudTrail. Para obtener más información, consulte [Integraciones y servicios admitidos de CloudTrail](#).

 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 servicio 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.

CloudTrail captura las acciones realizadas directamente por el usuario o en nombre del usuario por un servicio de AWS. Por ejemplo, una llamada a `CreateStack` de 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 CloudFormation. Este comportamiento es normal y previsible. Puede identificar si la acción la ha realizado un servicio de AWS al consultar el campo `invokedby` del evento de CloudTrail.

En la siguiente tabla se proporciona información sobre las tareas que puede realizar en los registros de seguimiento.

| Tarea                                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Registro de eventos de administración</a>      | Configure sus registros de seguimiento para que registren eventos de solo lectura y solo escritura o todos los eventos de administración.                                                                                                                                                                                                                                                                                                                       |
| <a href="#">Registrar eventos de datos</a>                 | Puede usar <a href="#">selectores de eventos avanzados</a> para crear selectores detallados que registren solo los eventos que le interesen. Por ejemplo, puede filtrar por el campo <code>eventName</code> para incluir o excluir el registro de llamadas a la API específicas, lo que puede ayudar a controlar los costos. Para obtener más información, consulte <a href="#">Filtrado de los eventos de datos mediante selectores de eventos avanzados</a> . |
| <a href="#">Registro de eventos de actividad de la red</a> | Configure sus registros de seguimiento para que registren eventos de actividad de la red. Puede configurar los selectores de eventos avanzados para filtrar en función de los campos <code>eventName</code> , <code>errorCode</code> y <code>vpcEndpointId</code> y registrar solo los eventos que le interesen.                                                                                                                                                |

| Tarea                                                                        | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Registrar eventos de Insights</a>                                | <p>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 .</p> <p>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 <a href="#">Precios de AWS CloudTrail</a>.</p> |
| <a href="#">Visualización de eventos de Insights</a>                         | <p>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.</p>                                                                                                                                                                                                                                                                                 |
| <a href="#">Descargar eventos de Insights</a>                                | <p>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.</p>                                                                                                                                                                                                                                           |
| <a href="#">Copiar eventos de registro de seguimiento en CloudTrail Lake</a> | <p>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.</p>                                                                                                                                                                                                                                                     |

| Tarea                                                           | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Creación de un tema de Amazon SNS y suscripción</a> | <p>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.</p> <div data-bbox="829 541 1507 1094"><p> <b>Note</b></p><p>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 <a href="#">Uso de la biblioteca de procesamiento de CloudTrail</a>.</p></div> |
| <a href="#">Visualización de los archivos de registro</a>       | <p>Busque y descargue los archivos de registro del bucket de S3.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Tarea                                                                              | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Monitoreo de eventos con Registros de CloudWatch</a>                   | <p>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.</p> <div> <b>Note</b><br/>Si configura un registro de seguimiento de varias 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.</div> |
| <a href="#">Habilitar el cifrado de SSE-KMS</a>                                    | El cifrado de archivos de registros y de resumen con una clave de KMS ofrece una capa adicional de seguridad para sus datos de CloudTrail.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <a href="#">Habilitar la integridad de los archivos de registro</a>                | 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.                                                                                                                                                                                                                                                                                                                                                                              |
| <a href="#">Compartir archivos de registro con otras cuentas de Cuentas de AWS</a> | Puede compartir archivos de registros entre cuentas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <a href="#">Agrupar archivos de registro de varias cuentas</a>                     | Puede agrupar archivos de registros de varias cuentas en un solo bucket.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Tarea                                                 | Descripción                                                                                                                                                                                                                                                   |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Trabajar con soluciones de los socios</a> | 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. |

Puede crear un registro de seguimiento para enviar una copia de los eventos de administración en curso a su bucket de 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](#).

## Eventos de CloudTrail Insights

AWS CloudTrail Insights ayuda a los usuarios de AWS a identificar y responder a la actividad inusual asociada a las tasas de llamada 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 las tasas de llamada a la API se generan para las API de administración de `write` y los eventos de Insights en la tasa de errores de la API se generan tanto para las API de administración `read` como `write`.

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos de CloudTrail no registran eventos de Insights. Debe configurar sus registros de seguimiento y almacenes de datos de eventos para que registren los eventos de Insights. Para obtener más información, consulte [Registro de eventos de Insights con la consola de CloudTrail](#) y [Registro de eventos de Insights con la AWS CLI](#).

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](#).

## Visualización de eventos de Insights para registros de seguimiento y almacenes de datos de eventos

CloudTrail admite los eventos de Insights tanto para los registros de seguimiento 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 ha habilitado los eventos de Insights en un registro de seguimiento y CloudTrail detecta actividad inusual, los eventos de Insights se registran en una carpeta o prefijo diferente en el bucket de S3 de destino para su registro de seguimiento. También puede ver el tipo de información y el periodo de tiempo del incidente al consultar los eventos de Insights en la consola de CloudTrail. Para obtener más información, consulte [Cómo visualizar eventos de Insights para registros de seguimiento con la consola](#).

Después de habilitar Insights de CloudTrail por primera vez en un registro de seguimiento, CloudTrail puede tardar hasta 36 horas en empezar a entregar los eventos de Insights después que habilite los eventos de Insights en un registro de seguimiento, siempre que se detecte actividad inusual durante ese tiempo.

### 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 almacén de datos de eventos de origen que habilite Insights y registre los eventos de administración. Para obtener más información, consulte [Creación de un almacén de datos de eventos para los eventos de Insights con la consola](#).

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.

Si ha habilitado CloudTrail Insights en un almacén de datos de eventos de origen y CloudTrail detecta actividad inusual, CloudTrail entrega los eventos de Insights en el almacén 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 S3. Para obtener más información, consulte [Creación o edición de una consulta con la consola de CloudTrail](#) y [Visualización de consultas de ejemplo con la consola de CloudTrail](#).



También puede ver el panel de Eventos de Insights para ver los eventos de Insights del almacén de datos de eventos de destino. Para obtener más información acerca de los paneles de Lake, consulte [Paneles de CloudTrail Lake](#).

## Canales de CloudTrail

CloudTrail es compatible con dos tipos de canales:

### Canales para integraciones de CloudTrail Lake con orígenes de eventos externos a AWS

CloudTrail Lake utiliza canales para incluir elementos ajenos a AWS en 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 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

Los servicios de AWS pueden crear un canal vinculado a servicios para recibir eventos de CloudTrail 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 solo a la región actual.

Puede usar la [consola de CloudTrail](#) o la [AWS CLI](#) para ver la información sobre cualquier canal vinculado a servicios de CloudTrail creado por los Servicios de AWS.

## Conceptos de CloudTrail

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

Conceptos:

- [Eventos de CloudTrail](#)
- [Historial de eventos](#)

- [Registros de seguimiento](#)
- [Registros de seguimiento de la organización](#)
- [CloudTrail Lake y los almacenes de datos de eventos](#)
- [CloudTrail Insights](#)
- [Etiquetas](#)
- [AWS Security Token Service y CloudTrail](#)
- [Eventos de servicios globales](#)

## Eventos de CloudTrail

Un evento en CloudTrail es el registro de una actividad en una cuenta de AWS. Esta actividad puede ser una acción de una identidad de IAM o un servicio que CloudTrail puede supervisar. Los eventos de CloudTrail proporcionan un historial de las actividades de la cuenta, tanto de la API como no de esta, que se realizan a través de la Consola de administración de AWS, los SDK de AWS, las herramientas de línea de comando y otros servicios de AWS.

Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas a la API públicas, por lo que los eventos no aparecen en un orden específico.

CloudTrail registra cuatro tipos de eventos:

- [Eventos de administración](#)
- [Eventos de datos](#)
- [Eventos de actividad de la red](#)
- [Eventos de Insights](#)

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

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.

Para obtener información sobre cómo integrar Servicios de AWS con CloudTrail, consulte [AWSTemas de servicio de para CloudTrail](#).

## Eventos de administración

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su 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 AWS Identity and Access Management de `AttachRolePolicy`).
- 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 AWS CloudTrail de `CreateTrail`).

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](#).

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos de CloudTrail Lake registran los eventos de administración. Para obtener más información sobre el registro de eventos de administración, consulte [Registro de eventos de administración](#).

## 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 el nivel de objeto de Amazon S3](#) (por ejemplo, las operaciones `GetObject`, `DeleteObject` y `PutObject` de la API) en objetos de los buckets de S3.
- Actividad de ejecución de funciones de AWS Lambda (la API `Invoke`).
- La actividad de [PutAuditEvents](#) de CloudTrail en un [canal de CloudTrail Lake](#) que se utiliza para registrar eventos externos a AWS.

- Operaciones de la API [Publish](#) y [PublishBatch](#) de Amazon SNS sobre temas.

En la siguiente tabla, se muestran los tipos de recursos disponibles para los registros de seguimiento y los almacenes de datos de eventos. En la columna Tipo de recurso (consola), se muestra la selección adecuada en la consola. En la columna `resources.type value`, se muestra el valor de `resources.type` que debe especificar para incluir eventos de datos de ese tipo en el registro de seguimiento o el almacén de datos de eventos por medio de la AWS CLI o las API de CloudTrail.

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

#### Eventos de datos compatibles con AWS CloudTrail

| Servicio de AWS | Descripción                                                                                                                                                                                               | Tipo de recurso (consola)                     | <code>resources.type value</code> |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|-----------------------------------|
| Amazon RDS      | <a href="#">Actividad de la API de Amazon RDS</a> en un clúster de base de datos.                                                                                                                         | API de datos de RDS: clúster de base de datos | <code>AWS::RDS::DBCluster</code>  |
| Amazon S3       | <a href="#">Actividad de la API en el nivel de objeto de Amazon S3</a> (por ejemplo, las operaciones <code>GetObject</code> , <code>DeleteObject</code> y <code>PutObject</code> de la API) en objetos de | S3                                            | <code>AWS::S3::Object</code>      |

| Servicio de AWS     | Descripción                                                                                                                                                                                                                          | Tipo de recurso (consola) | resources.type value             |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------------------|
|                     | los buckets de uso general.                                                                                                                                                                                                          |                           |                                  |
| Amazon S3           | <a href="#">Actividad de la API de Amazon S3</a> en los puntos de acceso.                                                                                                                                                            | Punto de acceso de S      | AWS::S3::AccessPoint             |
| Amazon S3           | <a href="#">Actividad de la API en el nivel de objeto de Amazon S3</a> (por ejemplo, las operaciones <code>GetObject</code> , <code>DeleteObject</code> y <code>PutObject</code> de la API) en objetos de los buckets de directorio. | S3 Express                | AWS::S3Express::Object           |
| Amazon S3           | <a href="#">Actividad de la API en los puntos de acceso de Amazon S3 Object Lambda</a> , como las llamadas a <code>CompleteMultipartUpload</code> y <code>GetObject</code> .                                                         | S3 Object Lambda          | AWS::S3ObjectLambda::AccessPoint |
| Amazon S3           | Actividad de la API de Amazon FSx en volúmenes.                                                                                                                                                                                      | Volumen de FSx            | AWS::FSx::Volume                 |
| Tablas de Amazon S3 | Actividad de la API de Amazon S3 en las <a href="#">tablas</a> .                                                                                                                                                                     | Tabla de S3               | AWS::S3Tables::Table             |

| Servicio de AWS       | Descripción                                                                                             | Tipo de recurso (consola)                 | resources.type value         |
|-----------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------|
| Tablas de Amazon S3   | Actividad de la API de Amazon S3 en los <a href="#">buckets de las tablas</a> .                         | Bucket de tablas de S3                    | AWS::S3Tables::TableBucket   |
| Amazon S3 Vectors     | Actividad de la API de Amazon S3 en los <a href="#">buckets de vectores</a> .                           | Bucket de vector S3                       | AWS::S3Vectors::VectorBucket |
| Amazon S3 Vectors     | Actividad de la API de Amazon S3 en <a href="#">índices de vectores</a> .                               | Índice de vector S3                       | AWS::S3Vectors::Index        |
| Amazon S3 en Outposts | <a href="#">Actividad de la API en cuanto a objetos de Amazon S3 en Outposts</a> .                      | S3 Outposts                               | AWS::S3Outposts::Object      |
| Amazon SNS            | Operaciones de la API <a href="#">Publish</a> de Amazon SNS en los puntos de conexión de la plataforma. | Punto de conexión de la plataforma de SNS | AWS::SNS::PlatformEndpoint   |
| Amazon SNS            | Operaciones de la API <a href="#">Publish</a> y <a href="#">PublishBatch</a> de Amazon SNS sobre temas. | Tema de SNS                               | AWS::SNS::Topic              |
| Amazon SQS            | <a href="#">Actividad de la API de Amazon SQS</a> en los mensajes.                                      | SQS                                       | AWS::SQS::Queue              |

| Servicio de AWS    | Descripción                                                                                                                                                      | Tipo de recurso (consola) | resources.type value          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------------|
| AWS Supply Chain   | Actividad de la API de AWS Supply Chain en una instancia.                                                                                                        | Supply Chain              | AWS::SCN::Instance            |
| Amazon SWF         | <a href="#">Actividad de la API de Amazon SWF</a> en los dominios.                                                                                               | Dominio de SWF            | AWS::SWF::Domain              |
| AWS AppConfig      | <a href="#">Actividad de la API de AWS AppConfig</a> para operaciones de configuración, como las llamadas a StartConfigurationSession y GetLatestConfiguration . | AWS AppConfig             | AWS::AppConfig::Configuration |
| AWS AppSync        | <a href="#">Actividad de la API de AWS AppSync</a> en las API GraphQL de AppSync.                                                                                | AppSync Graph             | AWS::AppSync::GraphQLApi      |
| Amazon Aurora DSQL | Actividad de la API de Amazon Aurora DSQL en los recursos del clúster.                                                                                           | Amazon Aurora DSQL        | AWS::DSQL::Cluster            |

| Servicio de AWS                 | Descripción                                                                                                                                                                         | Tipo de recurso (consola)              | resources.type value                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------------|
| Intercambio de datos B2B de AWS | Actividad de la API de intercambio de datos entre empresas para operaciones de Transformer, como las llamadas a <code>GetTransformerJob</code> y <code>StartTransformerJob</code> . | Intercambio de datos entre empresas    | <code>AWS::B2BI::Transformer</code>    |
| AWS Backup                      | Actividad de la API de datos de búsqueda de AWS Backup en trabajos de búsqueda.                                                                                                     | AWS Backup API de datos de búsqueda de | <code>AWS::Backup::SearchJob</code>    |
| Amazon Bedrock                  | <a href="#">Actividad de la API de Amazon Bedrock</a> en un alias de agente.                                                                                                        | Alias de agente de Bedrock             | <code>AWS::Bedrock::AgentAlias</code>  |
| Amazon Bedrock                  | Actividad de la API de Amazon Bedrock en invocaciones asíncronas.                                                                                                                   | Invocación asíncrona de Bedrock        | <code>AWS::Bedrock::AsyncInvoke</code> |
| Amazon Bedrock                  | Actividad de la API de Amazon Bedrock en un alias de flujo.                                                                                                                         | Alias de flujo de Bedrock              | <code>AWS::Bedrock::FlowAlias</code>   |
| Amazon Bedrock                  | Actividad de la API de Amazon Bedrock en barreras de protección.                                                                                                                    | Barrera de protección de Bedrock       | <code>AWS::Bedrock::Guardrail</code>   |



| Servicio de AWS | Descripción                                                                         | Tipo de recurso (consola)                        | resources.type value                   |
|-----------------|-------------------------------------------------------------------------------------|--------------------------------------------------|----------------------------------------|
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en un agente insertado                        | Agente insertado e invocado en Bedrock           | AWS::Bedrock::InlineAgent              |
| Amazon Bedrock  | <a href="#">Actividad de la API de Amazon Bedrock</a> en una base de conocimientos. | Base de conocimientos de Bedrock                 | AWS::Bedrock::KnowledgeBase            |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en modelos.                                   | Modelo de Bedrock                                | AWS::Bedrock::Model                    |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en peticiones.                                | Petición de Bedrock                              | AWS::Bedrock::PromptVersion            |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en sesiones.                                  | Sesión de Bedrock                                | AWS::Bedrock::Session                  |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en ejecuciones de flujo.                      | Ejecución de flujo de Bedrock                    | AWS::Bedrock::FlowExecution            |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en una política de razonamiento automatizado. | Política de razonamiento automatizado de Bedrock | AWS::Bedrock::AutomatedReasoningPolicy |

| Servicio de AWS | Descripción                                                                                       | Tipo de recurso (consola)                                      | resources.type value                          |
|-----------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------|
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en una versión de la política de razonamiento automatizado. | Versión de la política de razonamiento automatizado de Bedrock | AWS::Bedrock::AutomatedReasoningPolicyVersion |
| Amazon Bedrock  | Actividad de la API del proyecto de automatización de datos de Amazon Bedrock.                    | Proyectos de automatización de datos de Bedrock                | AWS::Bedrock::DataAutomationProject           |
| Amazon Bedrock  | Actividad de la API de invocación de automatización de datos de Bedrock.                          | Invocación de automatización de datos de Bedrock               | AWS::Bedrock::DataAutomationInvocation        |
| Amazon Bedrock  | Actividad de la API del perfil de automatización de datos de Amazon Bedrock.                      | Perfil de automatización de datos de Bedrock                   | AWS::Bedrock::DataAutomationProfile           |
| Amazon Bedrock  | Actividad de la API del esquema de Amazon Bedrock.                                                | Esquema de Bedrock                                             | AWS::Bedrock::Blueprint                       |
| Amazon Bedrock  | Actividad de la API de intérprete de código de Amazon Bedrock.                                    | Intérprete de código AgentCore de Bedrock                      | AWS::BedrockAgentCore::CodeInterpreter        |

| Servicio de AWS | Descripción                                                                            | Tipo de recurso (consola)                                           | resources.type value                             |
|-----------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------|
| Amazon Bedrock  | Actividad de la API del navegador Amazon Bedrock.                                      | Navegador AgentCore de Bedrock                                      | AWS::BedrockAgentCore::Browser                   |
| Amazon Bedrock  | Actividad de la API de identidad de carga de trabajo de Amazon Bedrock.                | Identidad de carga de trabajo de AgentCore de Bedrock               | AWS::BedrockAgentCore::WorkloadIdentity          |
| Amazon Bedrock  | Actividad de la API del directorio de identidad de carga de trabajo de Amazon Bedrock. | Directorio de identidad de carga de trabajo de AgentCore de Bedrock | AWS::BedrockAgentCore::WorkloadIdentityDirectory |
| Amazon Bedrock  | Actividad de la API de bóveda de token de Amazon Bedrock .                             | Bóveda de token de AgentCore de Bedrock                             | AWS::BedrockAgentCore::TokenVault                |
| Amazon Bedrock  | Actividad de la API de CredentialProvider de APIKey de Amazon Bedrock.                 | Credentia IProvider de APIKey de AgentCore de Bedrock               | AWS::BedrockAgentCore::APIKeyCredentialProvider  |
| Amazon Bedrock  | Actividad de la API de tiempo de ejecución de Amazon Bedrock.                          | Tiempo de ejecución de AgentCore de Bedrock                         | AWS::BedrockAgentCore::Runtime                   |

| Servicio de AWS | Descripción                                                                          | Tipo de recurso (consola)                                         | resources.type value                            |
|-----------------|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------|
| Amazon Bedrock  | Actividad de la API del tiempo de ejecución del punto de conexión de Amazon Bedrock. | Tiempo de ejecución de AgentCore del punto de conexión de Bedrock | AWS::BedrockAgentCore::RuntimeEndpoint          |
| Amazon Bedrock  | Actividad de la API de la puerta de enlace de Amazon Bedrock.                        | Puerta de enlace AgentCore de Bedrock                             | AWS::BedrockAgentCore::Gateway                  |
| Amazon Bedrock  | Actividad de la API de memoria de Amazon Bedrock.                                    | Memoria de AgentCore de Bedrock                                   | AWS::BedrockAgentCore::Memory                   |
| Amazon Bedrock  | Actividad de la API de CredentialProvider de OAuth2 de Amazon Bedrock.               | Credentia IProvider de OAuth2 de AgentCore de Bedrock             | AWS::BedrockAgentCore::OAuth2CredentialProvider |
| Amazon Bedrock  | Actividad de API personalizada del navegador Amazon Bedrock.                         | Navegador AgentCore personalizado de Bedrock                      | AWS::BedrockAgentCore::BrowserCustom            |
| Amazon Bedrock  | Actividad de la API de intérprete de código personalizado de Amazon Bedrock.         | Intérprete de código AgentCore personalizado de Bedrock           | AWS::BedrockAgentCore::CodeInterpreterCustom    |

| Servicio de AWS                              | Descripción                                                                                                                                                       | Tipo de recurso (consola)           | resources.type value             |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|----------------------------------|
| Amazon Bedrock                               | Actividad de la API de la herramienta de Amazon Bedrock.                                                                                                          | Herramienta de Bedrock              | AWS::Bedrock::Tool               |
| AWS Cloud Map                                | <a href="#">Actividad AWS Cloud Map de la API</a> en un <a href="#">espacio de nombres</a> .                                                                      | AWS Cloud Map Espacio de nombres de | AWS::ServiceDiscovery::Namespace |
| AWS Cloud Map                                | <a href="#">Actividad AWS Cloud Map de la API</a> en un <a href="#">servicio</a> .                                                                                | AWS Cloud Map Servicio de           | AWS::ServiceDiscovery::Service   |
| Amazon CloudFront                            | Actividad de la API de CloudFront en un <a href="#">KeyValueStore</a> .                                                                                           | CloudFront KeyValueStore            | AWS::CloudFront::KeyValueStore   |
| AWS CloudTrail                               | La actividad de <a href="#">PutAuditEvents</a> de CloudTrail en un <a href="#">canal de CloudTrail Lake</a> que se utiliza para registrar eventos externos a AWS. | Canal de CloudTrail                 | AWS::CloudTrail::Channel         |
| Amazon CloudWatch                            | <a href="#">Actividad de la API de Amazon CloudWatch</a> en las métricas.                                                                                         | Métrica de CloudWatch               | AWS::CloudWatch::Metric          |
| Monitor de flujo de red de Amazon CloudWatch | Actividad de la API del monitor de flujo de red de Amazon CloudWatch en los monitores.                                                                            | Monitor de flujo de red             | AWS::NetworkFlowMonitor::Monitor |

| Servicio de AWS                              | Descripción                                                                                           | Tipo de recurso (consola)                      | resources.type value                  |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------|---------------------------------------|
| Monitor de flujo de red de Amazon CloudWatch | Actividad de la API del monitor de flujo de red de Amazon CloudWatch en el alcance.                   | Agente del monitor de flujo de red del alcance | AWS::NetworkFlowMonitor::Scope        |
| Amazon CloudWatch RUM                        | Actividad de la API de Amazon CloudWatch RUM en los monitores de aplicaciones.                        | Monitor de aplicaciones de RUM                 | AWS::RUM::AppMonitor                  |
| Generador de perfiles de Amazon CodeGuru     | Actividad de la API de perfiles de CodeGuru en grupos de creación de perfiles.                        | Grupo de perfiles de CodeGuru                  | AWS::CodeGuruProfiler::ProfilingGroup |
| Amazon CodeWhisperer                         | Actividad de la API de Amazon CodeWhisperer en una personalización.                                   | Personalización de CodeWhisperer               | AWS::CodeWhisperer::Customization     |
| Amazon CodeWhisperer                         | Actividad de la API de Amazon CodeWhisperer en un perfil.                                             | CodeWhisperer                                  | AWS::CodeWhisperer::Profile           |
| Amazon Cognito                               | Actividad de la API de Amazon Cognito en los <a href="#">grupos de identidades</a> de Amazon Cognito. | Grupos de identidades de Cognito               | AWS::Cognito::IdentityPool            |
| AWS Data Exchange                            | Actividad de la API de AWS Data Exchange en los activos.                                              | Activo de Data Exchange                        | AWS::DataExchange::Asset              |

| Servicio de AWS      | Descripción                                                                   | Tipo de recurso (consola)    | resources.type value                 |
|----------------------|-------------------------------------------------------------------------------|------------------------------|--------------------------------------|
| Amazon Data Firehose | Actividad de la API del flujo de entrega de Amazon Data Firehose              | Amazon Data Firehose         | AWS::KinesisFirehose::DeliveryStream |
| AWS Deadline Cloud   | <a href="#">Deadline Cloud</a><br>Actividad de la API de en las flotas.       | Deadline Cloud Flota de      | AWS::Deadline::Fleet                 |
| AWS Deadline Cloud   | <a href="#">Deadline Cloud</a><br>Actividad de la API de en los trabajos.     | Deadline Cloud Trabajo de    | AWS::Deadline::Job                   |
| AWS Deadline Cloud   | <a href="#">Deadline Cloud</a><br>Actividad de la API de en las colas.        | Deadline Cloud Cola de       | AWS::Deadline::Queue                 |
| AWS Deadline Cloud   | <a href="#">Deadline Cloud</a><br>Actividad de la API de en los trabajadores. | Deadline Cloud Trabajador de | AWS::Deadline::Worker                |

| Servicio de AWS | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Tipo de recurso (consola) | resources.type value |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------|
| Amazon DynamoDB | <p><a href="#">Actividad de la API en el nivel de elemento de Amazon DynamoDB</a> en las tablas (por ejemplo, las operaciones PutItem, DeleteItem y UpdateItem de la API).</p> <div>  <b>Note</b><br/>           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,         </div> | DynamoDB                  | AWS::DynamoDB::Table |



| Servicio de AWS | Descripción                                                                                                                                                                                                       | Tipo de recurso (consola) | resources.type value  |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------------|
|                 | <p>registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir <a href="#">eventos de flujos</a>, agregue un filtro en el campo eventName .</p> |                           |                       |
| Amazon DynamoDB | Actividad de la API de <a href="#">Amazon DynamoDB</a> en los flujos.                                                                                                                                             | DynamoDB Streams          | AWS::DynamoDB::Stream |

| Servicio de AWS                   | Descripción                                                                                                                                                   | Tipo de recurso (consola)                    | resources.type value              |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------|
| Amazon Elastic Block Store        | API directas de <a href="#">Amazon Elastic Block Store (EBS)</a> , como PutSnapshotBlock, GetSnapshotBlock y ListChangedBlocks en instantáneas de Amazon EBS. | API directas de Amazon EBS                   | AWS::EC2::Snapshot                |
| Amazon Elastic Compute Cloud      | Actividad de la API del punto de conexión de Amazon EC2 Instance Connect                                                                                      | Punto de conexión a EC2 Instance Connect     | AWS::EC2::InstanceConnectEndpoint |
| Amazon Elastic Container Service  | Actividad de la API de Amazon Elastic Container Service en una instancia de contenedor.                                                                       | Instancia de contenedor de ECS               | AWS::ECS::ContainerInstance       |
| Amazon Elastic Kubernetes Service | Actividad de la API de Amazon Elastic Kubernetes Service en los paneles.                                                                                      | Paneles de Amazon Elastic Kubernetes Service | AWS::EKS::Dashboard               |

| Servicio de AWS                                         | Descripción                                                                                                                      | Tipo de recurso (consola)                                     | resources.type value                |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------|
| Amazon EMR                                              | <a href="#">Actividad de la API de Amazon EMR</a> en un espacio de trabajo de registros de escritura anticipada.                 | Espacio de trabajo de registro de escritura anticipada de EMR | AWS::EMRWAL::Workspace              |
| Mensajes SMS para usuarios finales de AWS               | Actividad de la API de <a href="#">Mensajes SMS para usuarios finales de AWS</a> en las identidades de origen.                   | Identidad de origen de SMS Voice                              | AWS::SMSVoice::OriginationIdentity  |
| Mensajes SMS para usuarios finales de AWS               | Actividad de la API de <a href="#">mensajes SMS para usuarios finales de AWS</a> en los mensajes.                                | Mensaje de voz de SMS                                         | AWS::SMSVoice::Message              |
| Mensajes de redes sociales para usuarios finales de AWS | Actividad de la API de <a href="#">Mensajes de redes sociales para usuarios finales de AWS</a> en los ID de números de teléfono. | ID de número de teléfono de mensajes de redes sociales        | AWS::SocialMessaging::PhoneNumberId |
| Mensajes de redes sociales para usuarios finales de AWS | Actividad de la API de Mensajes de redes sociales de AWS para usuarios finales en los ID de Waba.                                | ID de Waba ID de mensajes de redes sociales                   | AWS::SocialMessaging::WabaId        |

| Servicio de AWS         | Descripción                                                                                                 | Tipo de recurso (consola)                  | resources.type value              |
|-------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------|
| Amazon FinSpace         | <a href="#">Amazon FinSpace</a><br>Actividad de la API de en entornos.                                      | FinSpace                                   | AWS::FinSpace::Environment        |
| Amazon GameLift Streams | <a href="#">Actividad de la API de transmisión</a> de Amazon GameLift Streams en las aplicaciones.          | Aplicación de GameLift Streams             | AWS::GameLiftStreams::Application |
| Amazon GameLift Streams | <a href="#">Actividad de la API de transmisión</a> de Amazon GameLift Streams en los grupos de transmisión. | Grupo de transmisiones de GameLift Streams | AWS::GameLiftStreams::StreamGroup |
| AWS Glue                | Actividad de la API de AWS Glue en tablas creadas por Lake Formation.                                       | Lake Formation                             | AWS::Glue::Table                  |
| Amazon GuardDuty        | Actividad de la API de Amazon GuardDuty para un <a href="#">detector</a> .                                  | Detector de GuardDuty                      | AWS::GuardDuty::Detector          |
| AWS HealthImaging       | Actividad de la API de AWS HealthImaging en los almacenes de datos.                                         | Almacén de datos de MedicalImaging         | AWS::MedicalImaging::Datastore    |

| Servicio de AWS              | Descripción                                                                                                                                                                                                                                                                                            | Tipo de recurso (consola)              | resources.type value                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------|
| AWS HealthImaging            | Actividad de la API del conjunto de imágenes de AWS HealthImaging.                                                                                                                                                                                                                                     | Conjunto de imágenes de MedicalImaging | AWS::MedicalImaging::Imageset       |
| AWS IoT                      | <a href="#">Actividad de la API de AWS IoT en los certificados.</a>                                                                                                                                                                                                                                    | Certificado IoT                        | AWS::IoT::Certificate               |
| AWS IoT                      | <a href="#">Actividad de la API de AWS IoT en los objetos.</a>                                                                                                                                                                                                                                         | Objeto de IoT                          | AWS::IoT::Thing                     |
| AWS IoT Greengrass Version 2 | <a href="#">Actividad de la API de Greengrass</a> desde un dispositivo principal de Greengrass en una versión del componente. <div>  <b>Note</b><br/> Greengrass no registra los eventos de acceso denegado. </div> | Versión del componente IoT Greengrass  | AWS::GreengrassV2::ComponentVersion |

| Servicio de AWS               | Descripción                                                                                                                                                                                                                                                                                 | Tipo de recurso (consola)        | resources.type value                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|--------------------------------------|
| AWS IoT Greengrass Version 2  | <p><a href="#">Actividad de la API de Greengrass</a> desde un dispositivo principal de Greengrass en una implementación.</p> <div>  Note<br/>Greengrass no registra los eventos de acceso denegado. </div> | Implementación de IoT Greengrass | AWS::GreengrassV2::Deployment        |
| AWS IoT SiteWise              | <a href="#">Actividad de la API de IoT SiteWise</a> en los <a href="#">activos</a> .                                                                                                                                                                                                        | Activo de IoT SiteWise           | AWS::IoTSiteWise::Asset              |
| AWS IoT SiteWise              | <a href="#">Actividad de la API de IoT SiteWise</a> en las <a href="#">series temporales</a> .                                                                                                                                                                                              | Serie temporal de IoT SiteWise   | AWS::IoTSiteWise::TimeSeries         |
| AWS IoT SiteWise Assistant de | Actividad de la API de Sitewise Assistant en las conversaciones.                                                                                                                                                                                                                            | Conversación con Sitewise Assist | AWS::SitewiseAssistant::Conversation |
| AWS IoT TwinMaker             | Actividad de la API de IoT TwinMaker en una <a href="#">entidad</a> .                                                                                                                                                                                                                       | Entidad de IoT TwinMaker         | AWS::IoTTwinMaker::Entity            |

| Servicio de AWS                         | Descripción                                                                                                                  | Tipo de recurso (consola)           | resources.type value                |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| AWS IoT TwinMaker                       | Actividad de la API de IoT TwinMaker en un <a href="#">espacio de trabajo</a> .                                              | Espacio de trabajo de IoT TwinMaker | AWS::IoT::TwinMaker::Workspace      |
| Amazon Kendra Intelligent Ranking       | Actividad de la API de Amazon Kendra Intelligent Ranking en los <a href="#">planes de ejecución de nuevas puntuaciones</a> . | Kendra Ranking                      | AWS::Kendra::Ranking::ExecutionPlan |
| Amazon Keyspaces (for Apache Cassandra) | <a href="#">Actividad de la API de Amazon Keyspaces</a> en una tabla.                                                        | Tabla de Cassandra                  | AWS::Cassandra::Table               |
| Amazon Keyspaces (for Apache Cassandra) | Actividad de la API de Amazon Keyspaces (para Apache Cassandra) en transmisiones de Cassandra CDC.                           | Transmisiones de Cassandra CDC      | AWS::Cassandra::Stream              |
| Amazon Kinesis Data Streams             | Actividad de la API de Kinesis Data Streams en los <a href="#">flujos</a> .                                                  | Flujo de Kinesis                    | AWS::Kinesis::Stream                |
| Amazon Kinesis Data Streams             | Actividad de la API de Kinesis Data Streams en los <a href="#">consumidores de flujos</a> .                                  | Consumidor de flujos de Kinesis     | AWS::Kinesis::StreamConsumer        |

| Servicio de AWS              | Descripción                                                                                                  | Tipo de recurso (consola)                 | resources.type value                |
|------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------|
| Amazon Kinesis Video Streams | Actividad de la API de Kinesis Video Streams en transmisiones de video, como llamadas a GetMedia y PutMedia. | Kinesis Video Streams                     | AWS::KinesisVideo::Stream           |
| Amazon Kinesis Video Streams | Actividad de la API del canal de señalización de video de Kinesis Video Streams.                             | Canal de señalización de video de Kinesis | AWS::KinesisVideo::SignalingChannel |
| AWS Lambda                   | Actividad de ejecución de funciones de AWS Lambda (la API Invoke).                                           | Lambda                                    | AWS::Lambda::Function               |
| Mapas de Amazon Location     | Actividad de la API de mapas de Amazon Location                                                              | Mapas geográficos                         | AWS::GeoMaps::Provider              |
| Amazon Location Places       | Actividad de la API de Amazon Location Places.                                                               | Lugares geográficos                       | AWS::GeoPlaces::Provider            |
| Rutas de Amazon Location     | Actividad de la API de rutas de Amazon Location                                                              | Rutas geográficas                         | AWS::GeoRoutes::Provider            |
| Amazon Machine Learning      | Actividad de la API de machine learning en modelos de ML.                                                    | MLModel de machine learning               | AWS::MachineLearning::MLModel       |



| Servicio de AWS                              | Descripción                                                                                                                       | Tipo de recurso (consola) | resources.type value                  |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------|
| Amazon Managed Blockchain                    | Actividad de la API de Amazon Managed Blockchain en una red.                                                                      | Red de Managed Blockchain | AWS::ManagedBlockchain::Network       |
| Amazon Managed Blockchain                    | Llamadas JSON-RPC de <a href="#">Amazon Managed Blockchain</a> en nodos de Ethereum, como eth_getBalance o eth_getBlockByNumber . | Managed Blockchain        | AWS::ManagedBlockchain::Node          |
| Amazon Managed Blockchain Query              | Actividad de la API de Amazon Managed Blockchain Query.                                                                           | Managed Blockchain Query  | AWS::ManagedBlockchainQuery::QueryAPI |
| Amazon Managed Workflows para Apache Airflow | Actividad de la API de Amazon MWAA en entornos.                                                                                   | Managed Apache Airflow    | AWS::MWAA::Environment                |
| 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              |

| Servicio de AWS          | Descripción                                                                   | Tipo de recurso (consola)                     | resources.type value             |
|--------------------------|-------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------|
| Amazon One Enterprise    | Actividad de la API de Amazon One Enterprise en una clave de usuario.         | Clave de usuario de Amazon One                | AWS::One::UKey                   |
| Amazon One Enterprise    | Actividad de la API de Amazon One Enterprise en los usuarios.                 | Usuario de Amazon One                         | AWS::One::User                   |
| AWS Payment Cryptography | Actividad de la API de AWS Payment Cryptography en los alias.                 | Alias de Payment Cryptography                 | AWS::PaymentCryptography::Alias  |
| AWS Payment Cryptography | Actividad de la API de AWS Payment Cryptography en las claves.                | Clave de Payment Cryptography                 | AWS::PaymentCryptography::Key    |
| Amazon Pinpoint          | Actividad de la API de Amazon Pinpoint en aplicaciones de segmentación móvil. | Aplicación de segmentación móvil              | AWS::Pinpoint::App               |
| AWS Private CA           | Conector AWS Private CA para la actividad de la API de Active Directory.      | AWS Private CA Conector para Active Directory | AWS::PCAConnectorAD::Connector   |
| AWS Private CA           | Conector de AWS Private CA para la actividad de la API de SCEP.               | AWS Private CA Conector para SCEP             | AWS::PCAConnectorSCEP::Connector |

| Servicio de AWS    | Descripción                                                                      | Tipo de recurso (consola)            | resources.type value          |
|--------------------|----------------------------------------------------------------------------------|--------------------------------------|-------------------------------|
| Amazon Q Apps      | Actividad de la API de datos en <a href="#">Amazon Q Apps</a> .                  | Amazon Q Apps                        | AWS::QApps::QApp              |
| Amazon Q Apps      | Actividad de la API de datos en las sesiones de Amazon Q Apps.                   | Sesión de Amazon Q App               | AWS::QApps::QAppSession       |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en una aplicación.      | Aplicación de Amazon Q Business      | AWS::QBusiness::Application   |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en un origen de datos.  | Origen de datos de Amazon Q Business | AWS::QBusiness::DataSource    |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en un índice.           | Índice de Amazon Q Business          | AWS::QBusiness::Index         |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en una experiencia web. | Experiencia web de Amazon Q Business | AWS::QBusiness::WebExperience |
| Amazon Q Business  | Actividad de la API de integración de Amazon Q Business.                         | Integración de Amazon Q Business     | AWS::QBusiness::Integration   |
| Amazon Q Developer | Actividad de la API de Amazon Q Developer en una integración.                    | Integración para Q Developer         | AWS::QDeveloper::Integration  |

| Servicio de AWS     | Descripción                                                                                                 | Tipo de recurso (consola)                  | resources.type value             |
|---------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------|----------------------------------|
| Amazon Q Developer  | <a href="#">Actividad de la API de Amazon Q Developer en investigaciones operativas.</a>                    | Grupos de investigación de AIOps           | AWS::AIOps::InvestigationGroup   |
| Amazon Quick Suite  | Actividad de la API de Amazon Quick Suite en un conector de acciones.                                       | AWS Acciones de QuickSuite de              | AWS::Quicksight::ActionConnector |
| Amazon Quick Suite  | Actividad de la API de flujo de Amazon Quick Suite.                                                         | AWS::Quicksight::Flow                      | AWS::Quicksight::Flow            |
| Amazon Quick Suite  | Actividad de la API de FlowSession de Amazon Quick Suite.                                                   | AWS::Quicksight::FlowSession               | AWS::Quicksight::FlowSession     |
| Amazon SageMaker AI | Actividad de <a href="#">InvokeEndpointWithResponseStream</a> de Amazon SageMaker AI en puntos de conexión. | Punto de conexión de SageMaker AI          | AWS::SageMaker::Endpoint         |
| Amazon SageMaker AI | Actividad de la API de Amazon SageMaker AI en los almacenes de características.                             | Almacén de características de SageMaker AI | AWS::SageMaker::FeatureGroup     |

| Servicio de AWS             | Descripción                                                                                                              | Tipo de recurso (consola)                                        | resources.type value                     |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------|
| Amazon SageMaker AI         | Actividad de la API de Amazon SageMaker AI en los <a href="#">componentes del registro de seguimiento experimental</a> . | Componente de prueba del experimento de métricas de SageMaker AI | AWS::SageMaker::ExperimentTrialComponent |
| Amazon SageMaker AI         | Actividad de la API MLFlow de Amazon SageMaker AI.                                                                       | MLflow de Sagemaker                                              | AWS::SageMaker::MlflowTrackingServer     |
| AWS Signer                  | Actividad de la API de Signer sobre el trabajo de firma.                                                                 | Trabajo de firma de Signer                                       | AWS::Signer::SigningJob                  |
| AWS Signer                  | Actividad de la API de Signer sobre los trabajos de firma.                                                               | Perfil de firma del Signer                                       | AWS::Signer::SigningProfile              |
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en conjuntos de configuraciones.                         | Conjunto de configuración de SES                                 | AWS::SES::ConfigurationSet               |
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en identidades de correo electrónico.                    | Identidad de SES                                                 | AWS::SES::EmailIdentity                  |

| Servicio de AWS             | Descripción                                                                        | Tipo de recurso (consola)            | resources.type value             |
|-----------------------------|------------------------------------------------------------------------------------|--------------------------------------|----------------------------------|
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en plantillas.     | Plantilla de SES                     | AWS::SES::Template               |
| Amazon SimpleDB             | Actividad de la API de Amazon SimpleDB en los dominios.                            | Dominio de SimpleDB                  | AWS::SDB::Domain                 |
| AWS Step Functions          | <a href="#">Actividad de la API de Step Functions</a> en las actividades.          | Step Functions                       | AWS::StepFunctions::Activity     |
| AWS Step Functions          | <a href="#">Actividad de la API de Step Functions</a> en una máquina de estado.    | Máquina de estado de Step Functions  | AWS::StepFunctions::StateMachine |
| AWS Systems Manager         | <a href="#">Actividad de la API de Systems Manager</a> en los canales de control.  | Systems Manager                      | AWS::SSMMessages::ControlChannel |
| AWS Systems Manager         | Actividad de la API de Systems Manager sobre las evaluaciones de impacto.          | Evaluación de impacto de SSM         | AWS::SSM::ExecutionPreview       |
| AWS Systems Manager         | <a href="#">Actividad de la API de Systems Manager</a> en los nodos administrados. | Nodo administrado de Systems Manager | AWS::SSM::ManagedNode            |

| Servicio de AWS                     | Descripción                                                                                    | Tipo de recurso (consola)                | resources.type value                  |
|-------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------------|
| Amazon Timestream                   | Actividad de la API <a href="#">Query</a> de Amazon Timestream en las bases de datos.          | Base de datos de Timestream              | AWS::Timestream::Database             |
| Amazon Timestream                   | Actividad de la API de Amazon Timestream en los puntos de conexión regionales.                 | Punto de conexión regional de Timestream | AWS::Timestream::RegionalEndpoint     |
| Amazon Timestream                   | Actividad de la API <a href="#">Query</a> 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 |
| Cliente ligero de Amazon WorkSpaces | Actividad de la API de cliente ligero de WorkSpaces en un dispositivo.                         | Dispositivo de cliente ligero            | AWS::ThinClient::Device               |
| Cliente ligero de Amazon WorkSpaces | Actividad de la API de cliente ligero de WorkSpaces en un entorno.                             | Entorno de cliente ligero                | AWS::ThinClient::Environment          |
| AWS X-Ray                           | <a href="#">Actividad de la API de X-Ray</a> en los <a href="#">registros de seguimiento</a> . | Registros de seguimiento de X-Ray        | 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 eventos de datos de CloudTrail, debe agregar explícitamente cada tipo de recurso cuya actividad desee recopilar. Para obtener más información sobre el registro de eventos de datos, consulte [Registro de eventos de datos](#).

Se aplican cargos adicionales para registrar eventos de datos. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## Eventos de actividad de la red

Los eventos de actividad de la red de CloudTrail permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Los eventos de actividad de la red muestran información sobre las operaciones de recursos realizadas dentro de una VPC.

Puede registrar los eventos de actividad de la red para los siguientes servicios:

- AWS AppConfig
- AWS App Mesh
- Amazon Athena
- Intercambio de datos de AWS B2B
- AWS Backup gateway
- Amazon Bedrock
- Administración de facturación y costos
- Calculadora de precios de AWS
- AWS Cost Explorer
- API de control de nube de AWS
- AWS CloudHSM
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Señales de aplicación de CloudWatch



- AWS CodeDeploy
- Amazon Comprehend Medical
- AWS Config
- Exportaciones de datos de AWS
- Amazon Data Firehose
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon EventBridge
- Programador de Amazon EventBridge
- Amazon Fraud Detector
- capa gratuita de AWS
- Amazon FSx
- AWS Glue
- AWS HealthLake
- AWS IoT FleetWise
- AWS IoT Secure Tunneling
- Facturación de AWS
- Amazon Keyspaces (for Apache Cassandra)
- AWS KMS
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision

- Amazon Personalize
- Amazon Q Business
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon S3

 Note

Amazon S3 no admite [puntos de acceso de varias regiones](#).

- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Storage Gateway
- Administrador de incidentes de AWS Systems Manager
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS Transform
- Amazon Verified Permissions
- Amazon WorkMail

El registro de los eventos de actividad de la red está deshabilitado de forma predeterminada cuando crea un registro de seguimiento o un almacén de datos de eventos. A fin de registrar eventos de actividad de la red de CloudTrail, debe establecer explícitamente el origen de los eventos cuya actividad desea recopilar. Para obtener más información, consulte [Registro de eventos de actividad de la red](#).

Se aplican cargos adicionales por el registro de eventos de actividad de la red. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## Eventos de Insights

Los eventos de CloudTrail Insights capturan una tasa de llamadas inusuales de API o una actividad de tasa de error en su cuenta de AWS mediante el análisis de la actividad de administración de CloudTrail. 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 capturados en un registro de seguimiento o un almacén de datos de eventos de CloudTrail, los eventos de Insights solo se registran cuando CloudTrail detecta cambios en el registro de la tasa de error o de uso de la API de su cuenta que difieren considerablemente de los patrones de uso típicos de la cuenta. Para obtener más información, consulte [Trabajar con CloudTrail Insights](#).

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 eventos de Insights de CloudTrail, debe habilitar explícitamente los eventos de Insights en un registro de seguimiento o almacén de datos de eventos nuevo o existente. Para obtener más información acerca de la creación de un registro de seguimiento, consulte [Creación de un registro](#)

[de seguimiento con la consola de CloudTrail](#). Para obtener más información acerca de la creación de un almacén de datos de eventos, consulte [Creación de un almacén de datos de eventos para los eventos de Insights con la consola](#).

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](#).

## Historial de eventos

El historial de eventos de CloudTrail proporciona un registro visible e inmutable, que se puede buscar y descargar, de los últimos 90 días de eventos de administración de CloudTrail en una Región de AWS. Puede utilizar este historial para obtener información sobre las acciones llevadas a cabo en su cuenta de AWS en la Consola de administración de AWS, los SDK de AWS, las herramientas de línea de comando y otros servicios de AWS. Puede personalizar la vista del historial de eventos en la consola de CloudTrail al seleccionar las columnas que desea mostrar. Para obtener más información, consulte [Trabajar con el historial de eventos de CloudTrail](#).

## Registros de seguimiento

Un registro de seguimiento es una configuración que permite la entrega de eventos de CloudTrail a un bucket de S3, con envío opcional a [Registros de CloudWatch](#) y [Amazon EventBridge](#). Puede utilizar un registro de seguimiento para elegir los eventos de CloudTrail que desea enviar, cifrar sus archivos de registros de eventos de CloudTrail con una clave de AWS KMS y configurar las notificaciones de Amazon SNS para el envío del archivo de registros. 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](#).

## Registros de seguimiento multirregión y de una sola región

Puede crear registros de seguimiento multirregión y de una sola región para su Cuenta de AWS.

### registros de seguimiento multirregión

Cuando crea un registro de seguimiento de varias regiones, CloudTrail registra los eventos de todas las Regiones de AWS que están [habilitadas](#) en la Cuenta de AWS y envía los archivos de registro de eventos de CloudTrail al bucket de S3 que se especifique. Como práctica recomendada, le recomendamos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas. Todos los registros de seguimiento que

se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones. Puede convertir un registro de seguimiento de una sola región en uno de varias regiones mediante la AWS CLI. Para obtener más información, consulte [Cómo entender los registros de seguimiento de varias regiones y las regiones optativas](#), [Creación de un registro de seguimiento con la consola](#) y [Conversión de un registro de seguimiento de una sola región en un registro de seguimiento de varias regiones](#).

## registros de seguimiento de una sola región

Cuando crea un registro de seguimiento de una sola región, CloudTrail solo registra los eventos de esa región. A continuación, entrega los archivos de registros de eventos de CloudTrail al bucket de Amazon S3 que especifique. Solo puede crear un registro de seguimiento de una sola región mediante la AWS CLI. Si crea registros de seguimiento individuales adicionales, puede disponer que dichos registros de seguimiento envíen los archivos de registro de eventos de CloudTrail al mismo bucket de S3 o a buckets separados. Esta es la opción predeterminada al crear un registro de seguimiento mediante la AWS CLI o la API de CloudTrail. Para obtener más información, consulte [Creación, actualización y administración de registros de seguimiento con la AWS CLI](#).

### Note

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

Los registros de seguimiento multirregión tienen las siguientes ventajas:

- Los valores de configuración del registro de seguimiento se aplican de forma sistemática a todas las Regiones de AWS [habilitadas](#).
- Recibirá eventos de CloudTrail desde todas las Regiones de AWS habilitadas en un único bucket de Amazon S3 y, de manera opcional, en un grupo de registro de Registros de CloudWatch.
- Las configuraciones del registro de seguimiento para todas las Regiones de AWS habilitadas se administran desde una sola ubicación.

Crear un registro de seguimiento de varias regiones tiene los siguientes efectos:

- CloudTrail envía los archivos de registros sobre la actividad de la cuenta desde todas las Regiones de AWS [habilitadas](#) al bucket de Amazon S3 que se especifique y, de manera opcional, a un grupo de registro de registros de CloudWatch.
- Si ha configurado un tema de Amazon SNS para el registro de seguimiento, las notificaciones de SNS sobre los envíos de archivos de registros de todas las Regiones de AWS habilitadas se envían a este tema de SNS de forma exclusiva.
- Puede ver el registro de seguimiento de varias regiones en todas las Regiones de AWS habilitadas, pero solo puede modificar el registro de seguimiento en la región de origen en la que se creó.

Independientemente de si un registro de seguimiento consta de varias regiones o de una sola región, los eventos enviados a Amazon EventBridge se reciben en el [bus de eventos](#) de cada región, en lugar de en un solo 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 registros de seguimiento por región. Un registro de seguimiento multirregión cuenta como un registro de seguimiento por región.

Este es un ejemplo de 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 multirregión más en la región Oeste de EE. UU. (Norte de California).
- Crea otro registro de seguimiento multirregión en la región Asia-Pacífico (Sídney). Este registro de seguimiento también existe como un registro de seguimiento en la región EE. UU. Oeste (Norte de California).

Puede ver una lista de los registros de seguimiento de una Región de AWS en la página Registros de seguimiento de la consola de CloudTrail. Para obtener más información, consulte [Actualización de un registro de seguimiento con la consola de CloudTrail](#). Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## Registros de seguimiento de la organización

Un registro de seguimiento de organización es una configuración que permite el envío de eventos de CloudTrail en la cuenta de administración y en todas las cuentas miembro de una organización de AWS Organizations en el mismo bucket de Amazon S3, Registros de CloudWatch y 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 de seguimiento de la organización creados con la consola son registros de seguimiento multirregión que registran los eventos de las Regiones de AWS [habilitadas](#) en cada cuenta de miembro de la organización. Para registrar eventos en todas las particiones de AWS de su organización, cree un registro de seguimiento multirregión en cada partición. Puede crear un registro de seguimiento de la organización de una sola región o de varias regiones mediante la AWS CLI. Si crea un registro de seguimiento de una sola región, solo registrará la actividad en la Región de AWS del registro de seguimiento (también denominada región de origen).

Aunque la mayoría de Regiones de AWS están habilitadas por defecto en su Cuenta de AWS, debe habilitar manualmente determinadas regiones (también denominadas regiones optativas). Para obtener información sobre qué regiones están habilitadas por defecto, consulte [Considerations before enabling and disabling Regions](#) en la Guía de referencia de AWS Account Management. Para ver la lista de las regiones que admite CloudTrail, consulte [Regiones compatibles con CloudTrail](#).

Al crear un registro de seguimiento de la organización, se creará una copia con el nombre que le asigne en las cuentas de miembros que pertenezcan a su organización.

- Si el registro de seguimiento de la organización corresponde a una sola región y su región de origen no es una región optativa, se crea una copia en la región de origen del registro de seguimiento de la organización en cada cuenta de miembro.
- Si el registro de seguimiento de la organización corresponde a una sola región y su región de origen es una región optativa, se crea una copia en la región de origen del registro de seguimiento de la organización en las cuentas de miembros que tengan activada esa región.
- Si el registro de seguimiento de la organización es multirregión y su región de origen no es una región optativa, se crea una copia en cada Región de AWS habilitada en cada cuenta de miembro. Cuando una cuenta de miembro habilita una región optativa, tras la activación de dicha región se crea una copia del registro de seguimiento multirregión en la nueva región optativa habilitada.
- Si el registro de seguimiento de la organización es multirregión y la región de origen es una región optativa, las cuentas de miembros no enviarán la actividad al registro de seguimiento de la

organización a menos que habiliten la Región de AWS en la que se creó el registro de seguimiento de varias regiones. Por ejemplo, si crea un registro de seguimiento multirregión y elige la región de Europa (España) como región de origen dicho registro, solo las cuentas de miembros que hayan habilitado la región de Europa (España) en su cuenta enviarán su actividad al registro de seguimiento de la organización.

 Note

CloudTrail crea registros de seguimiento de la organización en las cuentas de miembros aunque falle la validación de un recurso. Ejemplos de errores de validación:

- Una política de buckets de Amazon S3 incorrecta
- Una política de temas de Amazon SNS incorrecta
- Incapacidad de realizar envíos a un grupo de registro de Registros de CloudWatch
- Permisos insuficientes para cifrar mediante una clave de KMS

Las cuentas de miembros con permisos de CloudTrail pueden ver cualquier error de validación de un registro de seguimiento de la organización consultando la página de detalles del registro en la consola de CloudTrail o ejecutando el comando [get-trail-status](#) de la AWS CLI.

Los usuarios con permisos de CloudTrail en las cuentas de miembros podrán ver el registro de seguimiento de la organización (incluido el ARN de registro de seguimiento) cuando inicien sesión en la consola de CloudTrail desde sus cuentas de AWS, o cuando ejecuten comandos de la AWS CLI, como `describe-trails` (aunque las cuentas de miembros deben utilizar el ARN del registro de seguimiento de la organización, y no el nombre, cuando utilicen la AWS CLI). Sin embargo, los usuarios de las cuentas de miembros no tendrán permisos suficientes para eliminar el registro de seguimiento de la organización, activar o desactivar el registro, cambiar los tipos de eventos registrados o alterar el registro de seguimiento 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](#).



## CloudTrail Lake y los almacenes de datos de eventos

CloudTrail Lake le permite ejecutar consultas precisas basadas en SQL sobre sus eventos y registrar eventos de orígenes externos a AWS, incluidas sus propias aplicaciones, y de socios que están integrados con CloudTrail. No necesita tener registros de seguimiento configurados en su cuenta para utilizar CloudTrail Lake.

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. 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 puede guardar los resultados de las consultas en un bucket de S3. CloudTrail Lake también puede almacenar eventos de una organización en AWS Organizations en un almacén de datos de eventos, o eventos de múltiples regiones y cuentas. 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 [Trabajar con AWS CloudTrail Lake](#) y [Conceptos y terminología de CloudTrail Lake](#).

## CloudTrail Insights

CloudTrail Insights ayuda a los usuarios de AWS a identificar y responder a volúmenes inusuales de llamadas a la API o errores registrados en llamadas a la API mediante el análisis continuo de eventos de administración de CloudTrail. 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 de seguimiento y los almacenes de datos de eventos no registran 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 utiliza la API de CloudTrail, puede registrar eventos de Insights al editar la configuración de un registro de seguimiento o almacén de datos de eventos existentes con la API [PutInsightSelectors](#). Se aplican cargos adicionales por registrar eventos de CloudTrail 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 [Trabajar con CloudTrail Insights](#) y [Precios de AWS CloudTrail](#).

## Etiquetas

Una etiqueta es una clave y un valor opcional definidos por el usuario que se pueden asignar a recursos de AWS, como los registros de seguimiento de CloudTrail, los almacenes de datos de eventos y canales, los buckets de S3 que se utilizan para almacenar los archivos de registro de CloudTrail, las organizaciones y las unidades organizativas de AWS Organizations y muchos más. Si agrega las mismas etiquetas a los registros de seguimiento y a los buckets de S3 que utiliza para almacenar los archivos de registro de los registros de seguimiento, puede hacer que sea más sencillo administrar, buscar y filtrar estos recursos con [Grupos de recursos de AWS](#). 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 [Prácticas recomendadas para el etiquetado de recursos de AWS](#).

## AWS Security Token Service y CloudTrail

AWS Security Token Service (AWS STS) es un servicio que tiene un punto de conexión global y que también admite puntos de conexión específicos para cada 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 de conexión específico para una región de AWS STS, el registro de seguimiento de esa región solo envía los eventos de AWS STS que se produzcan en esa región. Por ejemplo, si utiliza el punto de enlace `sts.us-west-2.amazonaws.com`, el registro de seguimiento en us-west-2 envía solamente los eventos de AWS STS que se originan en us-west-2. Para obtener más información sobre los puntos de enlace regionales de AWS STS, consulte [Activación y desactivación de AWS STS en una región de AWS](#) en la Guía del usuario de IAM.

Para obtener una lista completa de los puntos de enlace regionales de AWS, consulte [Regiones y puntos de enlace de AWS](#) 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, AWS CloudTrail cambió la forma en que los registros de seguimiento capturan eventos de servicios globales. Tras el cambio, los eventos creados

por Amazon CloudFront, AWS Identity and Access Management y AWS STS se registrarán en la región en la que se crearon, la región Este de EE. UU. (Norte de Virginia), us-east-1. Esto hace que el tratamiento de CloudTrail de estos servicios sea coherente con el de otros servicios globales de AWS. 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 consola de CloudTrail y el comando `aws cloudtrail lookup-events` mostrarán estos eventos en la Región de AWS en que se produjeron.

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), AWS STS y Amazon CloudFront, los eventos se envían a cualquier registro de seguimiento que incluya servicios globales.

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:

- De forma predeterminada, los eventos de servicios globales se envían a registros de seguimiento creados mediante la consola de CloudTrail. 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 de varias regiones a un registro de seguimiento de una sola región, el registro de eventos de servicios globales se desactiva de manera automática para dicho registro de seguimiento. De la misma manera, si cambia la configuración de un registro de seguimiento de una sola región a un registro de seguimiento de

varias regiones, el registro de eventos de servicios globales se activa de manera automática 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. Crea un registro de seguimiento en la consola de CloudTrail. 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 administración de registros de seguimiento con la AWS CLI](#).

 Note

Cuando crea o actualiza un registro de seguimiento con la AWS CLI, los SDK de AWS o la API de CloudTrail puede determinar si desea incluir o excluir eventos de servicios globales para los registros de seguimiento. No puede configurar el registro de eventos de servicios globales en la consola de CloudTrail.

## Regiones compatibles con CloudTrail

 Note

Para obtener información sobre las regiones compatibles con CloudTrail Lake, consulte [Regiones en las que se admite CloudTrail Lake](#).

Para obtener información sobre los puntos de conexión del plano de datos, consulte [Data plane endpoints](#) en la Referencia general de AWS.

| Nombre de la región                       | Región         | Punto de conexión del plano de control  | Protocolo | Fecha de compatibilidad |
|-------------------------------------------|----------------|-----------------------------------------|-----------|-------------------------|
| Este de EE. UU.<br>(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.<br>(Norte de California) | us-west-1      | cloudtrail.us-west-1.amazonaws.com      | HTTPS     | 13/5/2014               |
| EE. UU. Oeste<br>(Oregon)                 | us-west-2      | cloudtrail.us-west-2.amazonaws.com      | HTTPS     | 13/11/2013              |
| África<br>(Ciudad del Cabo)               | af-south-1     | cloudtrail.af-south-1.amazonaws.com     | HTTPS     | 22/04/2020              |
| Asia Pacífico<br>(Hong Kong)              | ap-east-1      | cloudtrail.ap-east-1.amazonaws.com      | HTTPS     | 24/02/2019              |
| Asia-Pacífico<br>(Hyderabad)              | ap-south-2     | cloudtrail.ap-south-2.amazonaws.com     | HTTPS     | 22/11/2022              |
| Asia-Pacífico<br>(Yakarta)                | ap-southeast-3 | cloudtrail.ap-southeast-3.amazonaws.com | HTTPS     | 13/12/2021              |

| Nombre de la región       | Región         | Punto de conexión del plano de control  | Protocolo | Fecha de compatibilidad |
|---------------------------|----------------|-----------------------------------------|-----------|-------------------------|
| Asia-Pacífico (Malasia)   | ap-southeast-5 | cloudtrail.ap-southeast-5.amazonaws.com | HTTPS     | 08/22/2024              |
| Asia-Pacífico (Melbourne) | ap-southeast-4 | cloudtrail.ap-southeast-4.amazonaws.com | HTTPS     | 01/23/2023              |
| Asia-Pacífico (Bombay)    | ap-south-1     | cloudtrail.ap-south-1.amazonaws.com     | HTTPS     | 27/6/2016               |
| Asia Pacífico (Osaka)     | ap-northeast-3 | cloudtrail.ap-northeast-3.amazonaws.com | HTTPS     | 12/02/2018              |
| Asia Pacífico (Seúl)      | ap-northeast-2 | cloudtrail.ap-northeast-2.amazonaws.com | HTTPS     | 6/1/2016                |
| 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 (Tailandia) | ap-southeast-7 | cloudtrail.ap-southeast-7.amazonaws.com | HTTPS     | 01/07/2025              |
| Asia-Pacífico (Tokio)     | ap-northeast-1 | cloudtrail.ap-northeast-1.amazonaws.com | HTTPS     | 30/06/2014              |

| Nombre de la región       | Región         | Punto de conexión del plano de control     | Protocolo | Fecha de compatibilidad |
|---------------------------|----------------|--------------------------------------------|-----------|-------------------------|
| Canadá (centro)           | 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              |
| China (Pekín)             | 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 (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 (Milán)            | eu-south-1     | cloudtrail.eu-south-1.amazonaws.com        | HTTPS     | 27/04/2020              |
| Europa (París)            | eu-west-3      | cloudtrail.eu-west-3.amazonaws.com         | HTTPS     | 18/12/2017              |
| Europa (España)           | eu-south-2     | cloudtrail.eu-south-2.amazonaws.com        | HTTPS     | 11/16/2022              |
| Europa (Estocolmo)        | eu-north-1     | cloudtrail.eu-north-1.amazonaws.com        | HTTPS     | 11/12/2018              |

| Nombre de la región            | Región        | Punto de conexión del plano de control | Protocolo | Fecha de compatibilidad |
|--------------------------------|---------------|----------------------------------------|-----------|-------------------------|
| Europa (Zúrich)                | eu-central-2  | cloudtrail.eu-central-2.amazonaws.com  | HTTPS     | 09/11/2022              |
| Israel (Tel Aviv)              | il-central-1  | cloudtrail.il-central-1.amazonaws.com  | HTTPS     | 31/07/2023              |
| México (central)               | mx-central-1  | cloudtrail.mx-central-1.amazonaws.com  | HTTPS     | 13/01/2025              |
| Medio Oriente (Baréin)         | me-south-1    | cloudtrail.me-south-1.amazonaws.com    | HTTPS     | 29/07/2019              |
| Medio Oriente (EAU)            | me-central-1  | cloudtrail.me-central-1.amazonaws.com  | HTTPS     | 08/30/2022              |
| América del Sur (São Paulo)    | sa-east-1     | cloudtrail.sa-east-1.amazonaws.com     | HTTPS     | 30/06/2014              |
| 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              |

Para obtener más información sobre el uso de CloudTrail en las AWS GovCloud (US) Regions, consulte [Service Endpoints](#) en la Guía del usuario de AWS GovCloud (US).



Para obtener más información sobre cómo utilizar CloudTrail en la región de China (Pekín), consulte [Endpoints and ARNs for AWS in China](#) en la Referencia general de Amazon Web Services.

## Integraciones y servicios admitidos de CloudTrail

CloudTrail admite eventos de registro de muchos Servicios de AWS. Encontrará información sobre los aspectos específicos de cada servicio compatible en la guía de dicho servicio. Para obtener una lista de temas específicos de los servicios, consulte [AWSTemas de servicio de para CloudTrail](#). Además, algunos Servicios de AWS se pueden utilizar para analizar los datos recopilados en los registros de CloudTrail y actuar en consecuencia.

### 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

- [Integraciones de servicios de AWS con registros de CloudTrail](#)
- [Integración de CloudTrail con Amazon EventBridge](#)
- [Integración de CloudTrail con AWS Organizations](#)
- [Integración de CloudTrail con AWS Control Tower](#)
- [Integración de CloudTrail con Amazon Security Lake](#)
- [Integración de CloudTrail Lake con Amazon Athena](#)
- [Integración de CloudTrail Lake con AWS Config](#)
- [Integración de CloudTrail Lake con AWS Audit Manager](#)
- [AWSTemas de servicio de para CloudTrail](#)
- [Servicios CloudTrail no compatibles](#)

## Integraciones de servicios de AWS con registros de CloudTrail

### Note

También puede usar CloudTrail Lake para consultar y analizar sus eventos. Las consultas de CloudTrail Lake ofrecen una visión más detallada y personalizable de los eventos que

las simples búsquedas de claves y valores en el Event history (Historial de eventos), o ejecutando `LookupEvents`. Los usuarios de CloudTrail Lake pueden ejecutar consultas complejas en Lenguaje de consulta estándar (SQL) en múltiples campos de un evento de CloudTrail. Para obtener más información, consulte [Trabajar con AWS CloudTrail Lake](#) y [Copia de eventos de registro de seguimiento en CloudTrail Lake](#).

Los almacenes de datos de eventos de CloudTrail Lake y las consultas conllevan cargos de CloudTrail. Para obtener más información sobre los precios de CloudTrail Lake, consulte [Precios de AWS CloudTrail](#).

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

| AWSServicio de | Tema                                                    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Athena  | <a href="#">Consulta de registros de AWS CloudTrail</a> | <p>La utilización de Athena con los registros de CloudTrail es un modo eficaz de mejorar el análisis de la actividad de un servicio de AWS. Por ejemplo, puede utilizar consultas para identificar tendencias y aislar la actividad por atributo, como el usuario o la dirección IP de fuente.</p> <p>Puede crear tablas de forma automática para consultar los registros directamente en la consola de CloudTrail y utilizar esas tablas para ejecutar consultas en Athena. Para obtener más información, consulte <a href="#">Creación de una tabla para CloudTrail Logs en la consola de CloudTrail</a> en la</p> |

| AWSServicio de | Tema | Descripción                                                                                                                                                                                                                                                                                                                              |
|----------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |      | <p><a href="#">Guía del usuario de Amazon Athena.</a></p> <div><p> <b>Note</b></p><p>La ejecución de consultas en Amazon Athena genera costos adicionales. Para obtener más información, consulte <a href="#">Precios de Amazon Athena.</a></p></div> |

| AWSServicio de         | Tema                                                                                        | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon CloudWatch Logs | <a href="#">Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs</a> | <p>Puede configurar CloudTrail con CloudWatch Logs para monitorear los registros de seguimiento y recibir notificaciones cuando se produzca una actividad específica. Por ejemplo, puede definir filtros de métricas de CloudWatch Logs que desencadenarán alarmas de CloudWatch y enviarán notificaciones cuando se desencadenen dichas alarmas.</p> <div> <b>Note</b><p>Se aplican los precios estándar de Amazon CloudWatch y Amazon CloudWatch Logs. Para obtener más información, consulte <a href="#">Precios de Amazon CloudWatch</a>.</p></div> |

## Integración de CloudTrail con Amazon EventBridge

Amazon EventBridge es un servicio de AWS que proporciona un flujo de eventos de sistema casi en tiempo real que describen cambios en los recursos de AWS. En EventBridge, puede crear reglas que respondan a eventos registrados por CloudTrail. Para obtener más información, consulte [Crear una regla en Amazon EventBridge](#).

Puede enviar eventos a los que se ha suscrito a su registro de seguimiento de EventBridge si crea una regla a través de la consola de EventBridge.

En la consola de EventBridge:

- Elija el detail-type `AWS API Call via CloudTrail` para enviar los datos y eventos de administración de CloudTrail con un eventType de `AwsApiCall`. Para registrar eventos con un valor de detail-type `AWS API Call via CloudTrail`, debe tener un registro de seguimiento que esté registrando actualmente los eventos de administración o de datos.
- Elija el detail-type `AWS Console Sign In via CloudTrail` para enviar [eventos de inicio de sesión de la Consola de administración de AWS](#). Para registrar eventos con un detail-type de `AWS Console Sign In via CloudTrail`, debe tener un registro de seguimiento que esté registrando actualmente los eventos de administración.
- Elija el detail-type `AWS Insight via CloudTrail` para enviar eventos de Insights. Para registrar eventos con un valor de detail-type `AWS Insight via CloudTrail`, debe tener un registro de seguimiento que esté registrando actualmente los eventos de Insights. Para obtener información sobre cómo registrar eventos de Insights, consulte [Trabajar con CloudTrail Insights](#).

Para obtener más información sobre cómo crear y administrar un registro de seguimiento, consulte [Creación de un registro de seguimiento con la consola de CloudTrail](#).

## Integración de CloudTrail con AWS Organizations

La cuenta de administración de una organización de AWS Organizations puede agregar un [administrador delegado](#) para que administre los recursos de CloudTrail 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 la organización](#) o un [almacén de datos de eventos de la organización](#) lo ayuda a definir una estrategia uniforme de registro de eventos para su organización.

## Integración de CloudTrail con AWS Control Tower

AWS Control Tower configura un nuevo registro de seguimiento de la organización de CloudTrail que registra los eventos de administración al configurar una zona de aterrizaje. Cuando se inscribe una cuenta en AWS Control Tower, esta se rige por el registro de seguimiento de la organización para la AWS Control Tower de la organización. Si ya dispone de un registro de seguimiento de la organización en esa cuenta, es posible que vea cargos duplicados, a menos que elimine el registro de seguimiento existente de la cuenta antes de inscribirla en AWS Control Tower. Puede ver la

página Registro de seguimiento en la consola de CloudTrail para saber si se creó algún registro de seguimiento de la organización. Para obtener más información sobre AWS Control Tower, consulte [Acerca del inicio de sesión de AWS Control Tower](#) en la Guía del usuario de AWS CloudTrail.

## Integración de CloudTrail con Amazon Security Lake

Security Lake puede recopilar registros asociados a los eventos de administración de CloudTrail y a los eventos de datos de CloudTrail para S3 y Lambda. Para obtener más información, consulte los [Registros de eventos de CloudTrail](#) en la Guía del usuario de Amazon Security Lake.

Para recopilar los eventos de administración de CloudTrail en Security Lake, debe tener al menos un registro de organización multirregional de CloudTrail que recopile los eventos de administración de CloudTrail de lectura y escritura.

## Integración de CloudTrail Lake con Amazon Athena

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 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](#).

## Integración de CloudTrail Lake con 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. Para obtener más información, consulte [Creación de un almacén de datos de eventos para los elementos de configuración con la consola](#).

## Integración de CloudTrail Lake con AWS Audit Manager

Puede crear un almacén de datos de eventos para evidencia de AWS Audit Manager mediante la consola de Audit Manager. Para obtener más información sobre cómo agregar evidencia en CloudTrail Lake con Audit Manager, consulte [Cómo funciona el buscador de evidencia con CloudTrail Lake](#) en la Guía del usuario de AWS Audit Manager.

## AWSTemas de servicio de para CloudTrail

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

### 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](#).

| AWSServicio de       | Temas de CloudTrail                                                                                           | Solución compatible desde |
|----------------------|---------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon API Gateway   | <a href="#">Registrar llamadas de administración a la API para Amazon API Gateway mediante AWS CloudTrail</a> | 09/07/2015                |
| Amazon AppFlow       | <a href="#">Registro de llamadas de la API de Amazon AppFlow con AWS CloudTrail</a>                           | 22/04/2020                |
| Amazon AppStream 2.0 | <a href="#">Registro de llamadas a la API de Amazon AppStream 2.0 con AWS CloudTrail</a>                      | 25/04/2019                |
| Amazon Athena        | <a href="#">Registro de llamadas a la API de Amazon Athena con AWS CloudTrail</a>                             | 19/05/2017                |

| AWSServicio de         | Temas de CloudTrail                                                                                              | Solución compatible desde |
|------------------------|------------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon Aurora          | <a href="#">Supervisión de llamadas a la API de Amazon Aurora en AWS CloudTrail</a>                              | 31/08/2018                |
| Amazon Bedrock         | <a href="#">Registro de llamadas a la API de Amazon Bedrock mediante AWS CloudTrail</a>                          | 23/10/2023                |
| Amazon Braket          | <a href="#">Registro de llamadas a la API de Amazon Braket con CloudTrail</a>                                    | 08/12/2020                |
| Amazon Chime           | <a href="#">Registrar llamadas de administración de Amazon Chime mediante AWS CloudTrail</a>                     | 27/09/2017                |
| Amazon Cloud Directory | <a href="#">Registro de llamadas a la API de Cloud Directory mediante AWS CloudTrail</a>                         | 26/01/2017                |
| Amazon CloudFront      | <a href="#">Uso de AWS CloudTrail para capturar solicitudes enviadas a la API de CloudFront</a>                  | 28/05/2014                |
| Amazon CloudSearch     | <a href="#">Registro de llamadas del servicio de configuración de Amazon CloudSearch mediante AWS CloudTrail</a> | 16/10/2014                |
| Amazon CloudWatch      | <a href="#">Registro de llamadas a la API de Amazon CloudWatch en AWS CloudTrail</a>                             | 30/04/2014                |
| Amazon CloudWatch Logs | <a href="#">Registro de llamadas a la API de Amazon CloudWatch Logs en AWS CloudTrail</a>                        | 10/03/2016                |



| AWSServicio de                                | Temas de CloudTrail                                                                                                | Solución compatible desde |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon CodeCatalyst                           | <a href="#">Registro de llamadas a la API de CodeCatalyst en Cuentas de AWS conectadas mediante AWS CloudTrail</a> | 12/01/2022                |
| Revisor de Amazon CodeGuru                    | <a href="#">Registro de llamadas a la API de Amazon CodeGuru Reviewer con AWS CloudTrail</a>                       | 02/12/2019                |
| Amazon Cognito                                | <a href="#">Registro de llamadas a la API de Amazon Cognito con AWS CloudTrail</a>                                 | 18/02/2016                |
| Amazon Comprehend                             | <a href="#">Registro de llamadas a la API de Amazon Comprehend con AWS CloudTrail</a>                              | 17/01/2018                |
| Amazon Comprehend Medical                     | <a href="#">Registro de llamadas a la API de Amazon Comprehend Medical mediante AWS CloudTrail</a>                 | 27/11/2018                |
| Amazon Connect                                | <a href="#">Registro de llamadas a la API de Amazon Connect con AWS CloudTrail</a>                                 | 11/12/2019                |
| Amazon Data Firehose                          | <a href="#">Monitoreo de llamadas a la API de Amazon Data Firehose con AWS CloudTrail</a>                          | 17/03/2016                |
| Administrador de vida útil de datos de Amazon | <a href="#">Registro de llamadas a la API de Amazon Data Lifecycle Manager mediante AWS CloudTrail</a>             | 24/07/2018                |

| AWSServicio de                                     | Temas de CloudTrail                                                                      | Solución compatible desde |
|----------------------------------------------------|------------------------------------------------------------------------------------------|---------------------------|
| Amazon Detective                                   | <a href="#">Registro de llamadas a la API de Amazon Detective con AWS CloudTrail</a>     | 03/31/2020                |
| Amazon DevOps Guru                                 | <a href="#">Registro de llamadas a la API de Amazon DevOps Guru con AWS CloudTrail</a>   | 05/04/2021                |
| Amazon DocumentDB (con compatibilidad con MongoDB) | <a href="#">Registro de llamadas a la API de Amazon DocumentDB con AWS CloudTrail</a>    | 01/09/2019                |
| Amazon DynamoDB                                    | <a href="#">Registro de operaciones de DynamoDB mediante AWS CloudTrail</a>              | 28/05/2015                |
| Amazon EC2                                         | <a href="#">Registro de llamadas a la API de Amazon EC2 mediante AWS CloudTrail</a>      | 13/11/2013                |
| Amazon EC2 Auto Scaling                            | <a href="#">Registro de llamadas a la API de Auto Scaling mediante CloudTrail</a>        | 16/07/2014                |
| Bloques de capacidad de Amazon EC2                 | <a href="#">Registro de llamadas a la API de bloques de capacidad con AWS CloudTrail</a> | 31/10/2023                |
| Amazon EC2 Image Builder                           | <a href="#">Registro de llamadas a la API de EC2 Image Builder mediante CloudTrail</a>   | 02/12/2019                |

| AWSServicio de                                 | Temas de CloudTrail                                                                           | Solución compatible desde       |
|------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------|
| Amazon Elastic Block Store (Amazon EBS)        | <a href="#">Registro de llamadas a la API mediante AWS CloudTrail</a>                         | Amazon EBS: 13/11/2013          |
| API directas de EBS                            | <a href="#">Registro de llamadas a la API de las API directas de EBS con AWS CloudTrail</a>   | API directas de EBS: 30/06/2020 |
| Amazon Elastic Container Registry (Amazon ECR) | <a href="#">Registro de llamadas a la API de Amazon ECR mediante AWS CloudTrail</a>           | 21/12/2015                      |
| Amazon Elastic Container Service (Amazon ECS)  | <a href="#">Registro de llamadas a la API de Amazon ECS mediante AWS CloudTrail</a>           | 09/04/2015                      |
| Amazon Elastic File System (Amazon EFS)        | <a href="#">Registro de llamadas a la API de Amazon EFS con AWS CloudTrail</a>                | 28/06/2016                      |
| Amazon Elastic Kubernetes Service (Amazon EKS) | <a href="#">Registro de llamadas a la API de Amazon EKS con AWS CloudTrail</a>                | 05/06/2018                      |
| Amazon Elastic Transcoder                      | <a href="#">Registro de llamadas a la API de Amazon Elastic Transcoder con AWS CloudTrail</a> | 27/10/2014                      |
| Amazon ElastiCache                             | <a href="#">Registro de llamadas a la API de Amazon ElastiCache mediante AWS CloudTrail</a>   | 15/09/2014                      |
| Amazon EMR                                     | <a href="#">Registro de llamadas a la API de Amazon EMR mediante AWS CloudTrail</a>           | 04/04/2014                      |

| AWSServicio de                                          | Temas de CloudTrail                                                                              | Solución compatible desde |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------|
| Amazon EMR en EKS                                       | <a href="#">Registro de llamadas a la API de Amazon EMR en EKS mediante AWS CloudTrail</a>       | 09/12/2020                |
| Amazon EventBridge                                      | <a href="#">Registro de llamadas a la API del Amazon EventBridge mediante AWS CloudTrail</a>     | 07/11/2019                |
| Amazon FinSpace                                         | <a href="#">Consulta de registros de AWS CloudTrail</a>                                          | 18/10/2022                |
| Amazon Forecast                                         | <a href="#">Registro de llamadas a la API de Amazon Forecast con AWS CloudTrail</a>              | 28/11/2018                |
| Amazon Fraud Detector                                   | <a href="#">Registro de llamadas a la API de Amazon Fraud Detector con AWS CloudTrail</a>        | 01/09/2020                |
| Amazon FSx for Lustre                                   | <a href="#">Registro de llamadas a la API de Amazon FSx for Lustre con AWS CloudTrail</a>        | 11/01/2019                |
| Amazon FSx for Windows File Server                      | <a href="#">Monitorización con AWS CloudTrail</a>                                                | 28/11/2018                |
| Servidores de Amazon GameLift (Amazon GameLift Servers) | <a href="#">Registro de llamadas a la API de Amazon GameLift Servers con AWS CloudTrail</a>      | 27/01/2016                |
| Amazon GameLift Streams                                 | <a href="#">Registro de llamadas a la API de Amazon GameLift Streams mediante AWS CloudTrail</a> | 05/03/2025                |
| Amazon GuardDuty                                        | <a href="#">Registro de llamadas a la API de Amazon GuardDuty con AWS CloudTrail</a>             | 12/02/2018                |

| AWSServicio de                           | Temas de CloudTrail                                                                                                                                                                                    | Solución compatible desde |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon Inspector                         | <a href="#">Registro de llamadas a la API de Amazon Inspector con AWS CloudTrail</a>                                                                                                                   | 29/11/2021                |
| Amazon Inspector Classic                 | <a href="#">Registro de llamadas a la API de Amazon Inspector Classic con AWS CloudTrail</a>                                                                                                           | 20/04/2016                |
| Escaneo de Amazon Inspector              | <a href="#">Información de escaneo de Amazon Inspector en CloudTrail</a>                                                                                                                               | 27/11/2023                |
| Amazon Interactive Video Service         | <a href="#">Registro de llamadas a la API de Amazon IVS con AWS CloudTrail</a>                                                                                                                         | 15/07/2020                |
| Amazon Kendra                            | <a href="#">Registro de llamadas a la API de Amazon Kendra con AWS CloudTrail</a> y <a href="#">Registro de llamadas a la API de Amazon Kendra Intelligent Ranking con registros de AWS CloudTrail</a> | 11/05/2020                |
| Amazon Keyspaces (for Apache Cassandra)  | <a href="#">Registro de llamadas a la API de Amazon Keyspaces con AWS CloudTrail</a>                                                                                                                   | 13/01/2020                |
| Amazon Managed Service para Apache Flink | <a href="#">Registro de llamadas a la API de Managed Service para Apache Flink con AWS CloudTrail</a>                                                                                                  | 22/03/2019                |
| Amazon Kinesis Data Streams              | <a href="#">Registro de llamadas a la API de Amazon Kinesis Data Streams mediante AWS CloudTrail</a>                                                                                                   | 25/04/2014                |

| AWSServicio de               | Temas de CloudTrail                                                                        | Solución compatible desde |
|------------------------------|--------------------------------------------------------------------------------------------|---------------------------|
| Amazon Kinesis Video Streams | <a href="#">Registro de llamadas a la API de Kinesis Video Streams con AWS CloudTrail</a>  | 24/05/2018                |
| Amazon Lex                   | <a href="#">Registro de llamadas a la API de Amazon Lex con CloudTrail</a>                 | 15/08/2017                |
| Amazon Lightsail             | <a href="#">Registro de llamadas a la API de Lightsail con AWS CloudTrail</a>              | 23/12/2016                |
| Amazon Location Service      | <a href="#">Registro y monitoreo con AWS CloudTrail</a>                                    | 12/15/2020                |
| Amazon Lookout for Equipment | <a href="#">Monitoreo de Amazon Lookout for Equipment</a>                                  | 12/01/2020                |
| Amazon Lookout for Metrics   | <a href="#">Ver la actividad de la API de Amazon Lookout for Metrics en AWS CloudTrail</a> | 12/08/2020                |
| Amazon Lookout for Vision    | <a href="#">Registro de llamadas de Amazon Lookout for Vision con AWS CloudTrail</a>       | 12/01/2020                |
| Amazon Machine Learning      | <a href="#">Registro de llamadas a la API de Amazon ML mediante AWS CloudTrail</a>         | 10/12/2015                |
| Amazon Macie                 | <a href="#">Registro de llamadas a la API de Amazon Macie mediante AWS CloudTrail</a>      | 13/05/2020                |

| AWSServicio de                                       | Temas de CloudTrail                                                                                                                                                                                                                    | Solución compatible desde |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon Managed Blockchain                            | <a href="#">Registro de llamadas a la API de Amazon Managed Blockchain mediante AWS CloudTrail</a><br><br><a href="#">Registro de Ethereum para las llamadas a la API de Managed Blockchain mediante AWS CloudTrail (vista previa)</a> | 04/01/2019                |
| Amazon Managed Grafana                               | <a href="#">Registro de llamadas a la API de Amazon Managed Grafana mediante AWS CloudTrail</a>                                                                                                                                        | 12/15/2020                |
| Amazon Managed Service para Prometheus               | <a href="#">Registro de llamadas a la API de Amazon Managed Service for Prometheus mediante AWS CloudTrail</a>                                                                                                                         | 12/15/2020                |
| Transmisión administrada de Amazon para Apache Kafka | <a href="#">Registro de llamadas a la API con AWS CloudTrail</a>                                                                                                                                                                       | 11/12/2018                |
| Amazon Managed Workflows para Apache Airflow         | <a href="#">Visualización de registros de auditoría en AWS CloudTrail</a>                                                                                                                                                              | 11/24/2020                |
| Amazon MemoryDB                                      | <a href="#">Registro de llamadas a la API de Amazon MemoryDB con AWS CloudTrail</a>                                                                                                                                                    | 19/08/2021                |
| Amazon MQ                                            | <a href="#">Registro de llamadas a la API de Amazon MQ mediante AWS CloudTrail</a>                                                                                                                                                     | 19/07/2018                |
| Amazon Neptune                                       | <a href="#">Registro de llamadas a la API de Amazon Neptune mediante AWS CloudTrail</a>                                                                                                                                                | 30/05/2018                |

| AWSServicio de                               | Temas de CloudTrail                                                                                | Solución compatible desde |
|----------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------|
| Amazon One Enterprise                        | <a href="#">Registro de llamadas a la API de Amazon One Enterprise mediante AWS CloudTrail</a>     | 27/11/2023                |
| Amazon OpenSearch Service                    | <a href="#">Monitoreo de las llamadas a la API de Amazon OpenSearch Service con AWS CloudTrail</a> | 01/10/2015                |
| Amazon Personalize                           | <a href="#">Registro de llamadas a la API de Amazon Personalize con AWS CloudTrail</a>             | 28/11/2018                |
| Amazon Pinpoint                              | <a href="#">Registro de llamadas a la API de Amazon Pinpoint con AWS CloudTrail</a>                | 06/02/2018                |
| API de SMS y voz de Amazon Pinpoint          | <a href="#">Registro de llamadas a la API de Amazon Pinpoint con AWS CloudTrail</a>                | 16/11/2018                |
| Amazon Polly                                 | <a href="#">Registro de llamadas a la API de Amazon Polly con AWS CloudTrail</a>                   | 30/11/2016                |
| Amazon Q Business                            | <a href="#">Registro de llamadas a la API de Amazon Q Business mediante AWS CloudTrail</a>         | 28/11/2023                |
| Amazon Q Developer                           | <a href="#">Registro de llamadas a la API de Amazon Q Developer mediante AWS CloudTrail</a>        | 28/11/2023                |
| Amazon Quantum Ledger Database (Amazon QLDB) | Registro de llamadas a la API de Amazon QLDB con AWS CloudTrail                                    | 10/09/2019                |



| AWSServicio de                                              | Temas de CloudTrail                                                                                                                                                             | Solución compatible desde |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon Quick Suite                                          | <a href="#">Registro de operaciones con CloudTrail</a>                                                                                                                          | 28/04/2017                |
| Amazon Relational Database Service (Amazon RDS)             | <a href="#">Registro de llamadas a la API de Amazon RDS mediante AWS CloudTrail</a>                                                                                             | 13/11/2013                |
| Información de rendimiento de Amazon RDS                    | <a href="#">Registro de llamadas a la API de Amazon RDS mediante AWS CloudTrail</a><br><br>La API de Amazon RDS Performance Insights es un subconjunto de la API de Amazon RDS. | 21/06/2018                |
| Amazon Redshift                                             | <a href="#">Registro de llamadas a la API de Amazon Redshift con AWS CloudTrail</a>                                                                                             | 10/06/2014                |
| Amazon Rekognition                                          | <a href="#">Registro de llamadas a la API de Amazon Rekognition mediante AWS CloudTrail</a>                                                                                     | 06/04/2018                |
| Amazon Route 53                                             | <a href="#">Uso de AWS CloudTrail para capturar las solicitudes enviadas a la API de Route 53</a>                                                                               | 11/02/2015                |
| Controlador de recuperación de aplicaciones (ARC) de Amazon | <a href="#">Registro de llamadas a la API del controlador de recuperación de aplicaciones (ARC) de Amazon mediante AWS CloudTrail</a>                                           | 27/07/2021                |

| AWSServicio de                                  | Temas de CloudTrail                                                                       | Solución compatible desde                                                    |
|-------------------------------------------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Amazon S3                                       | <a href="#">Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail</a>        | Eventos de administración:<br>01/09/2015<br><br>Eventos de datos: 21/11/2016 |
| Amazon Glacier                                  | <a href="#">Registro de llamadas a la API de Amazon Glacier mediante AWS CloudTrail</a>   | 11/12/2014                                                                   |
| Amazon SageMaker AI                             | <a href="#">Registro de llamadas a la API de Amazon SageMaker AI con AWS CloudTrail</a>   | 11/01/2018                                                                   |
| Amazon Security Lake                            | <a href="#">Registro de llamadas a la API de Amazon Security Lake mediante CloudTrail</a> | 05/30/2023                                                                   |
| Amazon Simple Email Service (Amazon SES)        | <a href="#">Registro de llamadas a la API de Amazon SES mediante AWS CloudTrail</a>       | 07/05/2015                                                                   |
| Amazon Simple Notification Service (Amazon SNS) | <a href="#">Registro de llamadas a la API de Amazon SNS mediante AWS CloudTrail</a>       | 09/10/2014                                                                   |
| Amazon Simple Queue Service (Amazon SQS)        | <a href="#">Registro de las acciones de la API de Amazon SQS mediante AWS CloudTrail</a>  | 16/07/2014                                                                   |
| Amazon Simple Workflow Service (Amazon SWF)     | <a href="#">Grabación de llamadas a la API con AWS CloudTrail</a>                         | Eventos de administración:<br>13/05/2014<br><br>Eventos de datos: 14/02/2024 |
| Amazon Textract                                 | <a href="#">Registro de llamadas a la API de Amazon Textract con AWS CloudTrail</a>       | 29/05/2019                                                                   |

| AWSServicio de                            | Temas de CloudTrail                                                                                                                          | Solución compatible desde |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Amazon Timestream                         | <a href="#">Registro de llamadas a la API de Timestream con AWS CloudTrail</a>                                                               | 30/09/2020                |
| Amazon Transcribe                         | <a href="#">Registro de llamadas a la API de Amazon Transcribe con AWS CloudTrail</a>                                                        | 28/06/2018                |
| Amazon Translate                          | <a href="#">Registro de llamadas a la API de Amazon Translate con AWS CloudTrail</a>                                                         | 04/04/2018                |
| Amazon Verified Permissions               | <a href="#">Registro de llamadas a la API de Amazon Verified Permissions mediante AWS CloudTrail</a>                                         | 13/06/2023                |
| Amazon Virtual Private Cloud (Amazon VPC) | <a href="#">Registro de llamadas a la API mediante AWS CloudTrail</a><br><br>La API de Amazon VPC es un subconjunto de la API de Amazon EC2. | 13/11/2013                |
| Amazon VPC Lattice                        | <a href="#">Registros de CloudTrail</a>                                                                                                      | 03/31/2023                |
| Analizador de accesibilidad de Amazon VPC | <a href="#">Registro de llamadas a la API de Reachability Analyzer mediante AWS CloudTrail</a>                                               | 27/11/2023                |
| Amazon WorkDocs                           | Registro de llamadas a la API de Amazon WorkDocs mediante AWS CloudTrail                                                                     | 27/08/2014                |
| Amazon WorkMail                           | <a href="#">Registro de llamadas a la API de Amazon WorkMail mediante AWS CloudTrail</a>                                                     | 12/12/2017                |

| AWS Servicio de                     | Temas de CloudTrail                                                                                           | Solución compatible desde                                                                  |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Amazon WorkSpaces                   | <a href="#">Registro de llamadas a la API de Amazon WorkSpaces Web mediante CloudTrail</a>                    | 09/04/2015                                                                                 |
| Cliente ligero de Amazon WorkSpaces | <a href="#">Registro de llamadas a la API del cliente ligero de Amazon WorkSpaces mediante AWS CloudTrail</a> | 26/11/2023                                                                                 |
| Amazon WorkSpaces Web               | <a href="#">Registro de llamadas a la API de Amazon WorkSpaces Web mediante AWS CloudTrail</a>                | 11/30/2021                                                                                 |
| Application Auto Scaling            | <a href="#">Registro de llamadas a la API de Application Auto Scaling con AWS CloudTrail</a>                  | 31/10/2016                                                                                 |
| AWS Account Management              | <a href="#">Registro de llamadas a la API de AWS Account Management mediante AWS CloudTrail</a>               | 10/01/2021                                                                                 |
| AWS Amplify                         | <a href="#">Registro de llamadas a la API de Amplify mediante AWS CloudTrail</a>                              | 11/30/2020                                                                                 |
| AWS App Mesh                        | <a href="#">Registro de llamadas a la API App Mesh con AWS CloudTrail</a>                                     | AWS App Mesh 30/10/2019<br><br>Servicio de administración de envíos de App Mesh 18/03/2022 |
| AWS App Runner                      | <a href="#">Registro de llamadas a la API de App Runner con AWS CloudTrail</a>                                | 05/18/2021                                                                                 |

| AWS Servicio de                        | Temas de CloudTrail                                                                                | Solución compatible desde                                                 |
|----------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| AWS AppConfig                          | <a href="#">Registro de llamadas a la API de AWS AppConfig mediante AWS CloudTrail</a>             | Eventos de administración: 31/07/2020<br><br>Eventos de datos: 04/01/2024 |
| AWS AppFabric                          | <a href="#">Registro de llamadas a la API de AWS AppFabric mediante AWS CloudTrail</a>             | 27/06/2023                                                                |
| AWS Application Discovery Service      | <a href="#">Registro de llamadas a la API de Application Discovery Service con AWS CloudTrail</a>  | 12/05/2016                                                                |
| AWS Application Transformation Service | (Servicio de backend utilizado por herramientas de AWS, como AWS Microservice Extractor para .NET) | 26/08/2023                                                                |
| AWS AppSync                            | <a href="#">Registro de llamadas a la API de AWS AppSync con AWS CloudTrail</a>                    | 13/02/2018                                                                |
| AWS Artifact                           | <a href="#">Registro de llamadas a la API de AWS Artifact con AWS CloudTrail</a>                   | 27/01/2023                                                                |
| AWS Audit Manager                      | <a href="#">Registro de llamadas a la API de AWS Audit Manager con AWS CloudTrail</a>              | 07/12/2020                                                                |
| AWS Auto Scaling                       | <a href="#">Registro de llamadas a la API de AWS Auto Scaling mediante CloudTrail</a>              | 15/08/2018                                                                |

| AWS Servicio de                               | Temas de CloudTrail                                                                                               | Solución compatible desde |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------|---------------------------|
| Intercambio de datos B2B de AWS               | <a href="#">Registro de llamadas a la API de intercambio de datos de AWS B2B mediante AWS CloudTrail</a>          | 01/12/2023                |
| AWS Backup                                    | <a href="#">Registro de llamadas a la API de AWS Backup con AWS CloudTrail</a>                                    | 04/02/2019                |
| AWS Batch                                     | <a href="#">Registro de llamadas a la API de AWS Batch con AWS CloudTrail</a>                                     | 10/01/2018                |
| Administración de facturación y costos de AWS | <a href="#">Registro de llamadas a la API de Administración de facturación y costos de AWS con AWS CloudTrail</a> | 07/06/2018                |
| AWS Billing Conductor                         | <a href="#">Registro de llamadas a la API de AWS Billing Conductor mediante AWS CloudTrail</a>                    | 03/12/2024                |
| AWS BugBust                                   | Registro de llamadas a la API de BugBust mediante CloudTrail                                                      | 24/06/2021                |
| AWS Certificate Manager                       | <a href="#">Uso de AWS CloudTrail</a>                                                                             | 25/03/2016                |
| AWS Clean Rooms                               | <a href="#">Registro de llamadas a la API de AWS Clean Rooms mediante AWS CloudTrail</a>                          | 21/03/2023                |
| AWS Cloud Map                                 | <a href="#">Registro de llamadas a la API de AWS Cloud Map con AWS CloudTrail</a>                                 | 28/11/2018                |

| AWSServicio de     | Temas de CloudTrail                                                                                                             | Solución compatible desde |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Cloud9         | <a href="#">Registro de llamadas a la API de AWS Cloud9 con AWS CloudTrail</a>                                                  | 21/01/2019                |
| AWS CloudFormation | <a href="#">Registro de llamadas a la API de AWS CloudFormation en AWS CloudTrail</a>                                           | 02/04/2014                |
| AWS CloudHSM       | <a href="#">Registro de llamadas a la API de AWS CloudHSM mediante AWS CloudTrail</a>                                           | 08/01/2015                |
| AWS CloudShell     | <a href="#">Registro y supervisión en AWS CloudShell</a>                                                                        | 12/15/2020                |
| AWS CloudTrail     | <a href="#">Referencia de la API de AWS CloudTrail</a> (Todas las llamadas a la API de CloudTrail se registran con CloudTrail). | 13/11/2013                |
| AWS CodeArtifact   | <a href="#">Registro de llamadas a la API de CodeArtifact con AWS CloudTrail</a>                                                | 10/06/2020                |
| AWS CodeBuild      | <a href="#">Registro de llamadas a la API de AWS CodeBuild con AWS CloudTrail</a>                                               | 01/12/2016                |
| AWS CodeCommit     | <a href="#">Registro de llamadas a la API de AWS CodeCommit con AWS CloudTrail</a>                                              | 11/01/2017                |
| AWS CodeDeploy     | <a href="#">Monitorizar implementaciones con AWS CloudTrail</a>                                                                 | 16/12/2014                |

| AWSServicio de                           | Temas de CloudTrail                                                                                     | Solución compatible desde |
|------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------|
| AWS CodePipeline                         | <a href="#">Registro de llamadas a la API de CodePipeline mediante AWS CloudTrail</a>                   | 09/07/2015                |
| AWS CodeStar                             | <a href="#">Registro de llamadas a la API de AWS CodeStar con AWS CloudTrail</a>                        | 14/06/2017                |
| AWS CodeStarNotificaciones de            | <a href="#">Registro de llamadas a la API de notificaciones de AWS CodeStar con AWS CloudTrail</a>      | 05/11/2019                |
| AWS Config                               | <a href="#">Registro de llamadas a la API de AWS Config con AWS CloudTrail</a>                          | 10/02/2015                |
| AWS Control Catalog                      | <a href="#">Registro de llamadas a la API de AWS Control Catalog mediante AWS CloudTrail</a>            | 04/08/2024                |
| AWS Control Tower                        | <a href="#">Registro de acciones de AWS Control Tower con AWS CloudTrail</a>                            | 12/08/2019                |
| AWS Data Pipeline                        | <a href="#">Registro de llamadas a la API de AWS Data Pipeline mediante AWS CloudTrail</a>              | 02/12/2014                |
| AWS Database Migration Service (AWS DMS) | <a href="#">Registro de llamadas a la API de AWS Database Migration Service mediante AWS CloudTrail</a> | 04/02/2016                |
| AWS DataSync                             | <a href="#">Registro de llamadas a la API de AWS DataSync con AWS CloudTrail</a>                        | 26/11/2018                |



| AWSServicio de                            | Temas de CloudTrail                                                                                    | Solución compatible desde |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Deadline Cloud                        | <a href="#">Registro de llamadas a la API de Deadline Cloud mediante AWS CloudTrail</a>                | 04/02/2024                |
| AWS Device Farm                           | <a href="#">Registro de llamadas a la API de AWS Device Farm mediante AWS CloudTrail</a>               | 13/07/2015                |
| Direct Connect                            | <a href="#">Registro de llamadas a la API de Direct Connect en AWS CloudTrail</a>                      | 08/03/2014                |
| Directory Service                         | <a href="#">Registro de llamadas a la API de Directory Service mediante CloudTrail</a>                 | 14/05/2015                |
| Datos de Directory Service                | <a href="#">Registro de llamadas a la API de datos de Directory Service mediante AWS CloudTrail</a>    | 09/18/2024                |
| AWS Elastic Beanstalk (Elastic Beanstalk) | <a href="#">Utilización de llamadas a la API de Elastic Beanstalk con AWS CloudTrail</a>               | 31/03/2014                |
| AWS Elastic Disaster Recovery             | <a href="#">Registro de llamadas a la API de AWS Elastic Disaster Recovery mediante AWS CloudTrail</a> | 17/11/2021                |
| AWS Elemental MediaConnect                | <a href="#">Registro de llamadas a la API de AWS Elemental MediaConnect con AWS CloudTrail</a>         | 27/11/2018                |
| AWS Elemental MediaConvert                | <a href="#">Registro de llamadas a la API de AWS Elemental MediaConvert con CloudTrail</a>             | 27/11/2017                |

| AWSServicio de                                          | Temas de CloudTrail                                                                                                              | Solución compatible desde |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Elemental MediaLive                                 | <a href="#">Registro de llamadas a la API de MediaLive con AWS CloudTrail</a>                                                    | 19/01/2019                |
| AWS Elemental MediaPackage                              | <a href="#">Registro de llamadas a la API de AWS Elemental MediaPackage con AWS CloudTrail</a>                                   | 21/12/2018                |
| AWS Elemental MediaStore                                | <a href="#">Registro de llamadas a la API de AWS Elemental MediaStore con CloudTrail</a>                                         | 27/11/2017                |
| AWS Elemental MediaTailor                               | <a href="#">Registro de llamadas a la API de AWS Elemental MediaTailor con AWS CloudTrail</a>                                    | 02/11/2019                |
| Mensajes SMS para usuarios finales de AWS               | <a href="#">Registro de llamadas a la API de mensajes SMS para usuarios finales de AWS mediante AWS CloudTrail</a>               | 10/10/2024                |
| Mensajes de redes sociales para usuarios finales de AWS | <a href="#">Registro de llamadas a la API de mensajes de redes sociales para usuarios finales de AWS mediante AWS CloudTrail</a> | 10/10/2024                |
| AWS Entity Resolution                                   | <a href="#">Registro de llamadas a la API de AWS Entity Resolution mediante AWS CloudTrail</a>                                   | 26/07/2023                |
| AWS Fault Injection Service                             | <a href="#">Registrar llamadas a la API con AWS CloudTrail</a>                                                                   | 15/03/2021                |
| AWS Firewall Manager                                    | <a href="#">Registro de llamadas a la API de AWS Firewall Manager con AWS CloudTrail</a>                                         | 05/04/2018                |

| AWSServicio de          | Temas de CloudTrail                                                                        | Solución compatible desde |
|-------------------------|--------------------------------------------------------------------------------------------|---------------------------|
| AWS Global Accelerator  | <a href="#">Registro de llamadas a la API de AWS Global Accelerator con AWS CloudTrail</a> | 26/11/2018                |
| AWS Glue                | <a href="#">Registro de operaciones de AWS Glue con AWS CloudTrail</a>                     | 07/11/2017                |
| AWS Ground Station      | <a href="#">Registro de llamadas a la API de AWS Ground Station con AWS CloudTrail</a>     | 31/05/2019                |
| AWS Health              | <a href="#">Registro de llamadas a la API de AWS Health con AWS CloudTrail</a>             | 21/11/2016                |
| AWS Health Dashboard    | <a href="#">Registro de llamadas a la API de AWS Health con AWS CloudTrail</a>             | 01/12/2016                |
| AWS HealthImaging       | <a href="#">Registro de llamadas a la API de AWS HealthImaging mediante AWS CloudTrail</a> | 26/07/2023                |
| AWS HealthLake          | <a href="#">Registro de llamadas a la API de AWS HealthLake con AWS CloudTrail</a>         | 07/12/2020                |
| AWS HealthOmics         | <a href="#">Registro de llamadas a la API de AWS HealthOmics mediante AWS CloudTrail</a>   | 29/11/2022                |
| AWS IAM Identity Center | <a href="#">Registro de llamadas de API de IAM Identity Center con AWS CloudTrail</a>      | 07/12/2017                |

| AWSServicio de                           | Temas de CloudTrail                                                                       | Solución compatible desde |
|------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------|
| AWS IAM Identity Center: SCIM            | <a href="#">Registro de llamadas de API de IAM Identity Center con AWS CloudTrail</a>     | 28/10/2024                |
| AWS Identity and Access Management (IAM) | <a href="#">Registro de eventos de IAM con AWS CloudTrail</a>                             | 13/11/2013                |
| AWS IoT                                  | <a href="#">Registro de llamadas a la API de AWS IoT con AWS CloudTrail</a>               | 11/04/2016                |
| AWS IoT Analytics                        | <a href="#">Registro de llamadas de la API de análisis de AWS IoT con AWS CloudTrail</a>  | 23/04/2018                |
| AWS IoT Events                           | <a href="#">Descripción de las entradas de los archivos de registro de AWS IoT Events</a> | 11/06/2019                |
| AWS IoT Greengrass                       | <a href="#">Registro de llamadas a la API de AWS IoT Greengrass con AWS CloudTrail</a>    | 29/10/2018                |
| AWS IoT Greengrass V2                    | <a href="#">Registrar llamadas a la API de AWS IoT Greengrass V2 con AWS CloudTrail</a>   | 14/12/2020                |
| AWS IoT SiteWise                         | <a href="#">Registro de llamadas a la API de AWS IoT SiteWise con AWS CloudTrail</a>      | 29/04/2020                |
| AWS Key Management Service (AWS KMS)     | <a href="#">Registro de llamadas a la API de AWS KMS mediante AWS CloudTrail</a>          | 12/11/2014                |

| AWSServicio de                                     | Temas de CloudTrail                                                                                   | Solución compatible desde                                                    |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| AWS Lake Formation                                 | <a href="#">Registro de llamadas a la API de AWS Lake Formation mediante AWS CloudTrail</a>           | 08/09/2019                                                                   |
| AWS Lambda                                         | <a href="#">Registro de llamadas a la API de AWS Lambda mediante AWS CloudTrail</a>                   | Eventos de administración:<br>09/04/2015<br><br>Eventos de datos: 30/11/2017 |
| AWS Launch Wizard                                  | <a href="#">Registro de llamadas a la API de AWS Launch Wizard mediante AWS CloudTrail</a>            | 08/11/2023                                                                   |
| AWS License Manager                                | <a href="#">Registro de llamadas a la API de AWS License Manager con AWS CloudTrail</a>               | 01/03/2019                                                                   |
| AWS Mainframe Modernization                        | <a href="#">Registro de llamadas a la API de AWS Mainframe Modernization mediante AWS CloudTrail</a>  | 08/06/2022                                                                   |
| Managed integrations for AWS IoT Device Management | <a href="#">Registro de llamadas a la API de integraciones administradas mediante AWS CloudTrail</a>  | 03/03/2025                                                                   |
| AWS Managed Services                               | <a href="#">Administración de registros en AMS Accelerate</a>                                         | 21/12/2016                                                                   |
| Acuerdos de AWS Marketplace                        | <a href="#">Registro de llamadas a la API de acuerdos mediante AWS CloudTrail</a>                     | 09/01/2023                                                                   |
| Servicio de implementación de AWS Marketplace      | <a href="#">Registro de llamadas del servicio de implementación de AWS Marketplace con CloudTrail</a> | 29/11/2023                                                                   |

| AWS Servicio de                    | Temas de CloudTrail                                                                                  | Solución compatible desde |
|------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Marketplace Discovery          | <a href="#">Registro de llamadas a la API de AWS Marketplace Discovery mediante AWS CloudTrail</a>   | 12/15/2022                |
| AWS Marketplace Metering Service   | <a href="#">Registro de llamadas a la API de AWS Marketplace con AWS CloudTrail</a>                  | 22/08/2018                |
| AWS Migration Hub                  | <a href="#">Registro de llamadas a la API de AWS Migration Hub con AWS CloudTrail</a>                | 14/08/2017                |
| AWS Migration Hub Recorridos de    | <a href="#">Registro de llamadas a la API de Journeys AWS Migration Hub con AWS CloudTrail</a>       | 12/03/2024                |
| Aprobación multipartita            | <a href="#">Registro de llamadas a la API de aprobación de varias partes mediante AWS CloudTrail</a> | 17/06/2025                |
| AWS Network Firewall               | <a href="#">Registro de llamadas a la API de AWS Network Firewall con AWS CloudTrail</a>             | 11/17/2020                |
| AWS OpsWorks for Chef Automate     | Registro de llamadas a la API de AWS OpsWorks for Chef Automate con AWS CloudTrail                   | 16/07/2018                |
| AWS OpsWorks for Puppet Enterprise | Registro de llamadas a la API de OpsWorks for Puppet Enterprise con AWS CloudTrail                   | 16/07/2018                |

| AWSServicio de                                     | Temas de CloudTrail                                                                               | Solución compatible desde |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------|
| AWS OpsWorks Stacks                                | Registro de llamadas a la API de AWS OpsWorks Stacks con AWS CloudTrail                           | 04/06/2014                |
| Oracle Database@AWS                                | <a href="#">Registro de llamadas a la API de Oracle Database@ de AWS con AWS CloudTrail</a>       | 01/12/2024                |
| AWS Organizations                                  | <a href="#">Registro de llamadas a la API de AWS Organizations con AWS CloudTrail</a>             | 27/02/2017                |
| AWS Outposts                                       | <a href="#">Registro de llamadas a la API de AWS Outposts con AWS CloudTrail</a>                  | 02/04/2020                |
| AWS Panorama                                       | <a href="#">AWS Panorama Referencia de la API de</a>                                              | 20/10/2021                |
| AWS Payment Cryptography                           | <a href="#">Registro de llamadas a la API de AWS Payment Cryptography mediante AWS CloudTrail</a> | 08/06/2023                |
| AWS Private 5G                                     | Registro de llamadas a la API de AWS Private 5G mediante AWS CloudTrail                           | 11/08/2022                |
| AWS Private Certificate Authority (AWS Private CA) | <a href="#">Uso de CloudTrail</a>                                                                 | 04/04/2018                |
| AWS Proton                                         | <a href="#">Registro y supervisión en AWS Proton</a>                                              | 09/06/2021                |
| AWS re:Post Private                                | <a href="#">Registro de llamadas a la API de AWS re:Post Private mediante AWS CloudTrail</a>      | 26/11/2023                |

| AWSServicio de                               | Temas de CloudTrail                                                                                                          | Solución compatible desde |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Resilience Hub                           | <a href="#">AWS CloudTrail</a>                                                                                               | 10/11/2021                |
| AWS Resource Access Manager (AWS RAM)        | <a href="#">Registro de llamadas a la API de AWS RAM con AWS CloudTrail</a>                                                  | 20/11/2018                |
| Explorador de recursos de AWS                | <a href="#">Registro de llamadas a la API de Explorador de recursos de AWS mediante AWS CloudTrail</a>                       | 11/07/2022                |
| Grupos de recursos de AWS                    | <a href="#">Registro y supervisión en Resource Groups</a>                                                                    | 29/06/2018                |
| AWS RoboMaker                                | Registro de llamadas a la API de AWS RoboMaker con AWS CloudTrail                                                            | 16/01/2019                |
| AWS Secrets Manager                          | <a href="#">Monitoreo de la utilización de los secretos de AWS Secrets Manager</a>                                           | 05/04/2018                |
| AWS Security Hub CSPM                        | <a href="#">Registro de llamadas a la API de AWS Security Hub CSPM con AWS CloudTrail</a>                                    | 27/11/2018                |
| AWS Respuesta a un incidente de seguridad de | <a href="#">Registro de llamadas a la API de Respuesta ante incidentes de seguridad de AWS mediante AWS CloudTrail</a>       | 01/12/2024                |
| AWS Security Token Service (AWS STS)         | <a href="#">Registro de eventos de IAM con AWS CloudTrail</a><br><br>En el tema de IAM, se incluye información para AWS STS. | 13/11/2013                |



| AWSServicio de                                  | Temas de CloudTrail                                                                                       | Solución compatible desde |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Serverless Application Repository           | <a href="#">Registro de llamadas a la API de AWS Serverless Application Repository con AWS CloudTrail</a> | 20/02/2018                |
| AWS Service Catalog                             | <a href="#">Registro de llamadas a la API de Service Catalog con AWS CloudTrail</a>                       | 06/07/2016                |
| AWS Shield                                      | <a href="#">Registro de llamadas a la API de Shield Advanced con AWS CloudTrail</a>                       | 08/02/2018                |
| AWS Snowball Edge Edge                          | <a href="#">Registro de llamadas a la API de AWS Snowball Edge Edge con AWS CloudTrail</a>                | 25/01/2019                |
| AWS Step Functions                              | <a href="#">Registro de llamadas a la API de AWS Step Functions con AWS CloudTrail</a>                    | 01/12/2016                |
| AWS Storage Gateway                             | <a href="#">Registro de llamadas a la API de Storage Gateway mediante AWS CloudTrail</a>                  | 16/12/2014                |
| AWS Support                                     | <a href="#">Registro de llamadas a la API de AWS Support con AWS CloudTrail</a>                           | 21/04/2016                |
| Recomendaciones de Soporte (versión preliminar) | <a href="#">Registro de llamadas a la API de Recomendaciones de Soporte con AWS CloudTrail</a>            | 05/22/2024                |
| AWS Systems Manager                             | <a href="#">Registro de llamadas a la API de AWS Systems Manager con AWS CloudTrail</a>                   | 29/11/2017                |

| AWSServicio de                                          | Temas de CloudTrail                                                                                                     | Solución compatible desde |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------|
| AWS Systems Manager Incident Manager de                 | <a href="#">Registro de llamadas a la API de AWS Systems Manager Incident Manager mediante AWS CloudTrail</a>           | 05/10/2021                |
| Creador de redes de telecomunicaciones de AWS (AWS TNB) | <a href="#">Registro de llamadas a la API del Creador de redes de telecomunicaciones de AWS mediante AWS CloudTrail</a> | 21/02/2023                |
| AWS Transfer for SFTP                                   | <a href="#">Registro de llamadas a la API de AWS Transfer for SFTP con AWS CloudTrail</a>                               | 08/01/2019                |
| AWS Transit Gateway                                     | <a href="#">Registro de llamadas a la API para Transit Gateway con AWS CloudTrail</a>                                   | 26/11/2018                |
| AWS Trusted Advisor                                     | <a href="#">Registro de acciones de la consola de AWS Trusted Advisor con AWS CloudTrail</a>                            | 22/10/2020                |
| Acceso verificado de AWS                                | <a href="#">Registre las llamadas a la API de Acceso verificado de AWS con AWS CloudTrail</a>                           | 04/27/2023                |
| AWS WAF                                                 | <a href="#">Registro de llamadas a la API de AWS WAF con AWS CloudTrail</a>                                             | 28/04/2016                |
| AWS Well-Architected Tool                               | <a href="#">Registro de llamadas a la API de AWS Well-Architected Tool con AWS CloudTrail</a>                           | 12/15/2020                |
| AWS X-Ray                                               | <a href="#">Registro de llamadas a la API de AWS X-Ray con CloudTrail</a>                                               | 25/04/2018                |

| AWSServicio de                                             | Temas de CloudTrail                                                                                                                                     | Solución compatible desde |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| Elastic Load Balancing                                     | <a href="#">Registro de AWS CloudTrail para el Classic Load Balancer</a> y <a href="#">Registro de AWS CloudTrail para el Application Load Balancer</a> | 04/04/2014                |
| Actualizaciones de transmisión terrestre (OTA) de FreeRTOS | <a href="#">Registro de llamadas a la API de OTA de AWS IoT con AWS CloudTrail</a>                                                                      | 22/05/2019                |
| Service Quotas                                             | <a href="#">Registro de llamadas a la API Service Quotas mediante AWS CloudTrail</a>                                                                    | 06/24/2019                |

## 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

Para obtener una lista de los servicios de AWS compatibles, consulte [AWS Temas de servicio de para CloudTrail](#).

## Cuotas en AWS CloudTrail

En esta sección, se describen las cuotas de recursos (anteriormente denominadas límites) de CloudTrail. Para obtener información acerca de todas las cuotas de CloudTrail, consulte [Service Quotas](#) en la Referencia general de AWS.

### Note

CloudTrail no cuenta con cuotas ajustables.

## Cuotas de recursos de CloudTrail

En la siguiente tabla se describen las cuotas de recursos dentro de CloudTrail.

| Recurso                             | Cuota predeterminada | Comentarios                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registros de seguimiento por región | 5                    | <p>El número máximo de registros de seguimiento por Región de AWS.</p> <p>En las regiones ocultas, para obtener la última métrica de recuento de recursos, llame a la API <code>ListTrails</code> .</p> <p>Esta cuota no puede incrementarse.</p>                                                                                                                                                                                                                                                          |
| Almacenes de datos de eventos       | 10                   | <p>Número máximo de almacenes de datos de eventos por 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 multirregión para todas las Regiones de AWS y los almacenes de datos de eventos de la organización. Esto incluye los almacenes de datos de eventos en cualquier <a href="#">etapa del ciclo de vida</a>.</p> <p>En las regiones ocultas, para obtener la última métrica de recuento de recursos,</p> |

| Recurso            | Cuota predeterminada | Comentarios                                                                                                                                                                                                                                                              |
|--------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    |                      | <p>llame a la API <code>ListEvent DataStores</code> .</p> <p>Esta cuota no puede incrementarse.</p>                                                                                                                                                                      |
| Canales            | 25                   | <p>Esta cuota se aplica a los canales utilizados para las integraciones de CloudTrail Lake con orígenes de eventos externos a AWS y no se aplica a los canales vinculados a servicios.</p> <p>Esta cuota no puede incrementarse.</p>                                     |
| Paneles por región | 100                  | <p>La cantidad máxima de paneles personalizados de CloudTrail Lake por Región de AWS.</p> <p>En las regiones ocultas, para obtener la última métrica de recuento de recursos, llame a la API <code>ListDashboards</code> .</p> <p>Esta cuota no puede incrementarse.</p> |
| Widgets por panel  | 10                   | <p>Esta cantidad máxima de widgets por panel de CloudTrail Lake.</p> <p>Esta cuota no puede incrementarse.</p>                                                                                                                                                           |

| Recurso                                 | Cuota predeterminada          | Comentarios                                                                                                                                                      |
|-----------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Actualizaciones simultáneas del panel   | 1                             | <p>La cantidad máxima de actualizaciones simultáneas por panel.</p> <p>Esta cuota no puede incrementarse.</p>                                                    |
| Consultas simultáneas                   | 10                            | <p>El número máximo de consultas en cola o en ejecución que se pueden ejecutar simultáneamente en CloudTrail Lake.</p> <p>Esta cuota no puede incrementarse.</p> |
| Eventos por solicitud de PutAuditEvents | 100                           | <p>Puede agregar hasta 100 eventos de actividad (o hasta 1 MB) por solicitud PutAuditEvents .</p> <p>Esta cuota no puede incrementarse.</p>                      |
| Selectores de eventos                   | 5 por registro de seguimiento | <p>Esta cuota no puede incrementarse.</p>                                                                                                                        |

| Recurso                         | Cuota predeterminada                                         | Comentarios                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Selectores de eventos avanzados | 500 condiciones en todos los selectores de eventos avanzados | <p>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.</p> <p>Esta cuota no puede incrementarse.</p> |

| Recurso                                    | Cuota predeterminada                                                  | Comentarios                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recursos de datos en selectores de eventos | 250 en todos los selectores de eventos, en un registro de seguimiento | <p>Si elige limitar eventos de datos mediante selectores de eventos, 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.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"><li>• Se permite un registro de seguimiento con 5 selectores de evento (cada evento configurado con 50 recursos de datos). <math>(5 \times 50 = 250)</math></li><li>• 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. <math>[(3 \times 50) + 1 + 99 = 250]</math></li><li>• No se permite un registro de seguimiento configura</li></ul> |



| Recurso | Cuota predeterminada | Comentarios                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                      | <p>do con 5 selectores de eventos, cada uno de ellos configurado con 100 recursos de datos. (5*100=500)</p> <p>Los selectores de eventos se aplican solo a los registros de seguimiento. Para almacenes de datos de eventos, debe utilizar selectores de eventos avanzados.</p> <p>Esta cuota no puede incrementarse.</p> <p>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.</p> |

| Recurso                                             | Cuota predeterminada                                                                                                                                                                                  | Comentarios                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamaño de eventos                                   | <p>Todas las versiones de eventos: los eventos de más de 256 KB no se pueden enviar a los CloudWatch Logs</p> <p>Versión 1.05 y posterior del evento: límite de tamaño total del evento de 256 KB</p> | <p>Registros de Amazon CloudWatch y Amazon EventBridge permiten un tamaño máximo de evento de 256 KB. CloudTrail no envía eventos de más de 256 KB a Registros de CloudWatch Logs o EventBridge.</p> <p>A partir de la versión 1.05 del evento, 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.</p> |
| Tamaño de archivo de CloudTrail enviado a Amazon S3 | 50 MB antes de la compresión                                                                                                                                                                          | <p>Para los eventos de administración, de datos y de actividad de la red, CloudTrail envía eventos a S3 en archivos ZIP comprimidos. El tamaño máximo de archivo antes de la compresión es de 50 MB.</p> <p>Si se habilita en el registro de seguimiento, Amazon SNS envía notificaciones de entrega de registros después de que CloudTrail envíe archivos gzip a S3.</p>                                                                                                                 |

## Cuotas de transacciones por segundo (TPS) en CloudTrail

En la [Referencia general de AWS](#) se enumeran las cuotas de transacciones por segundo (TPS) para las API AWS. La cuota de transacciones por segundo (TPS) de una API representa el número de solicitudes que puede realizar por segundo para una API determinada sin limitación. Por ejemplo, la cuota de TPS para la API `LookupEvents` de CloudTrail es 2.

Para más información acerca de las cuotas de TPS de cada API de CloudTrail, consulte [Service Quotas](#) en la Referencia general de AWS.

# Tutoriales de introducción a AWS CloudTrail

Si es la primera vez que trabaja con AWS CloudTrail, estos tutoriales le enseñarán a utilizar sus características. Para utilizar las características de CloudTrail, debe tener los permisos adecuados. En esta página, se describen las políticas administradas disponibles para CloudTrail y se proporciona información sobre cómo conceder permisos.

Ejemplos:

- [Concesión de permisos para utilizar CloudTrail](#)
- [Visualización del historial de eventos](#)
- [Creación de un registro de seguimiento para registrar los eventos de administración](#)
- [Creación de un almacén de datos de eventos para eventos de datos de S3](#)

## Concesión de permisos para utilizar CloudTrail

Para crear, actualizar y administrar los recursos de CloudTrail, como registros de seguimiento, almacenes de datos de eventos y canales, debe conceder permisos para utilizar CloudTrail. Esta sección también proporciona información sobre las políticas administradas disponibles para CloudTrail.

### Note

Los permisos que conceda a los usuarios para hacer tareas de administración de CloudTrail no son los mismos que los permisos que CloudTrail requiere para enviar los archivos de registro a buckets de Amazon S3 o enviar notificaciones a 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 requiere un rol que pueda adoptar para enviar los eventos a un grupo de registros de CloudWatch Logs. Debe crear el rol que usa CloudTrail. Para obtener más información, consulte [Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la consola de CloudTrail](#) y [Envío de eventos a Amazon CloudWatch Logs](#).

Las siguientes políticas administradas de AWS están disponibles para CloudTrail:

- [AWSCloudTrail\\_FullAccess](#) – esta política proporciona acceso completo a las acciones de CloudTrail en los recursos de CloudTrail, como los registros de seguimiento, los almacenes de datos de eventos y los canales. Esta política proporciona los permisos necesarios para crear, actualizar y eliminar registros de seguimiento, almacenes de datos de eventos y canales de CloudTrail.

Esta política también ofrece permisos para administrar el bucket de Amazon S3, el grupo de registro de Registros de CloudWatch y un tema de Amazon SNS para un registro de seguimiento. Sin embargo, la política administrada `AWSCloudTrail_FullAccess` no proporciona permisos para eliminar el bucket de Amazon S3, el grupo de registro de Registros de CloudWatch 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 concede permisos para ver la consola de CloudTrail, incluidos los últimos eventos 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 gestionados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en [Creación de un rol para un proveedor de identidad de terceros \(federación\)](#) en la Guía del usuario de IAM.

- Usuarios de IAM:

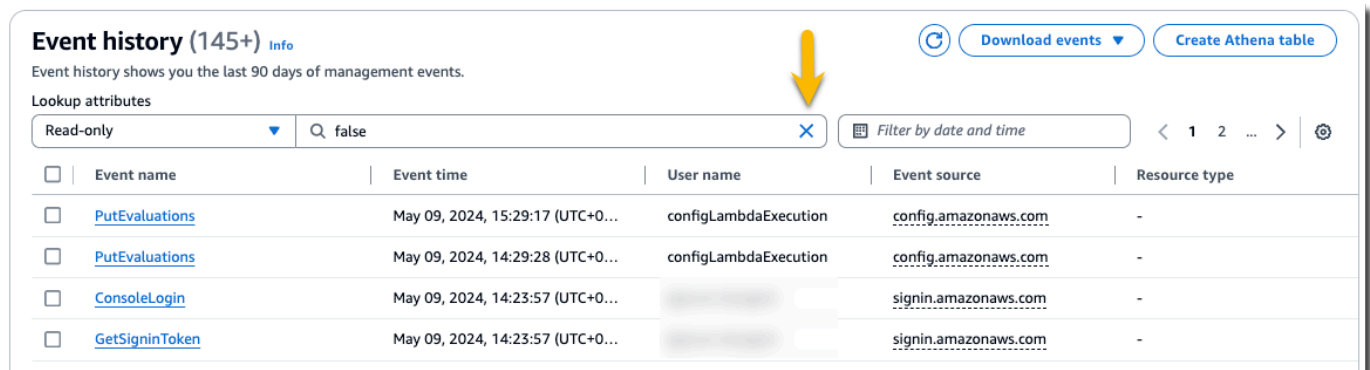
- Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en [Creación de un rol para un usuario de IAM](#) en la Guía del usuario de IAM.
- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en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

## Visualización del historial de eventos

En esta sección se describe cómo usar la página Historial de eventos en la consola de CloudTrail para ver los últimos 90 días de eventos de administración de su Cuenta de AWS para la Región de AWS actual.

Para ver el historial de eventos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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. Elija un atributo por el que filtrar e introduzca el valor completo. CloudTrail no puede filtrar por un valor parcial. Por ejemplo, para ver todos los eventos de inicio de sesión en la consola, puede elegir el filtro Nombre del evento y especificar ConsoleLogin como valor del atributo.

Event history (14)

Info

Event history shows you the last 90 days of management events.

Lookup attributes

Event name

ConsoleLogin

Filter by date and time

Event name

Event time

User name

Event source

Resource type

ConsoleLogin

May 09, 2024, 16:27:50 (UTC+0...)

signin.amazonaws.com

-

ConsoleLogin

May 09, 2024, 14:23:57 (UTC+0...)

signin.amazonaws.com

-

ConsoleLogin

May 08, 2024, 18:52:17 (UTC+0...)

signin.amazonaws.com

-

ConsoleLogin

May 07, 2024, 18:18:31 (UTC+0...)

signin.amazonaws.com

-

O bien, para ver los eventos de administración recientes de CloudTrail, elija Origen del evento y especifique `cloudtrail.amazonaws.com`. Para obtener información sobre los eventos que un servicio registra en CloudTrail, consulte la referencia de la API del servicio.

Event history (50+)

Info

Event history shows you the last 90 days of management events.

Lookup attributes

Event source

cloudtrail.amazonaws.com

Filter by date and time

Event name

Event time

User name

Event source

Resource type

LookupEvents

May 09, 2024, 16:34:57 (UTC+0...)

cloudtrail.amazonaws.com

-

LookupEvents

May 09, 2024, 16:34:57 (UTC+0...)

cloudtrail.amazonaws.com

-

LookupEvents

May 09, 2024, 16:28:26 (UTC+0...)

cloudtrail.amazonaws.com

-

LookupEvents

May 09, 2024, 16:28:23 (UTC+0...)

cloudtrail.amazonaws.com

-

LookupEvents

May 09, 2024, 16:27:57 (UTC+0...)

cloudtrail.amazonaws.com

-

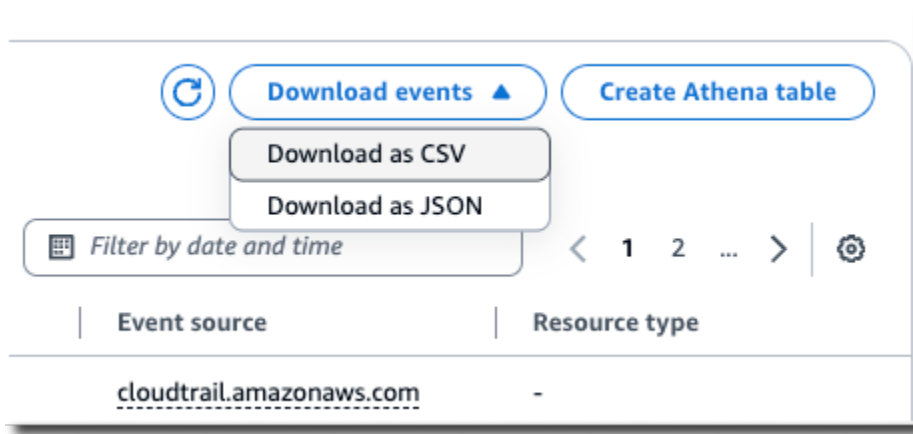
LookupEvents

May 09, 2024, 16:27:57 (UTC+0...)

cloudtrail.amazonaws.com

-

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 comparar eventos, seleccione hasta cinco para completar las casillas de verificación en el margen izquierdo de la tabla Event history (Historial de eventos). Puede ver los detalles de los eventos seleccionados en paralelo en la tabla Comparación de los detalles 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 eventos de CloudTrail](#).

## Creación de un registro de seguimiento para registrar los eventos de administración

Para su primer registro de seguimiento, le recomendamos crear uno que registre todos los [eventos de administración](#) y que no registre ningún [evento de datos](#) o eventos de Insights. 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 bucket de Amazon S3 en el que almacenará los archivos de registros para el registro de seguimiento como parte de la creación del registro de seguimiento en la consola de CloudTrail.

### Note

AWS Control Tower configura un nuevo registro de seguimiento de CloudTrail que registra los eventos de administración al configurar una zona de aterrizaje. Es un registro de seguimiento a nivel de organización, lo que significa que registra todos los eventos de administración de la cuenta de administración y de todas las cuentas de miembros de la organización. Para obtener más información, consulte [About logging in AWS Control Tower](#) en la Guía del usuario de AWS CloudTrail.

En este tutorial, se presupone que está creando su primer registro de seguimiento. En función del número de registros de seguimiento que tenga en su cuenta de AWS y cómo estén configurados, el siguiente procedimiento podría generar cargos o no. CloudTrail almacena archivos de registros en un bucket de Amazon S3, lo que supone costos. 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 Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En la selección de Region (Región), elija la región de AWS en la que desea que se cree el registro de seguimiento. Esta es la región principal del registro de seguimiento.

 Note

La región de origen es la única Región de AWS en la que puede actualizar el registro de seguimiento una vez que se haya creado.

3. En la página de inicio del servicio CloudTrail, la página Trails (Registros de seguimiento), o la sección Trails (Registros de seguimiento) en la página Dashboard (Panel), elija Create trail (Crear registro de seguimiento).
4. En Nombre del registro de seguimiento, indique el nombre del registro de seguimiento; por ejemplo, *management-events*. 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. Cuando se crea un bucket, CloudTrail crea y aplica las políticas de buckets necesarias. Si opta por crear un nuevo bucket de S3, su política de IAM debe incluir permiso para la acción `s3:PutEncryptionConfiguration` porque el cifrado en el servidor está habilitado de forma predeterminada para el bucket. Especifique un nombre para el bucket que sea fácil de identificar.

Para facilitar la búsqueda de registros, cree una carpeta nueva (también conocida como prefijo) en un bucket existente a fin de almacenar los registros de 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 [Uso del cifrado del servidor con claves administradas por Amazon S3 \(SSE-S3\)](#).
8. Mantenga la configuración predeterminada de los Ajustes adicionales.
9. Mantenga la configuración predeterminada para Registros de CloudWatch. Por el momento, no envíe registros a Amazon CloudWatch Logs.
10. (Opcional) En el caso de las etiquetas, puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su registro de seguimiento y controlar el acceso a él. Las etiquetas pueden ayudarlo a identificar los registros de seguimiento de CloudTrail y otros recursos, como los buckets de Amazon S3 que contienen archivos de registros de CloudTrail. Por ejemplo, podría adjuntar una etiqueta con el nombre **Compliance** y el valor **Auditing**.

 Note

Aunque puede agregar etiquetas a los registros de seguimiento al crearlos en la consola de CloudTrail y puede crear un bucket de Amazon S3 para almacenar los archivos de registros en la consola de CloudTrail, no puede agregar etiquetas al bucket de Amazon S3 desde la consola de CloudTrail. 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. Para registrar todos los eventos de administración, deje sin marcar las casillas

de verificación en Excluir eventos de AWS KMS y Excluir eventos de la API de datos de Amazon RDS.

## Choose log events

**Events** [Info](#)  
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

**Event type**  
Choose the type of events that you want to log.

☒ **Management events**  
Capture management operations performed on your AWS resources.

☐ **Data events**  
Log the resource operations performed on or within a resource.

☐ **Insights events**  
Identify unusual activity, errors, or user behavior in your account.

**Management events** [Info](#)  
Management events show information about management operations performed on resources in your AWS account.

**i** No additional charges apply to log management events on this trail because this is your first copy of management events.

**API activity**  
Choose the activities you want to log.

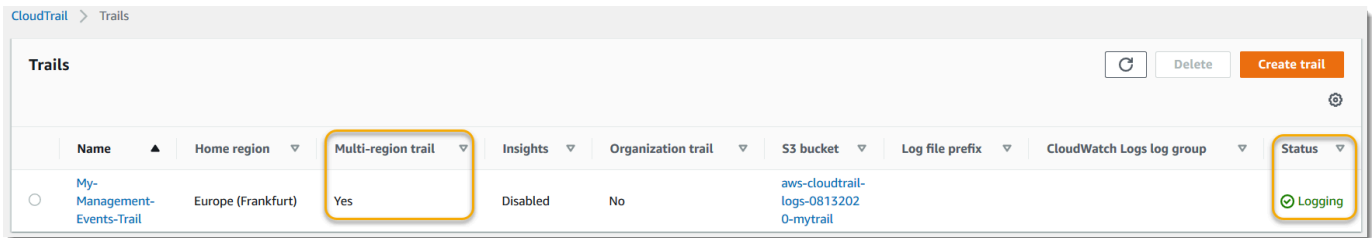
☒ **Read**      ☒ **Write**

☐ **Exclude AWS KMS events**

☐ **Exclude Amazon RDS Data API events**

12. Mantenga la configuración predeterminada para Eventos de datos, Eventos de Insights y Eventos de actividad de la red. Este registro de seguimiento no registrará ningún evento de datos, eventos de Insights ni eventos de actividad de la red. 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.



The screenshot shows the AWS CloudTrail 'Trails' page. At the top, there are buttons for 'Refresh', 'Delete', and 'Create trail'. Below is a table with the following columns: Name, Home region, Multi-region trail, Insights, Organization trail, S3 bucket, Log file prefix, CloudWatch Logs log group, and Status. A single trail is listed: 'My-Management-Events-Trail' in the 'Europe (Frankfurt)' region, with 'Multi-region trail' set to 'Yes', 'Insights' as 'Disabled', 'Organization trail' as 'No', 'S3 bucket' as 'aws-cloudtrail-logs-0813202-0-mytrail', and 'Status' as 'Logging'.

| Name                       | Home region        | Multi-region trail | Insights | Organization trail | S3 bucket                             | Log file prefix | CloudWatch Logs log group | Status  |
|----------------------------|--------------------|--------------------|----------|--------------------|---------------------------------------|-----------------|---------------------------|---------|
| My-Management-Events-Trail | Europe (Frankfurt) | Yes                | Disabled | No                 | aws-cloudtrail-logs-0813202-0-mytrail |                 |                           | Logging |

Para obtener más información acerca de los registros de seguimiento, consulte [Trabajar con registros de seguimiento de CloudTrail](#).

## Ver los archivos de registros

Pasados unos 5 minutos en promedio desde la creación del primer registro de seguimiento, CloudTrail envía el primer conjunto de archivos de registro al bucket de Amazon S3 del registro de seguimiento. Puede ver estos archivos y analizar la información que contienen.

### Note

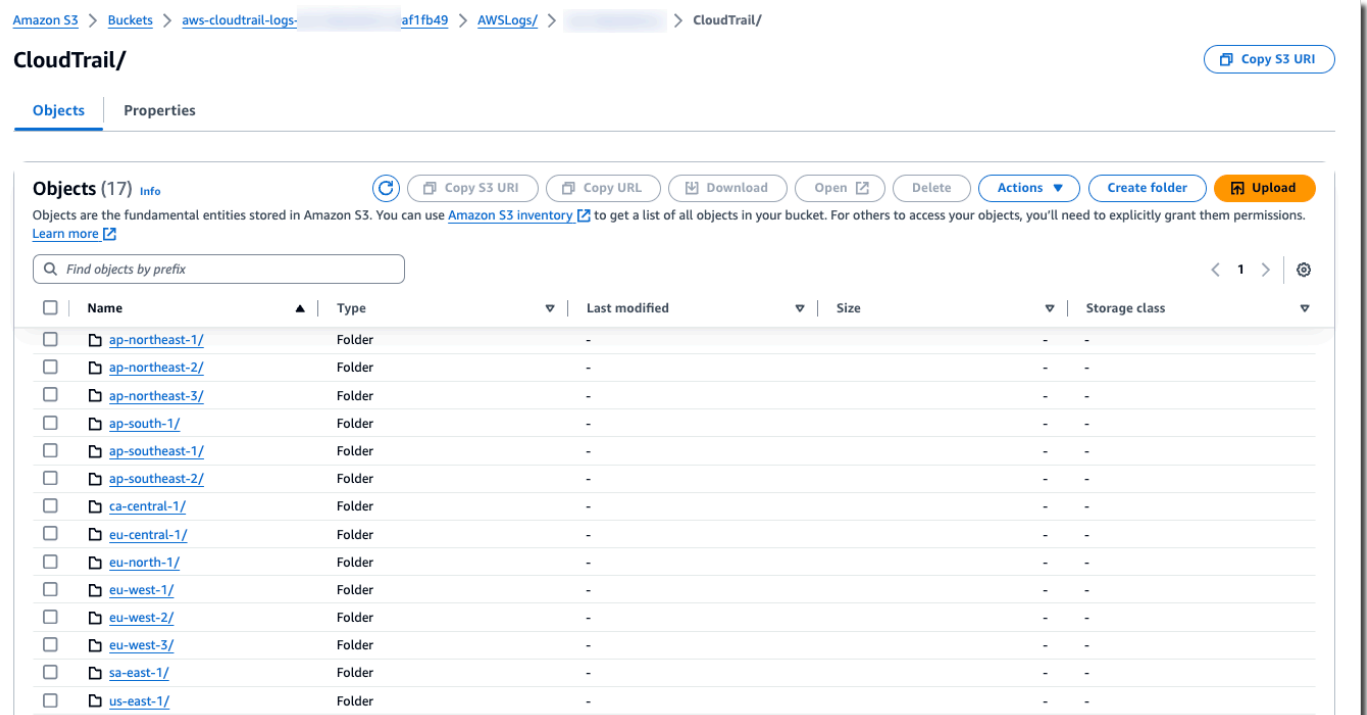
En general, CloudTrail envía registros en un plazo de 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo. Para obtener más información, consulte el [Acuerdo de nivel de servicio de AWS CloudTrail](#).

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.

Para ver los archivos de registro

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, seleccione Trails. En la página Registros de seguimiento, busque el nombre del registro de seguimiento que acaba de crear (en el ejemplo, *management-events*).

3. En la fila del registro de seguimiento, elija el valor del bucket de S3.
4. La consola de Amazon S3 se abre y muestra dos carpetas para el bucket: CloudTrail-Digest y CloudTrail. Elija la carpeta CloudTrail para ver los archivos de registro.
5. Si ha creado un registro multirregión, hay una carpeta para cada Región de AWS. Elija la carpeta correspondiente a la Región de AWS cuyos archivos de registro desea examinar. Por ejemplo, si desea examinar los archivos de registros de la región EE. UU. Este (Ohio), elija us-east-2.



6. 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. Los nombres de los archivos comienzan por el ID de la Cuenta de AWS y terminan por la extensión .gz. Por ejemplo, si el ID de la cuenta fuera **123456789012**, vería archivos con nombres similares a este: **123456789012\_CloudTrail\_us-east-2\_20240512T0000Z\_EXAMPLE.json.gz**.

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. Recomendamos que utilice un lector de archivos JSON, ya que facilita la labor de analizar la información de los archivos de registros de CloudTrail.

# Creación de un almacén de datos de eventos para eventos de datos de S3

Puede crear un almacén de datos de eventos para registrar eventos de CloudTrail (eventos de administración, eventos de datos), [eventos de CloudTrail Insights](#), [pruebas de AWS Audit Manager](#), [elementos de configuración de AWS Config](#) o [eventos que no son de AWS](#).

Cuando crea un almacén de datos de eventos, debe seleccionar los Servicios de AWS y los tipos de recursos para los que desea registrar eventos de datos. Para obtener información sobre los Servicios de AWS que registran los eventos de datos, consulte [Eventos 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.

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

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 más información acerca de los requisitos de nomenclatura de CloudTrail, consulte [Requisitos de nomenclatura de los recursos de CloudTrail, los buckets de S3 y las claves de KMS](#).
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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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. 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.

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

Para habilitar el cifrado con su propia clave de KMS, seleccione Usar mi propia AWS KMS key. Elija New (Nueva) si desea que se cree una AWS KMS key para usted, o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de la clave para permitir que se cifren y descifren los registros de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).



Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 eventos de CloudTrail. 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 costos definidas por el usuario para 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 más información sobre cómo usar las etiquetas en AWS, consulte [Tagging your AWS resources](#) en la Guía del usuario para el etiquetado de recursos de AWS.

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

The screenshot shows the 'Event type' configuration page. At the top, it says 'Event type Info' and 'Choose the type of events you want to add to your event data store. Additional charges apply'. Below this, there are two main sections: 'Choose event types' and 'Specify the type of AWS events'. In 'Choose event types', 'AWS events' is selected with a radio button, and 'Events from integrations' is unselected. In 'Specify the type of AWS events', 'CloudTrail events' is selected with a radio button, 'CloudTrail Insights events' is unselected, and 'Configuration items' is unselected.

**Event type** [Info](#)  
Choose the type of events you want to add to your event data store. [Additional charges apply](#)

**Choose event types**

☒ **AWS events**  
Capture operations performed on or within your AWS resources.

☐ **Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

**Specify the type of AWS events**

☒ **CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.

☐ **CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account. You will be charged separately if you enable Insights for both trails and event data stores.

☐ **Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

13. En Eventos de CloudTrail, seleccione Eventos de datos y anule la selección de Eventos de administración. Para obtener más información sobre los eventos de datos, consulte [Registro de eventos de datos](#).

The screenshot shows the 'CloudTrail events' configuration page. It has a section 'CloudTrail events Info' with a list of options. 'Management events' is checked with a checkbox, while 'Data events', 'Network activity event source - Preview', 'Copy trail events', and 'Enable for all accounts in my organization' are unchecked. At the bottom, there is a section 'Additional settings' with a right-pointing arrow.

**CloudTrail events** [Info](#)

☒ **Management events**  
Capture management operations performed on your AWS resources.

☐ **Data events**  
Log the resource operations performed on or within a resource.

☐ **Network activity event source - Preview**  
Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

☐ **Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.

☐ **Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

► **Additional settings**

14. 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](#).
15. 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.

16. En Configuración adicional, deje las selecciones predeterminadas. De forma predeterminada, un almacén de datos de eventos recopila eventos de todas las Regiones de AWS y comienza a ingerir eventos cuando se crea.
17. En Eventos de datos, lleve a cabo las siguientes selecciones:
  - a. En Tipo de recurso, elija S3. El tipo de recurso identifica el Servicio de AWS y el recurso en los 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 [AdvancedFieldSelector](#) en la Referencia de la API de AWS CloudTrail.
  - 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 las llamadas a la API DeleteObject de un bucket 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.

▼ JSON view

```
[
  {
    "Name": "Log DeleteObject API calls for a specific S3 bucket",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      }
    ]
  },
]
```

- d. En Selectores de eventos avanzados, crearemos un selector de eventos personalizado para filtrar por los campos `eventName` y `resources.ARN`. 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**. Seleccione + Campo para filtrar por otro campo.
- ii. En Campo, seleccione resources.ARN. En Operador, seleccione StartsWith. En Valor, introduzca el ARN del bucket (por ejemplo, `arn:aws:s3:::amzn-s3-demo-bucket`). Para obtener información acerca de cómo obtener el ARN, consulte [Recursos de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource.

▼ Data event: S3 Remove

**Resource type**  
Choose the resource type for which you want to log data events.  
S3 ▼

**Log selector template**  
Custom ▼

**Selector name - optional**  
Log DeleteObject API calls for a specific bucket  
1,000 character limit

**Collect events**  
Log all events, or choose a template to log specific, filtered events to your event data store. You can edit templates later.

**Advanced event selectors** [Info](#)  
Log or exclude events based on the values of advanced event selector fields.

| Field                                               | Operator      | Value                            |   |
|-----------------------------------------------------|---------------|----------------------------------|---|
| eventName ▼                                         | equals ▼      | DeleteObject                     | × |
| AND                                                 |               |                                  |   |
| resources.ARN ▼                                     | starts with ▼ | arn:aws:s3:::amzn-s3-demo-bucket | × |
| <a href="#">+ Field</a> <a href="#">+ Condition</a> |               |                                  |   |

► JSON view

[Add data event type](#)

18. Elija Next (Siguiente) para revisar las opciones seleccionadas.
19. 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).

20. 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 [Visualización de consultas de ejemplo con la consola de CloudTrail](#).

Para obtener más información acerca de CloudTrail Lake, consulte [Trabajar con AWS CloudTrail Lake](#).

# Visualización del costo y el uso de CloudTrail con AWS Cost Explorer

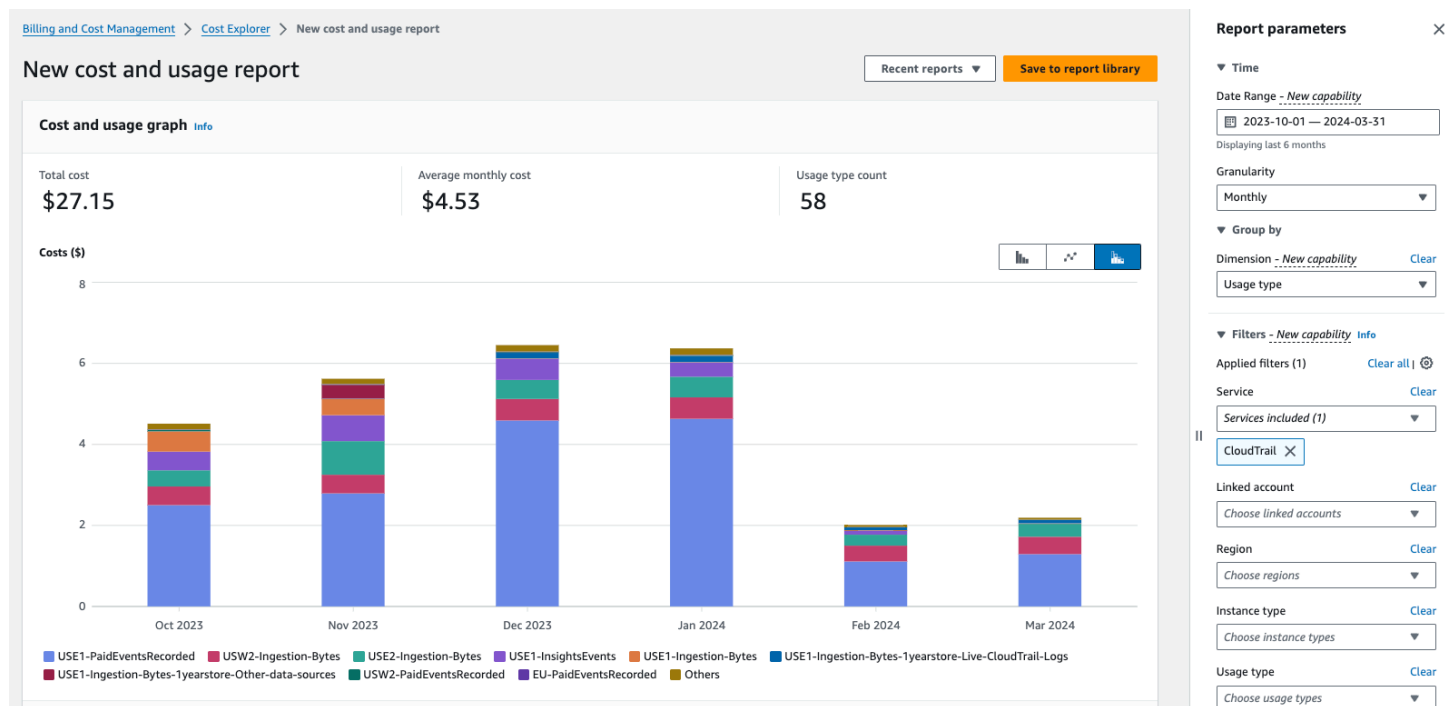
En esta página, se describe cómo puede ver los costos y el uso de CloudTrail mediante [AWS Cost Explorer](#). El Explorador de costos le permite visualizar, comprender y administrar sus costos de AWS y el uso a lo largo del tiempo.

Para obtener más detalles sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

Para ver el costo y el uso de CloudTrail con el Explorador de costos

1. Inicie sesión en la Consola de administración de AWS y abra la consola del Explorador de costos en <https://console.aws.amazon.com/cost-management/home#/custom>.
2. En Tiempo, elija el intervalo de fechas que desee analizar.
3. En Agrupar por, para Dimensión, elija Tipo de uso.
4. En Filtros, para Servicio, seleccione CloudWatch.

La siguiente imagen muestra un ejemplo de un informe de costos filtrado para CloudTrail y agrupado por tipo de uso.



Revise el tipo de uso para ver qué características de CloudTrail generaron el mayor costo. Cada tipo de uso comienza con el código de la Región de AWS en la que se incurrió en el cargo.

La tabla siguiente describe los tipos de uso de CloudTrail para cada característica de CloudTrail.

| Característica de CloudTrail           | Tipo de uso                          | Descripción                                                                                                    |
|----------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Registros de seguimiento de CloudTrail | <i>region</i> -FreeEventsRecorded    | La primera copia de los eventos de administración se entrega de forma gratuita en una Región de AWS.           |
| Registros de seguimiento de CloudTrail | <i>region</i> -PaidEventsRecorded    | Cargo por la entrega de copias adicionales de los eventos de administración a una Región de AWS.               |
| Registros de seguimiento de CloudTrail | <i>region</i> -DataEventsRecorded    | Cargo por la entrega de eventos de datos a una Región de AWS. Los eventos de datos siempre incurren en cargos. |
| Registros de seguimiento de CloudTrail | <i>region</i> -NetworkEventsRecorded | Cargo por la entrega de eventos de actividad de la red a una Región de                                         |

| Característica de CloudTrail | Tipo de uso                    | Descripción                                                                                                                                                                                                                                              |
|------------------------------|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |                                | AWS. Los eventos de actividad de la red siempre incurren en cargos.                                                                                                                                                                                      |
| CloudTrail Lake              | <i>region</i> -Ingestion-Bytes | Cargo por ingerir eventos en un almacén de datos de eventos de CloudTrail Lake mediante la opción Precios de retención de siete años. Los precios de ingesta se basan en el volumen de datos ingeridos y son los mismos para todos los tipos de eventos. |



| Característica de CloudTrail | Tipo de uso                                                    | Descripción                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CloudTrail Lake              | <i>region</i> -Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs | Cargo por ingerir eventos de datos de CloudTrail, eventos de actividad de la red y eventos de administración en un almacén de datos de eventos de CloudTrail Lake mediante la opción Precios de retención ampliables por un año. |

| Característica de CloudTrail | Tipo de uso                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CloudTrail Lake              | <i>region</i> -Ingestion-Bytes-1yearstore-Other-data-sources | Cargo por ingerir otros orígenes de eventos en un almacén de datos de eventos de CloudTrail Lake mediante la opción Precios de retención ampliables por un año. Esto incluye los eventos de CloudTrail Insights, los elementos de configuración de AWS Config, las pruebas de AWS Audit Manager, los registros históricos de CloudTrail (sin comprimir) importados desde S3 y los eventos ajenos a AWS. |

| Característica de CloudTrail | Tipo de uso                       | Descripción                                                                                                                                                                                                                                                                      |
|------------------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CloudTrail Lake              | <i>region</i> -QueryScanned-Bytes | Cargo por ejecutar consultas de CloudTrail Lake. Cuando ejecuta consultas en CloudTrail Lake, incurre en cargos según la cantidad de datos optimizados y comprimidos que se hayan escandeado.                                                                                    |
| CloudTrail Insights          | <i>region</i> -InsightsEvents     | Cargo por los eventos de CloudTrail Insights. En el caso de los eventos de Insights, incurrirá en cargos según el número de eventos de administración analizados por tipo de Insight. Para obtener más información, consulte <a href="#">Costos de los eventos de Insights</a> . |

# Se utiliza AWS Budgets para administrar los costos

AWS Budgets, una característica de Administración de facturación y costos de AWS, le permite definir presupuestos personalizados que le avisan cuando los costos o el uso superan (o se prevé que superen) el importe presupuestado.

Se recomienda crear un presupuesto para CloudTrail mediante el uso de AWS Budgets, el cual puede ayudarlo a realizar un seguimiento de sus gastos de CloudTrail. Los presupuestos basados en costos ayudan a tomar conciencia sobre cuánto se facturará por el uso de 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.

## Note

Aunque puede aplicar etiquetas a los registros de seguimiento de CloudTrail, AWS Billing no puede utilizar etiquetas aplicadas a registros de seguimiento para la asignación de costos. El Explorador de costos puede mostrar los costos de los almacenes de datos de eventos de CloudTrail Lake y los costos del servicio de CloudTrail en su conjunto.

Para comenzar a utilizar Presupuestos de AWS, abra [Administración de facturación y costos de AWS](#) y, a continuación, elija Budgets (Presupuestos) en la barra de navegación izquierda. Cuando cree un presupuesto, recomendamos configurar alertas de presupuesto para realizar un seguimiento de los gastos de CloudTrail. A fin de obtener más información sobre cómo utilizar AWS Budgets, consulte [Administración de costos con AWS Budgets](#) y [Prácticas recomendadas para AWS Budgets](#).

## Creación de etiquetas de asignación de costos definidas por el usuario para almacenes de datos de eventos de CloudTrail Lake

Puede crear [etiquetas de asignación de costos definidas por el usuario](#) para hacer un seguimiento de los costos 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. Después de activar las etiquetas de asignación de costos, AWS las utiliza para organizar los costos de los recursos en el informe de asignación de costos.

- Para crear etiquetas en la consola, consulte el paso 9 del procedimiento [Para crear un almacén de datos de eventos para eventos de CloudTrail](#).

- Para crear etiquetas con la API de CloudTrail, consulte [CreateEventDataStore](#) y [AddTags](#) en la Referencia de la API de AWS CloudTrail.
- Para crear etiquetas con la AWS CLI, consulte [create-event-data-store](#) y [add-tags](#) en la Referencia de los comandos de la AWS CLI.

Para obtener más información, consulte [Activación de etiquetas de asignación de costos definidas por el usuario](#).

## Administración de los costos de los registros de seguimiento de CloudTrail

Puede configurar y administrar los registros de seguimiento de CloudTrail de forma que capture los datos que necesita sin dejar de ser rentable. Para obtener más información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

### Configuración de registros de seguimiento

CloudTrail ofrece flexibilidad en la configuración de registros de seguimiento en su cuenta. Algunas decisiones que toma durante el proceso de configuración requieren que conozca las repercusiones en la factura de CloudTrail. A continuación se muestran ejemplos de cómo las configuraciones de registro de seguimiento pueden repercutir en su factura de CloudTrail.

#### Creación de varios registros de seguimiento

La primera copia de los eventos de administración de cada región se entrega de forma gratuita. Por ejemplo, si su cuenta tiene 2 registros de seguimiento de una sola región (uno en us-east-1 y otro en us-west-2), no se cobrarán cargos de CloudTrail porque solo hay un registro de seguimiento registrando los eventos de cada región respectiva. Sin embargo, si su cuenta tiene un registro de seguimiento multirregión y otro de una sola región, el de una sola región incurrirá en cargos porque el multirregión ya registra los eventos de todas las regiones.

Si crea más registros de seguimiento que envían los mismos eventos de administración a otros destinos, las entregas posteriores generarán costos de CloudTrail. 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 eventos de datos, todas las entregas generan costos de CloudTrail, 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 del lado del servidor administrado por AWS KMS (SSE-KMS) en los buckets de S3 puede dar lugar a un gran número de eventos de administración de AWS KMS en CloudTrail. Los volúmenes de mayor tamaño de eventos en varios registros de seguimiento también pueden repercutir en los costos.

Para ayudar a limitar la cantidad de eventos que se registran en el registro de seguimiento, puede filtrar los eventos de AWS KMS o de la API de datos de Amazon RDS al elegir Excluir eventos de AWS KMS o Excluir eventos de la API de datos de Amazon RDS en las páginas Crear registro de seguimiento o Actualizar registro de seguimiento. 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, lo que le permite registrar solo los eventos de datos que le interesen. Para obtener más información, consulte [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#).

Puede utilizar selectores de eventos avanzados para incluir o excluir eventos de actividad de la red en función de los campos `eventName`, `resources.type`, `resources.ARN`, `errorCode` y `vpcEndpointId`, lo que le permite registrar solo los eventos de datos que le interesen. Para obtener más información, consulte [Registro de eventos de actividad de la red](#).

Para obtener más información acerca de la creación y actualización de un registro de seguimiento, consulte [Creación de un registro de seguimiento con la consola de CloudTrail](#) o [Actualización de un registro de seguimiento con la consola de CloudTrail](#) en esta guía.

## AWS Organizations

Al configurar un registro de seguimiento de Organizations con CloudTrail, CloudTrail reproduce el registro de seguimiento en cada cuenta miembro de su 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 de](#)
- [Administración de costos con AWS Budgets](#)
- [Introducción al Explorador de costos](#)
- [Prepararse a fin de crear un registro de seguimiento para la organización](#)

## Administración de los costos de CloudTrail Lake

Los almacenes de datos de eventos de AWS CloudTrail Lake y las consultas conllevan cargos. Puede configurar los almacenes de datos de eventos de forma que capturen los datos que necesita y, al mismo tiempo, le siga resultando rentable. Para obtener información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

### Temas

- [Opciones de precios del almacén de datos de eventos](#)
- [Comprensión de los cargos de CloudTrail Lake](#)
- [Recomendaciones sobre cómo reducir 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 | <p>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.</p> <p>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 extendida está disponible a precio de pago por uso.</p> <p>Esta es la opción predeterminada.</p> <p>Periodo de retención predeterminado: 366 días.</p> <p>Periodo máximo de retención: 3653 días.</p> |
| Precios de retención de siete años         | FIXED_RETENTION_PRICING      | <p>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.</p> <p>La retención está incluida en los precios de incorporación sin costo adicional.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



| Opción de precios (consola) | BillingMode (API) | Descripción                                     |
|-----------------------------|-------------------|-------------------------------------------------|
|                             |                   | Periodo de retención predeterminado: 2557 días. |
|                             |                   | Periodo máximo de retención: 2557 días.         |

## Comprensión de los cargos de CloudTrail Lake

En las tablas siguientes, se proporciona información sobre cómo los almacenes de datos de eventos de CloudTrail Lake y las consultas conllevan cargos. Para obtener información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

| Tipo de cargo                          | Cómo se incurre en los cargos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ingesta de datos (datos sin comprimir) | <p>En el caso de CloudTrail Lake, usted paga en función de los datos no comprimidos incorporados. La <a href="#">opción de precios</a> del almacén de datos de eventos determina el costo de la incorporación de eventos:</p> <ul style="list-style-type: none"> <li>Precios de retención ampliables por un año: ofrecen precios de incorporación en función del tipo de evento.</li> <li>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.</li> </ul> <p>Copiar eventos de registro de seguimiento</p> <p>Al copiar <a href="#">eventos de registros de seguimiento</a> en 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 almacenam</p> |

| Tipo de cargo | Cómo se incurre en los cargos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <p>imiento 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.</p> <div data-bbox="591 382 1510 1171"><p> <b>Note</b></p><p>CloudTrail no copiará un evento si la hora del evento 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:</p><p>Periodo de retención = <i>el evento más antiguo registrado en días</i> + <i>el número de días que se debe retener</i></p><p>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.</p></div> |

| Tipo de cargo                                                               | Cómo se incurre en los cargos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Retención de datos (datos optimizados y comprimidos)                        | <p>CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato <a href="#">ORC de Apache</a>. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos comprimidos.</p> <p>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 verificando si el tiempo 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 la duración del evento sea superior a 90 días.</p> <p>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.</p> <p>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 incorporación durante los primeros 366 días (el periodo de retención predeterminado). Después de 366 días, el almacenamiento se ofrece a precios de pago por consumo y se cobra en función de los datos optimizados y comprimidos del almacén de datos de eventos.</p> |
| Ejecución de consultas en CloudTrail Lake (datos optimizados y comprimidos) | Cuando ejecuta consultas en CloudTrail Lake, paga según la cantidad de datos escaneados optimizados y comprimidos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Recomendaciones sobre cómo reducir los costos

En esta sección, se proporcionan recomendaciones sobre cómo reducir los costos cuando trabaja 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 configuración de AWS Config, pruebas de Audit Manager y eventos externos a 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 Precios de retención de siete años, puede cambiar la opción de precios mediante la [consola de CloudTrail](#), [AWS CLI](#), o la operación de la API [UpdateEventDataStore](#).

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 almacén de datos de eventos para los eventos de administración, de datos o de actividad de la red de CloudTrail, filtre los eventos que no sean de interés mediante selectores de eventos avanzados.

Puede filtrar los eventos administrados en los siguientes campos del selector de eventos avanzados: `eventName`, `eventSource`, `eventType`, `readOnly`, `sessionCredentialFromConsole` y `userIdentity.arn`.

Puede filtrar los eventos de datos en los siguientes campos del selector de eventos avanzados: `eventName`, `eventSource`, `eventType`, `resources.type`, `resources.ARN`, `readOnly`, `sessionCredentialFromConsole` y `userIdentity.arn`. Para obtener más información, consulte [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#).

Puede filtrar los eventos de actividad de la red en los siguientes campos del selector de eventos avanzados: `eventName`, `errorCode` y `vpcEndpointId`. Para obtener más información, consulte [Registro de eventos de actividad de la red](#).

Elija un periodo más reducido al copiar los eventos de los registros de seguimientos

Al copiar los eventos de registros de seguimiento en CloudTrail Lake, especifique momentos de inicio y de finalización del evento más cercanos para reducir la cantidad de datos ingeridos.

Si va a copiar eventos de registros de seguimiento en CloudTrail Lake para llevar a cabo un análisis histórico y no quiere ingerir eventos futuros, desactive la opción de ingerir eventos para no generar cargos por la ingesta 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.

## Véase también

- [AWS CloudTrail Precios de](#)
- [Métricas de CloudWatch compatibles](#)
- [Administración de costos con AWS Budgets](#)
- [Introducción al Explorador de costos](#)

# Trabajar con el historial de eventos de CloudTrail

CloudTrail está habilitado de forma predeterminada en su cuenta de AWS y usted tiene acceso automático al Historial de eventos de CloudTrail. En el Historial de eventos se ofrece 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 hecha a través de la Consola de administración de AWS, la AWS Command Line Interface y los SDK y las API de AWS. El Historial de eventos registra los eventos en la Región de AWS donde ocurrió el evento. No se cobran cargos de CloudTrail por ver el Historial de eventos.

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

Puede utilizar la página Historial de eventos en la consola de CloudTrail para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en la infraestructura de 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 en paralelo los detalles de los eventos en el Historial de eventos. Puede [buscar eventos](#) mediante programación con los SDK de AWS o la AWS Command Line Interface.

## Note

Con el tiempo, es posible que los Servicios de AWS agreguen más eventos. CloudTrail registra estos eventos en el Historial de eventos, pero el registro completo de 90 días de actividad que incluye los eventos adicionales no estará disponible hasta 90 días después de la fecha en la que los agregó.

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 administración recientes mediante la consola de CloudTrail y la AWS CLI, y se describe cómo descargar un archivo de eventos. A fin de obtener más información sobre el uso de la API `LookupEvents` para recuperar

información de los eventos de CloudTrail, consulte [LookupEvents](#) en la Referencia de la API de AWS CloudTrail.

## Temas

- [Limitaciones del Historial de eventos](#)
- [Visualización de eventos de administración recientes con la consola](#)
- [Visualización de eventos de administración recientes con la AWS CLI](#)

# Limitaciones del Historial de eventos

Las siguientes limitaciones son aplicables al Historial de eventos.

- La página Historial de eventos de la consola de CloudTrail solo muestra los eventos de administración. No muestra eventos de datos ni de Insights ni de actividad de la red.
- El Historial de eventos está limitado a los últimos 90 días. 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](#).
- Al descargar eventos de la página historial de eventos de la consola de CloudTrail, puede descargar hasta 200 000 eventos en un solo archivo. Si alcanza el límite de 200 000 eventos, la consola de CloudTrail le ofrecerá la opción de descargar archivos adicionales.
- En el Historial de eventos no se ofrece el agregado 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 está limitada a una sola Cuenta de AWS y solo devuelve eventos de una única Región de AWS; además, no se pueden consultar varios atributos. Solo puede aplicar un filtro de atributo y un filtro de intervalo de tiempo.

Puede crear un almacén de datos de eventos de CloudTrail Lake para hacer consultas en varios atributos y Regiones de AWS. También puede hacer consultas en varias Cuentas de AWS de una organización de AWS Organizations. 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 configuración de AWS Config, las pruebas de Audit Manager y los eventos que no son de AWS. Las consultas de CloudTrail Lake ofrecen una visión más detallada y personalizable de los eventos que las simples búsquedas de claves y valores en la página Historial de eventos, o

ejecutando `LookupEvents`. Para obtener más información, consulte [Trabajar con AWS CloudTrail Lake](#) y [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

- 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.

## Visualización de eventos de administración recientes con la consola

Puede utilizar la página Historial de eventos de la consola de CloudTrail para ver los últimos 90 días de eventos de administración en 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. Puede seleccionar hasta cinco eventos en el Event history (Historial de eventos) y comparar los detalles en paralelo.

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 Historial de eventos. No puede eliminar de manera manual los eventos del Historial de eventos.

Para obtener más información sobre aspectos específicos relacionados con el modo en que CloudTrail registra los eventos de un determinado servicio, consulte la documentación de dicho servicio. Para obtener más información, consulte [AWSTemas de servicio de para CloudTrail](#).

### Note

Para mantener un registro continuo de la actividad y de los eventos de los últimos 90 días, cree un [almacén de datos de eventos](#) o un [registro de seguimiento](#).

Para ver el Historial de eventos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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.
3. Puede filtrar los eventos por un solo atributo, que puede elegir en la lista desplegable. Para filtrar por un atributo, elija un atributo en la lista desplegable e introduzca el valor completo. Por ejemplo, para ver todos los eventos de inicio de sesión en la consola, puede elegir el filtro Nombre del evento y especificar ConsoleLogin. O bien, para ver los eventos de administración recientes de S3, elija Origen del evento y especifique s3.amazonaws.com.
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 comparar eventos, seleccione hasta cinco para completar las casillas de verificación en el margen izquierdo de la tabla Event history (Historial de eventos). Puede ver los detalles de los eventos seleccionados en paralelo en la tabla Comparación de los detalles 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.

## Contenido

- [Navegación entre páginas](#)
- [Personalización de la pantalla](#)
- [Filtro de eventos de CloudTrail](#)
- [Ver los detalles de un evento](#)
- [Descarga de eventos](#)
- [Ver los recursos a los que se hace referencia con 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 consola de CloudTrail al seleccionar 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 del evento
  - Hora del evento
  - Nombre del 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. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija 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.

## Filtro de eventos de CloudTrail

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.

### AWSClave de acceso de

El ID de clave de acceso de AWS 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 ID de CloudTrail 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 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.

## 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 tipos de recursos varían en función de cada servicio de AWS.

## 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. Puede descargar hasta 200 000 eventos en un solo archivo. Si alcanza el límite de 200 000 eventos, la consola de CloudTrail le ofrecerá la opción de descargar archivos adicionales. 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. 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 con AWS Config

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

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



en la columna Escala de tiempo de los recursos de AWS Config para ver el recurso en la consola de AWS Config.

Si el icono



está atenuado, AWS Config no está activado o no está registrando el tipo de recurso. Elija el icono para ir a la consola de AWS Config para activar el servicio o comenzar el registro de ese tipo de recurso. Para obtener más información, consulte [Configuración de AWS Config mediante la consola](#) en la Guía para desarrolladores de AWS Config.

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 el 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 agregó recientemente compatibilidad con el tipo de recurso, pero aún no está disponible en la consola de CloudTrail. Puede buscar el recurso en la consola de AWS Config para ver la escala de tiempo del recurso.
- El recurso es propiedad de otra Cuenta de AWS.
- El recurso es propiedad de otro Servicio de AWS, como una política de IAM administrada.
- 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 en la consola de AWS Config, consulte [Concesión de permisos para ver la información de AWS Config en la consola de CloudTrail](#).

Para obtener más información sobre AWS Config, consulte la [Guía para desarrolladores de AWS Config](#).

# Visualización de eventos de administración recientes con la AWS CLI

Puede consultar los eventos de administración de CloudTrail de los últimos 90 días para la Región de AWS actual a través del comando `aws cloudtrail lookup-events`. El comando `aws cloudtrail lookup-events` muestra los eventos en la Región de AWS en que se produjeron.

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

- AWSClave de acceso de
- 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 de la 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 cómo utilizar la interfaz de la línea de comandos de AWS, consulte la [Guía del usuario de AWS Command Line Interface](#).

## 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 comandos de AWS CLI, debe instalar la AWS CLI. Para informarse, consulte [Introducción a la AWS CLI](#).
- Asegúrese de que la versión de AWS CLI es posterior a la versión 1.6.6. Para comprobar la versión de la CLI, ejecute `aws --version` en la línea de comandos.

- Para configurar la cuenta, la Región de AWS y el formato de salida predeterminado para una sesión de AWS CLI, utilice el comando `aws configure`. Para obtener más información, consulte [Configuración de la interfaz de línea de comandos de AWS](#).

#### Note

Los comandos de la AWS CLI de CloudTrail 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": "kb0t5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YA1ju3oXd12juy3CIZ
  "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 evento de CloudTrail, consulte [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

## 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 de AttributeValue es de 2000 caracteres. Los siguientes caracteres («\_», «», «,», » y «\n») cuentan como dos caracteres en el 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 para el de CloudTrail especificado 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=kb0t5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YAlju3oXd12juy3CIZ
```

## Obtener datos de entrada JSON de un archivo

La AWS CLI de algunos servicios de AWS tiene dos parámetros, --generate-cli-skeleton y --cli-input-json, que puede utilizar para generar una plantilla JSON que se puede modificar y

utilizar como datos de entrada en el parámetro `--cli-input-json`. En esta sección se describe cómo utilizar estos parámetros con `aws cloudtrail lookup-events`. Para obtener más información general, consulte [AWS CLI skeletons and input files](#).

Para buscar los eventos de CloudTrail mediante la obtención de 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 --generate-cli-skeleton > LookupEvents.txt
```

El archivo de plantilla generado (en este caso, `LookupEvents.txt`) tiene este 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

### Events (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 representación de cadena del evento de CloudTrail recuperado.

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 servicio de AWS para el 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.

# Trabajar con CloudTrail Insights

AWS CloudTrail Insights ayuda a los usuarios de AWS a identificar y responder a la actividad inusual asociada a las tasas de llamada 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 eventos de administración anteriores para establecer sus patrones normales de tasas de llamada a la API y tasas de error de API, también conocido como referencia. A continuación, CloudTrail genera eventos de Insights cuando las tasas actuales de llamada a la API o las tasas de error se desvían de la referencia.

Puede recopilar dos tipos de Insights:

- **Tasa de llamada a la API:** medida de las llamadas a la API de administración de solo escritura que se producen por minuto en comparación con una cantidad de llamadas a la API de referencia. Para registrar los eventos de Insights en la cantidad de llamadas a la API, el registro de seguimiento o almacén de datos de eventos debe habilitar Insights y registrar los eventos de administración de `write`.
- **Tasa de errores de la API:** medida de las llamadas a la API de administración que producen códigos de error. El error se muestra si la llamada a la API no se hace correctamente. 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 habilitar Insights y registrar los eventos de administración de `read` o `write`, o los dos eventos de administración de `read` y `write`.

CloudTrail Insights analiza los eventos de administración que se producen en cada región para el registro de seguimiento o el almacén de datos de eventos y genera un evento de Insights cuando se detecta una actividad inusual que se desvía del valor de referencia. El evento de CloudTrail Insights se genera en la misma región en la que se genera el evento de administración correspondiente.

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](#).

## Temas

- [Costos de los eventos de Insights](#)
- [Entrega de eventos de Insights](#)
- [Registro de eventos de Insights con la consola de CloudTrail](#)

- [Registro de eventos de Insights con la AWS CLI](#)
- [Visualización de eventos de Insights para registros de seguimiento](#)
- [Visualización de eventos de Insights para los almacenes de datos de eventos](#)

## Costos de los eventos de Insights

Al habilitar los eventos de Insights en un registro de seguimiento o almacén de datos de eventos existente, CloudTrail analiza los últimos 28 días de los eventos de administración recopilados por el registro de seguimiento o almacén de datos de eventos para establecer una referencia de la actividad normal. Una vez que se crea la referencia inicial, esta se recalcula todos los días sobre los datos de los últimos 28 días. No se cobran cargos de CloudTrail por el análisis de referencia.

Después del el análisis de referencia, se le cobrarán cargos de CloudTrail por cualquier evento de administración futuro analizado por CloudTrail. Incurre en cargos según el número de eventos de administración analizados por los tipos de Insights habilitados.

Si decide registrar ambos tipos de Insights para un registro de seguimiento o almacén de datos de eventos que registre eventos de administración de `read` y `write`, la cantidad total de eventos analizados será mayor que la cantidad total de eventos de administrados registrados. Esto se debe a que CloudTrail analizará los eventos de administración de solo escritura dos veces, una para calcular la tasa de llamadas a la API y otra para determinar la tasa de errores de la API. Los eventos de administración de solo lectura se analizarán una vez para calcular la tasa de errores de la API.

Puede identificar los cargos de los eventos de Insights en la factura si busca el tipo de uso de `InsightsEvents`. Para obtener más información, consulte [Visualización del costo y el uso de CloudTrail con AWS Cost Explorer](#).

Si tiene Insights habilitado, se le cobrarán cargos por separado para cada registro de seguimiento o almacén de datos de eventos. Para obtener más información sobre los precios, consulte [Precios de AWS CloudTrail](#).

Ejemplo 1: habilite Insights para medir la tasa de llamadas a la API y la tasa de errores de la API en un registro de seguimiento

En este primer ejemplo, se habilita Insights en un registro de seguimiento y se elige recopilar ambos tipos de Insights. El registro de seguimiento este ejemplo consiste en registrar tanto los eventos de administración de `read` y `write`.

- CloudTrail analiza los eventos de administración que se registraron en los últimos 28 días para formar una referencia. No se cobran cargos de CloudTrail por el análisis.
- Una vez creada la referencia, el registro de seguimiento registra 300 000 eventos de administración, de los cuales 270 000 son eventos de administración de `read` y 30 000 son eventos de administración de `write`.
  - Los eventos de administración de `write` se analizan dos veces, una para determinar la tasa de llamadas a la API y otra para determinar la tasa de errores de la API ( $30\,000 * 2 = 60\,000$ ).
  - Los eventos de administración de `read` se analizan una vez para determinar la tasa de errores de la API ( $270\,000 * 1 = 270\,000$ ).
  - El total de eventos de administración analizados es de 330 000 ( $60\,000 + 270\,000$ ). Tendrá costos por el análisis de 330 000 eventos de administración para este registro de seguimiento. Se le cobrará por separado si habilita Insights para el registro de seguimiento y almacén de datos de eventos.

## Ejemplo 2: habilitar Insights para dos registros de seguimiento

En el siguiente ejemplo, habilita Insights en dos registros de seguimiento, el A y el B. Elige habilitar Insights de la tasa de llamadas a la API solo en el registro de seguimiento A e Insights de la tasa de errores de la API solo en el registro de seguimiento B. Los registros de seguimiento registran los eventos de administración de `read` y de `write`.

- CloudTrail analiza los eventos de administración de `write` que se registraron en los últimos 28 días para formar una referencia. No se cobran cargos de CloudTrail por el análisis.
- Una vez creada la referencia, el registro de seguimiento registra 800 000 eventos de administración, de los cuales 710 000 son eventos de `read` y 90 000 son eventos de `write`.

En el caso del registro de seguimiento A, se produce el siguiente análisis:

- Los eventos de administración de `write` se analizan una vez para determinar la tasa de llamadas a la API ( $90\,000 * 1 = 90\,000$ ).
- Los eventos de administración de `read` no se analizan, ya que CloudTrail solo analiza los eventos de administración de `write` para obtener Insights de la tasa de llamadas a la API.
- El total de eventos de administración analizados es de 90 000. Tendrá costos por el análisis de 90 000 eventos de administración para el registro de seguimiento A.

En el caso del registro de seguimiento B, se produce el siguiente análisis:

- Los eventos de administración de `write` se analizan una vez para determinar la tasa de errores de la API ( $90\,000 * 1 = 90\,000$ ).
- Los eventos de administración de `read` se analizan una vez para determinar la tasa de errores de la API ( $710\,000 * 1 = 710\,000$ ).
- El total de eventos de administración analizados es de 800 000 ( $90\,000 + 710\,000$ ). Tendrá costos por el análisis de 800 000 eventos de administración para el registro de seguimiento B.

Ejemplo 3: habilite Insights para medir la tasa de llamadas a la API y la tasa de errores de la API en un registro de seguimiento y un almacén de datos de eventos

En este último ejemplo, se habilita Insights para medir la tasa de llamadas a la API y la tasa de errores de la API en un registro de seguimiento y un almacén de datos de eventos. Tanto en el registro de seguimiento como en el almacén de datos de eventos permiten registrar del eventos de administración de `read` y de `write`. Se le cobrarán cargos de CloudTrail Insights por el registro de seguimiento y el almacén de datos de eventos por separado, ya que habilitó Insights en ambos.

- CloudTrail analiza los eventos de administración que se registraron en los últimos 28 días para formar una referencia. No se cobran cargos de CloudTrail por el análisis.
- Una vez creada la referencia, el registro de seguimiento y el almacén de datos de eventos registran 500 000 eventos de administración, de los cuales 380 000 son eventos de administración de `read` y 120 000 son eventos de administración de `write`.

En el caso del registro de seguimiento, se produce el siguiente análisis:

- Los eventos de administración de `write` se analizan dos veces para el registro de seguimiento, una para determinar la tasa de llamadas a la API y otra para determinar la tasa de errores de la API ( $120\,000 * 2 = 240\,000$ ).
- Los eventos de administración de `read` se analizan una vez para el registro de seguimiento para determinar la tasa de errores de la API ( $380\,000 * 1 = 380\,000$ ).
- El total de eventos de administración que se analizaron para el registro de seguimiento es de 620 000 ( $240\,000 + 380\,000$ ). Tendrá costos por el análisis de 620 000 eventos de administración para el registro de seguimiento.

En el caso del almacén de datos de eventos, se realiza el siguiente análisis:

- Los eventos de administración de `write` se analizan dos veces para el almacén de datos de eventos, una para determinar la tasa de llamadas a la API y otra para determinar la tasa de errores de la API ( $120\,000 * 2 = 240\,000$ ).

- Los eventos de administración de `read` se analizan una vez para el almacén de datos de eventos para determinar la tasa de errores de la API ( $380\,000 * 1 = 380\,000$ ).
- El total de eventos de administración que se analizaron para el almacén de datos de eventos es de 620 000 (240 000 + 380 000). Tendrá costos por el análisis de 620 000 eventos de administración para el almacén de datos de eventos.

## 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 habilitar CloudTrail Insights por primera vez en un registro de seguimiento, CloudTrail puede tardar hasta 36 horas en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual en ese tiempo.

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, siempre que se detecte una actividad inusual en ese momento.

### 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 habilitar CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights al almacén de datos de eventos de destino, siempre que se detecte actividad inusual en ese tiempo.

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, siempre que se detecte una actividad inusual en ese momento. 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 consola de CloudTrail

En esta sección, se describe cómo puede habilitar eventos de Insights en un registro de seguimiento o un almacén de datos de eventos existentes en la consola de CloudTrail.

Para obtener más información sobre cómo crear un registro de seguimiento nuevo para registrar eventos de Insights, consulte [Creación de un registro de seguimiento con la consola](#).

Para obtener más información sobre cómo crear un almacén de datos de eventos nuevo para recopilar los eventos de Insights, consulte [Creación de un almacén de datos de eventos para los eventos de Insights con la consola](#).

### Temas

- [Habilitación de CloudTrail Insights en un registro de seguimiento existente con la consola](#)
- [Habilitación CloudTrail Insights en un almacén de datos de eventos existente con la consola](#)

## Habilitación de CloudTrail Insights en un registro de seguimiento existente con la consola

Utilice el siguiente procedimiento para habilitar CloudTrail Insights en un registro de seguimiento existente.

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 Eventos de Insights, elija 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 Eventos de Insights, en Elegir los tipos de Insights, elija Tasa de llamada a la API, 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 empezar a entregar los eventos de Insights después de que habilite los eventos de Insights en un registro de seguimiento, siempre que se detecte actividad inusual durante ese tiempo.

## Habilitación CloudTrail Insights en un almacén de datos de eventos existente con la consola

Utilice el siguiente procedimiento para habilitar CloudTrail Insights en un almacén de datos de eventos existente.

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 CloudTrail Insights en los almacenes de datos de eventos que contengan eventos de administración de CloudTrail. No puede habilitar 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 la captura de eventos de Insights.
5. Elija el almacén de eventos de destino que recopilará 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. 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.
7. Elija Guardar cambios para guardar los cambios.

CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual durante ese tiempo.

## Registro de eventos de Insights con la AWS CLI

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 las tasas de llamada 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

- [Registro de eventos de Insights para un registro de seguimiento mediante la AWS CLI](#)
- [Registro de eventos de Insights para un almacén de datos de eventos mediante la AWS CLI](#)

## Registro de eventos de Insights para un registro de seguimiento mediante la AWS CLI

Para volver a los selectores de Insights actuales para un registro de seguimiento, ejecute el comando `get-insight-selectors`.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

En el siguiente ejemplo de respuesta se muestran los selectores de Insights de un registro de seguimiento denominado `insights-trail`.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/insights-trail",
  "InsightSelectors": [
    {
      "InsightType": "ApiCallRateInsight"
    },
    {
      "InsightType": "ApiErrorRateInsight"
    }
  ]
}
```

Si el registro de seguimiento no tiene Insights habilitado, el comando `get-insight-selectors` muestra el siguiente mensaje de error: “Se produjo un error (`InsightNotEnabledException`) al llamar a la operación `GetInsightSelectors`: el registro de seguimiento `arn:aws:cloudtrail:us-east-1:123456789012:trail/trailName` no tiene Insights habilitado. Edite la configuración de la traza para habilitar Insights y, a continuación, vuelva a intentar la operación”.

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.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
  "InsightSelectors":
    [
      {
        "InsightType": "ApiErrorRateInsight"
      }
    ]
}
```

```
    },  
    {  
      "InsightType": "ApiCallRateInsight"  
    }  
  ]  
}
```

## Registro de 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
```

Si un almacén de datos de eventos está configurado para recibir eventos de Insights, la `eventCategory` se configurará en `Insight`.

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 habilitar CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual en ese tiempo.

# Visualización de eventos de Insights para registros de seguimiento

En esta sección, se describe cómo buscar los últimos 90 días de eventos de Insights para un registro de seguimiento con Insights de CloudTrail habilitado. Para obtener información acerca de cómo ver Insights de CloudTrail para un almacén de datos de eventos, consulte [Visualización del panel de Insights de un almacén de datos de eventos](#).

Puede ver, filtrar y descargar los últimos 90 días de eventos de Insights para un registro de seguimiento desde la página Insights de la consola.

Puede buscar los últimos 90 días de los eventos de Insights mediante la programación al ejecutar el comando AWS CLI [lookup-events](#) o la operación de la API [LookupEvents](#).

Para obtener las descripciones de los campos de registro de eventos de Insights para los registros de seguimiento, consulte [CloudTrail registra el contenido de los eventos de Insights para registros de seguimiento](#).

## Note

La página Insights y el comando AWS CLI `lookup-events` solo muestran los eventos de Insights si habilitó Insights en un registro de seguimiento que registra eventos de administración. Para obtener información sobre cómo habilitar Insights en un registro de seguimiento, consulte [Habilitación de CloudTrail Insights en un registro de seguimiento existente con la consola](#) y [Registro de eventos de Insights para un registro de seguimiento mediante la AWS CLI](#).

Para registrar los eventos de Insights sobre el volumen de llamadas a 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

- [Cómo visualizar eventos de Insights para registros de seguimiento con la consola](#)
- [Cómo visualizar eventos de Insights para registros de seguimiento con la AWS CLI](#)

# Cómo visualizar eventos de Insights para registros de seguimiento con la consola

En esta sección se describe cómo ver, buscar y descargar los últimos 90 días de eventos de Insights para un registro de seguimiento desde la página Insights de la consola de CloudTrail. Para obtener información acerca de cómo ver Insights de CloudTrail para un almacén de datos de eventos, consulte [Visualización del panel de Insights de un almacén de datos de eventos](#).

Una vez registrados los eventos de Insights para el registro de seguimiento, estos se muestran en la página Insights durante 90 días. No se pueden eliminar manualmente eventos de la página Insights. Como los eventos de Insights habilitados para un registro de seguimiento se almacenan en el bucket de Amazon S3 configurado para ese registro de seguimiento, al eliminar los eventos de Insights del bucket se eliminarán esos eventos.

Puede monitorear sus registros de seguimiento y recibir notificaciones cuando se produzcan eventos de Insights específicos al habilitar los registros de CloudWatch. Para obtener más información, consulte [Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs](#).

## Note

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 durante ese tiempo. Para registrar los eventos de Insights sobre el volumen de llamadas a 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`.

## Para ver eventos de Insights

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/home/>.
2. En el panel de navegación, elija Insights a fin de ver todos los eventos de Insights registrados en su cuenta en los últimos 90 días. También puede ver los cinco eventos más recientes de Insights en la página de Paneles.



3. En la página de Insights, puede filtrar los eventos de Insights por origen, nombre o ID del evento. Para obtener más información sobre el filtrado de eventos de Insights, consulte [Filtrado de eventos de Insights](#).
4. Puede limitar aún más la lista a un Rango relativo o un Rango absoluto.

## 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

De manera predeterminada, los eventos de la página Insights se muestran en orden cronológico inverso según la hora de inicio del evento.

Puede filtrar la lista mediante el uso de uno de los siguientes tres atributos:

### Nombre de evento

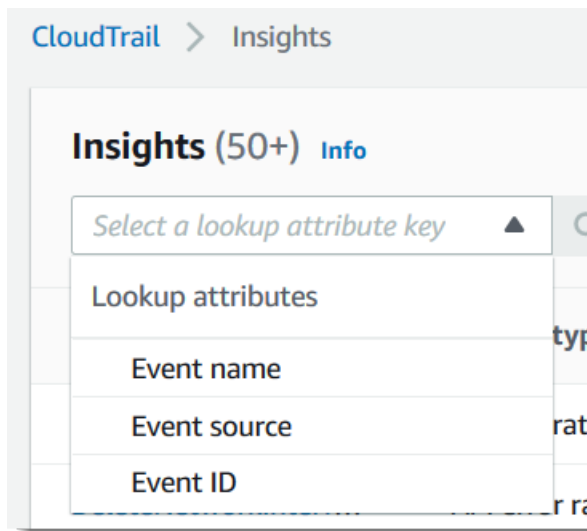
El nombre del evento, normalmente la API de AWS en la que se registraron niveles inusuales de actividad.

### Origen del evento

El servicio de AWS para el que se ha realizado la solicitud, como `iam.amazonaws.com` o `s3.amazonaws.com`. Si elige filtrar por origen de evento, puede desplazarse por una lista de orígenes de eventos.

### 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.



En la siguiente lista se describen los atributos de un evento que no se pueden filtrar:

#### 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.

#### 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

La referencia representa el patrón normal de actividad de tasa de error o de llamadas a la API, calculada de manera diaria. El promedio de referencia es el promedio de estas referencias diarias a lo largo de los siete días anteriores al inicio de un evento de Insights. Si bien este periodo suele ser de siete días, CloudTrail redondea el periodo de cálculo a un número entero de días, por lo que la duración exacta de referencia puede variar ligeramente.

#### 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, luego, escriba o elija un valor en el cuadro 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

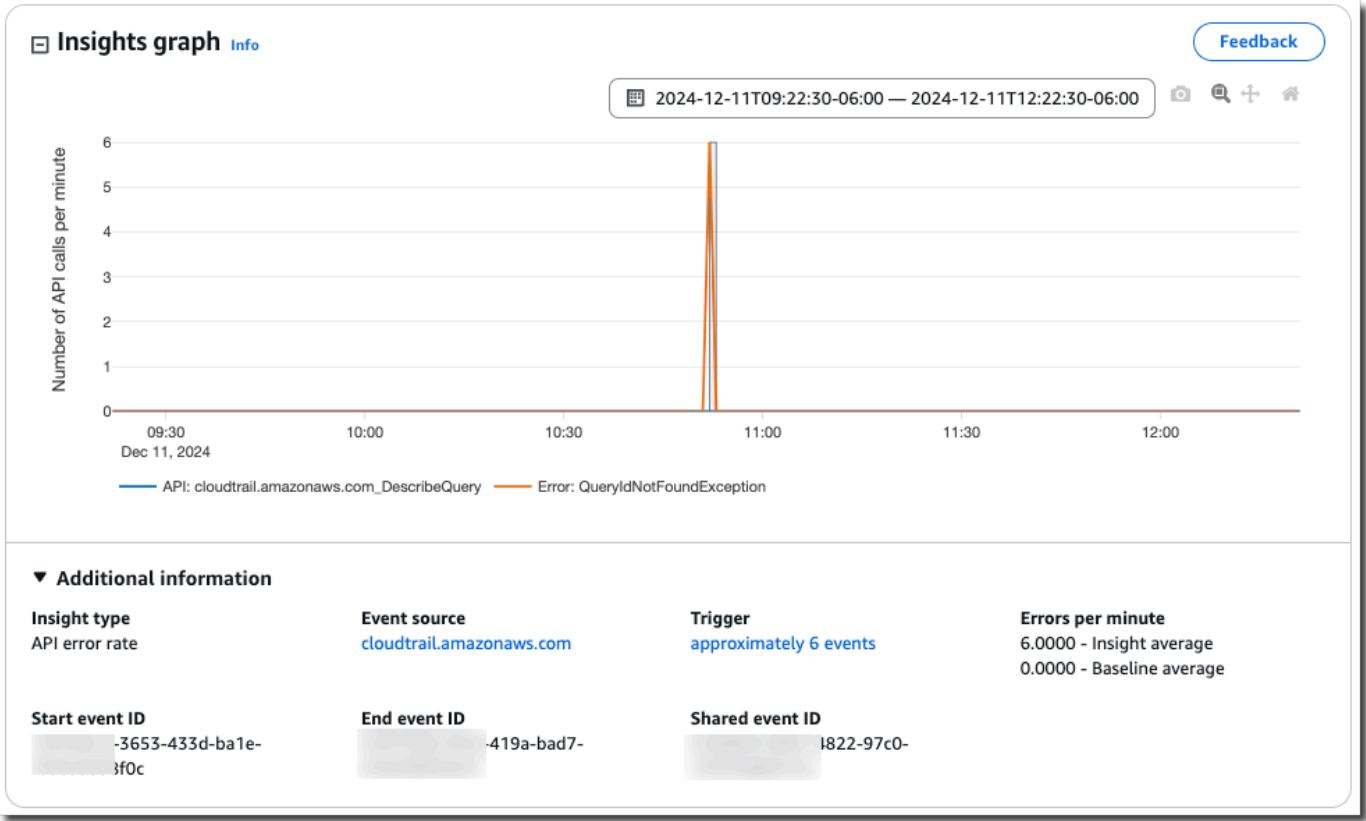
1. En Filtrar por fecha y hora, elija una de las siguientes opciones:
  - Rango absoluto: permite elegir una hora específica. Continúe con el paso siguiente.
  - Rango relativo: se selecciona de manera predeterminada. Permite elegir un periodo de tiempo relativo a la hora de inicio de un evento de Insights. Continúe con el paso 3.
2. Para establecer un Rango absoluto, haga lo siguiente.
  - a. Elija el día en el que desea que comience el rango 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**.

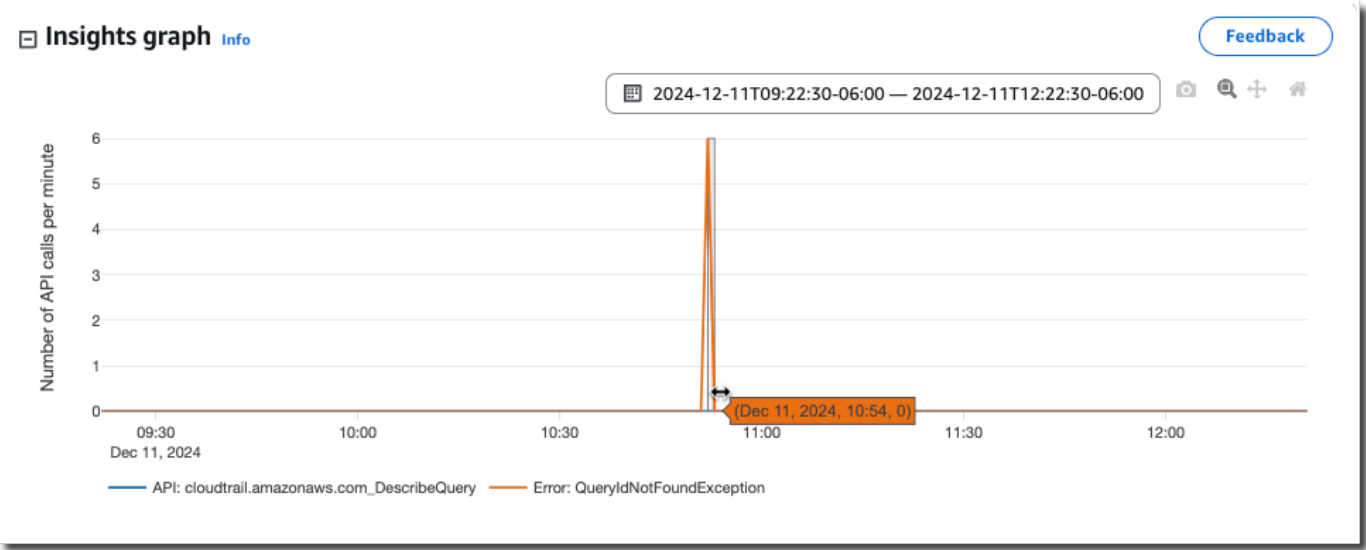
- b. Elija una fecha de finalización para el intervalo en el calendario o especifique una fecha y hora de finalización debajo del calendario. Seleccione Aplicar.
3. Para establecer un Rango relativo, haga lo siguiente.
  - a. Elija un periodo de tiempo predefinido relativo a la hora de inicio de los eventos de Insights. Los intervalos de tiempo preestablecidos incluyen 30 minutos, 1 hora, 12 horas o 1 día. Para especificar un intervalo de tiempo personalizado, elija Custom (Personalizado).
  - b. Cuando haya establecido la hora relativa que desea, elija Apply (Aplicar).
4. Para eliminar un filtro de rango de tiempo, elija el icono de calendario situado a la derecha del cuadro Filtrar por día y hora y, luego, elija Borrar y descartar.

## 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 o Errores 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.
  - **Origen 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.
  - **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.
  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.



2024-12-11T09:22:30-06:00 — 2024-12-11T12:22:30-06:00

## 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 especificar un intervalo de tiempo de las últimas 12 horas de actividad.
2. Elija **Download events** (Descargar eventos) y, a continuación, **Download as CSV** (Descargar como CSV) o **Download as JSON** (Descargar como 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 Cancelar. 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.

## Cómo visualizar eventos de Insights para registros de seguimiento con la AWS CLI

En esta sección se describe cómo utilizar el comando AWS CLI `lookup-events` para buscar los últimos 90 días de eventos de Insights de un registro de seguimiento con los eventos de Insights habilitados. Para obtener información acerca de cómo habilitar Insights de CloudTrail en un registro de seguimiento, consulte [Registro de eventos de Insights para un registro de seguimiento mediante la AWS CLI](#).

### Note

No puede usar el comando `lookup-events` para buscar eventos de Insights para un almacén de datos de eventos; sin embargo, CloudTrail Lake ofrece una serie de consultas de muestra para los almacenes de datos de eventos de Insights. Para obtener más información, consulte [Visualización de consultas de muestra para los eventos de Insights](#).

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 de la AWS Command Line Interface, consulte la [Guía del usuario de AWS Command Line Interface](#).

## 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 comandos de AWS CLI, debe instalar la AWS CLI. Para obtener más información, consulte [Introducción a la AWS CLI](#).
- Asegúrese de que la versión de AWS CLI es posterior a la versión 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 para una sesión de AWS CLI, utilice el comando `aws configure`. 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 a 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 comandos de la AWS CLI de CloudTrail 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
```

## 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": "kb0t5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YA1ju3oXd12juEXAMP
  "Events": [
    {
      "eventVersion": "1.09",
      "eventTime": "2024-12-11T16:52:00Z",
      "awsRegion": "us-east-1",
      "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
      "eventType": "AwsCloudTrailInsight",
      "recipientAccountId": "888888888888",
      "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
      "insightDetails": {
        "state": "Start",
        "eventSource": "cloudtrail.amazonaws.com",
        "eventName": "DescribeQuery",
        "insightType": "ApiErrorRateInsight",
        "errorCode": "QueryIdNotFoundException",
        "insightContext": {
          "statistics": {
            "baseline": {
              "average": 0
            },
            "insight": {
              "average": 1.2
            },
            "insightDuration": 5,
            "baselineDuration": 11092
          },
          "attributions": [
            {
              "attribute": "userIdentityArn",
```

```

        "insight": [
            {
                "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                "average": 1.2
            }
        ],
        "baseline": []
    },
    {
        "attribute": "userAgent",
        "insight": [
            {
                "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                "average": 1.2
            }
        ],
        "baseline": []
    }
]
}
},
"eventCategory": "Insight"
},
{
    "eventVersion": "1.09",
    "eventTime": "2024-12-11T16:53:00Z",
    "awsRegion": "us-east-1",
    "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
    "eventType": "AwsCloudTrailInsight",
    "recipientAccountId": "888888888888",
    "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
    "insightDetails": {
        "state": "End",
        "eventSource": "cloudtrail.amazonaws.com",
        "eventName": "DescribeQuery",
        "insightType": "ApiErrorRateInsight",
        "errorCode": "QueryIdNotFoundException",
        "insightContext": {
            "statistics": {
                "baseline": {
                    "average": 0
                }
            }
        }
    }
},

```

```

        "insight": {
            "average": 6
        },
        "insightDuration": 1,
        "baselineDuration": 11092
    },
    "attributions": [
        {
            "attribute": "userIdentityArn",
            "insight": [
                {
                    "value": "arn:aws:sts::888888888888:assumed-role/Admin",
                    "average": 6
                }
            ],
            "baseline": []
        },
        {
            "attribute": "userAgent",
            "insight": [
                {
                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                    "average": 6
                }
            ],
            "baseline": []
        }
    ]
},
"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 registra el contenido de los eventos de Insights para registros de seguimiento](#).

## 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 de `AttributeValue` es de 2000 caracteres. Los siguientes caracteres («`_`», «`»`, «`,`» y «`\n`») cuentan como dos caracteres en el 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+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqq66b5YGssKutDYIyII4lrP4IDbeQdi0bkp9YAlju3oXd12juEXAMP
```

## Obtener datos de entrada JSON de un archivo

La AWS CLI de algunos servicios de AWS tiene dos parámetros, `--generate-cli-skeleton` y `--cli-input-json`, que puede utilizar para generar una plantilla JSON que se puede modificar y utilizar como datos de entrada en el parámetro `--cli-input-json`. En esta sección se describe cómo utilizar estos parámetros con `aws cloudtrail lookup-events`. Para obtener más información, consulte [Esqueletos y archivos de entrada de AWS CLI](#).

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 este 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

### Events (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 representación de cadena del evento de CloudTrail recuperado.

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 servicio de AWS para el 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 [Trabajar con CloudTrail Insights](#) en esta guía.

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

En esta sección, se describe cómo puede ver los eventos de Insights para un almacén de datos de eventos de Insights mediante la consulta del panel de eventos de Insights y de realizar consultas de ejemplo. Para obtener información acerca de cómo habilitar CloudTrail Insights en un almacén de datos de eventos, consulte [Habilitación CloudTrail Insights en un almacén de datos de eventos existente con la consola](#).

Las consultas de CloudTrail generan cargos según 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. Para obtener más información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

Para obtener las descripciones de los campos de registro de eventos de Insights para los almacenes de datos de eventos, consulte [CloudTrail registra el contenido de los eventos de Insights para los almacenes de datos de eventos](#).

## Temas

- [Visualización del panel de Insights de un almacén de datos de eventos](#)
- [Visualización de consultas de muestra para los eventos de Insights](#)

## Visualización del panel de Insights de un almacén de datos de eventos

En el panel de eventos de Insights se 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 la cantidad de eventos de Insights por día. El panel también incluye un widget que muestra hasta 30 días de eventos de Insights.

### Note

- Después de habilitar CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual durante ese tiempo. Para obtener más información, consulte [Entrega de eventos de Insights](#).
- El Panel de 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`.

Para ver el panel de eventos de Insights

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En los Paneles administrados de AWS, elija el Panel de eventos de Insights.
5. Elija el almacén de datos de eventos de Insights.
6. 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](#).

7. Elija el icono de actualización para completar los gráficos de los widgets del panel. Cada widget indica el estado de la actualización.

Para obtener más información acerca de los paneles de Lake, consulte [Paneles de CloudTrail Lake](#).

## Visualización de consultas de muestra para los eventos de Insights

La consola de CloudTrail brinda una serie de consultas de muestra para los eventos de Insights que pueden ayudarlo a empezar a escribir sus propias consultas.

Para ver las consultas de muestra para los eventos de Insights

1. Inicie sesión en la Consola de administración de AWS 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. Busque las consultas sobre eventos de Insights. Elija el Nombre de la consulta para abrirla en la pestaña Editor.

| Sample queries (202) <a href="#">Info</a>                  |                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="text" value="Insights"/> 5 found              |                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Query name                                                 | Query description                                                                                                 | Query SQL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <a href="#">Top 10 Insights event sources</a>              | Find the top 10 event sources that generated the most Insights events within the past month.                      | <pre>SELECT insightEventSource, -- insightEventName, -- Group by event name COUNT(*) AS eventCount FROM \$INSIGHTS_EDS_ID WHERE insightState = 'End' AND insightType = 'ApiCallRateInsight' -- AND insightType = 'ApiErrorRateInsight' -- Filter on API error rate insights AND eventTime &gt; DATE_ADD('month', -1, CURRENT_TIMESTAMP) GROUP BY insightEventSource -- insightEventName -- Group by event name ORDER BY eventCount DESC LIMIT 10</pre>                                                                                                                  |
| <a href="#">Top 10 Insights event errors</a>               | Find the top 10 errors that generated the most Insights events within the past month.                             | <pre>SELECT insightErrorCode, COUNT(*) AS eventCount FROM \$INSIGHTS_EDS_ID WHERE insightState = 'End' AND insightType = 'ApiCallErrorInsight' AND eventTime &gt; DATE_ADD('month', -1, CURRENT_TIMESTAMP) GROUP BY insightErrorCode ORDER BY eventCount DESC LIMIT 10</pre>                                                                                                                                                                                                                                                                                            |
| <a href="#">Rank the number of Insights events per day</a> | Query the Insights event data store over the past month to rank the number of Insights events generated each day. | <pre>SELECT DATE_TRUNC('day', eventTime) AS eventDate, COUNT(*) AS eventCount, DENSE_RANK() OVER( ORDER BY COUNT(*) DESC ) AS eventRank FROM \$INSIGHTS_EDS_ID WHERE insightState = 'End' AND insightType = 'ApiCallRateInsight' -- AND insightType = 'ApiErrorRateInsight' -- Filter on API error rate insights AND eventTime &gt; DATE_ADD('month', -1, CURRENT_TIMESTAMP) GROUP BY DATE_TRUNC('day', eventTime) ORDER BY eventRank</pre>                                                                                                                             |
| <a href="#">Investigate Insights events</a>                | Find all CloudTrail management events that generated an Insights event.                                           | <pre>SELECT * FROM \$EDS_ID AS me INNER JOIN ( SELECT awsRegion, recipientAccountId, insightEventSource, insightEventName, MIN(eventTime) AS insight_start, MAX(eventTime) AS insight_end FROM \$INSIGHTS_EDS_ID WHERE sharedEventID = '&lt;sharedEventID&gt;' GROUP BY 1, 2, 3, 4 ) AS ie ON me.awsRegion = ie.awsRegion AND me.recipientAccountId = ie.recipientAccountId AND me.eventSource = ie.insightEventSource AND me.eventName = ie.insightEventName AND me.eventTime &gt;= ie.insight_start AND me.eventTime &lt;= ie.insight_end ORDER BY me.eventTime</pre> |
| <a href="#">Insights events caused by a user</a>           | Find all Insights events caused by a particular user within the past month.                                       | <pre>SELECT sharedEventID, eventTime, insightType, insightEventSource AS eventSource, insightEventName AS eventName, insightcontext.attributes [1].insightvalue AS user FROM \$INSIGHTS_EDS_ID WHERE insightState = 'End' AND insightcontext.attributes [1].insightvalue LIKE '%&lt;username&gt;%' AND eventTime &gt; DATE_ADD('month', -1, CURRENT_TIMESTAMP) ORDER BY eventTime DESC</pre>                                                                                                                                                                            |

- En la pestaña Editor, elija el almacén de datos de eventos de Insights. Al seleccionar el almacén de datos de eventos de la lista, CloudTrail rellena automáticamente el ID del almacén de datos de eventos en la línea FROM del editor de consultas.
- Seleccione Ejecutar para ejecutar la consulta. Una vez que se complete la consulta, podrá ver el resultado del comando y los resultados de 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 con la consola de CloudTrail](#). Para obtener más información sobre cómo ejecutar una consulta y guardar los resultados, consulte [Ejecutar una consulta y guardar los resultados de la consulta con la consola](#).

# Trabajar con AWS CloudTrail Lake

AWS CloudTrail Lake le permite ejecutar consultas basadas en SQL sobre sus eventos.

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 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 los eventos que perduran y están disponibles para la consulta. CloudTrail Lake es una solución de auditoría que puede complementar su pila de conformidad y ayudarlo a resolver problemas casi en tiempo real.

## Almacenes de datos de eventos de CloudTrail Lake

Cuando crea un almacén de datos de eventos, elige el tipo de eventos que desea incluir en él. Puede crear un almacén de datos de eventos para que incluya los [eventos de CloudTrail](#) (eventos de administración, de datos y de actividad de la red), los [eventos de CloudTrail Insights](#), los [elementos de configuración de AWS Config](#), las [pruebas de AWS Audit Manager](#) o los [eventos externos a AWS](#). Cada almacén de datos de eventos solo puede contener una categoría de eventos específica (por ejemplo, elementos de configuración de AWS Config), ya que el [esquema de eventos](#) de cada categoría es único. Puede almacenar eventos de una organización en 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 registro de seguimiento en un almacén de datos de eventos nuevo o existente para crear una instantánea puntual de los eventos registrados en el registro de seguimiento. 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 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](#).

Puede asociar una política basada en recursos a su almacén de datos de eventos para ofrecer acceso entre cuentas a las entidades principales seleccionadas. Puede agregar una política basada en recursos al crear o actualizar un almacén de datos de eventos en la consola de CloudTrail o al ejecutar el comando AWS CLI `put-resource-policy`. Para obtener más información, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

De forma predeterminada, CloudTrail cifra todos los eventos que se encuentran en un almacén de datos de eventos. Cuando configure un almacén de datos de eventos, puede optar por utilizar su propia 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. 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.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

CloudTrail Lake es compatible con las métricas de Amazon CloudWatch, que proporcionan información sobre los datos incorporados y los bytes de almacenamiento. Para obtener más información acerca de las métricas de Amazon CloudWatch admitidas, consulte [Métricas de CloudWatch admitidas](#).

#### Note

En general, CloudTrail envía eventos en un plazo de 5 minutos tras una llamada a la API. No hay garantía de que suceda en este plazo.



# Consultas de CloudTrail Lake

Las consultas de CloudTrail Lake ofrecen una visión más detallada y personalizable de los eventos que las simples búsquedas de claves y valores en el Event history (Historial de eventos), o ejecutando `LookupEvents`. La búsqueda en el Event history (Historial de eventos) está limitada a una sola Cuenta de AWS y solo devuelve eventos de una única Región de AWS; además, no se pueden 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 funciones e instrucciones `SELECT` de Trino válidas. Para obtener más información acerca de los operadores y las funciones SQL compatibles, consulte [Funciones y operadores](#) en el sitio web de documentación de Trino.

Puede crear una consulta en la pestaña Editor de CloudTrail Lake mediante la escritura de la consulta en SQL desde cero, la apertura de una consulta guardada o de muestra y su edición, o mediante el generador de consultas para crear una consulta a partir de una petición redactada en inglés. Para obtener más información, consulte [Creación o edición de una consulta con la consola de CloudTrail](#) y [Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural](#).

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

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 con la consola de CloudTrail](#).

Las consultas de CloudTrail Lake incurren en cargos. 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 [Administración de los costos de CloudTrail Lake](#).

## Paneles de CloudTrail Lake

Puede usar los paneles de CloudTrail Lake para consultar las tendencias de eventos de los almacenes de datos de eventos de la cuenta. CloudTrail Lake ofrece los siguientes tipos de paneles:

- Paneles administrados: puede ver un panel administrado para ver las tendencias de eventos de un almacén de datos de eventos que recopila eventos de administración, de datos o de Insights. Estos paneles están disponibles de manera automática y CloudTrail Lake los administra.

CloudTrail ofrece 14 paneles administrados entre los que puede elegir. Puede actualizar de manera manual los paneles administrados. No puede modificar, agregar ni eliminar los widgets de estos paneles; sin embargo, puede guardar un panel administrado como un panel personalizado si quiere modificar los widgets o establecer un programa de actualización.

- **Paneles personalizados:** estos le permiten consultar eventos en cualquier tipo de almacén de datos de eventos. Puede agregar hasta 10 widgets a un panel personalizado. Puede actualizar de manera manual un panel personalizado o puede establecer un programa de actualización.
- **Paneles destacados:** habilite el panel de aspectos destacados para ver un resumen rápido de la actividad recopilada de AWS por los almacenes de datos de eventos de la cuenta. CloudTrail administra el panel de aspectos destacados e incluye widgets que son pertinentes para la cuenta. Los widgets que se muestran en el panel de aspectos destacados son únicos para cada cuenta. Estos widgets podrían mostrar la actividad anormal o las anomalías detectadas. Por ejemplo, en el panel de aspectos destacados se podría incluir el Widget de acceso entre cuentas total, que muestra si hay un aumento en la actividad anormal entre cuentas. CloudTrail actualiza el panel de aspectos destacados cada 6 horas. En el panel se muestran los datos de las últimas 24 horas de la última actualización.

Cada panel consta de uno o más widgets y cada uno representa una consulta SQL.

Para obtener más información, consulte [Paneles de CloudTrail Lake](#).

## Integraciones de CloudTrail Lake

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. Después de crear almacenes de datos de eventos en CloudTrail Lake y crear un canal para registrar eventos de actividad, llame a la API `PutAuditEvents` para ingerir la actividad de la aplicación en CloudTrail. A continuación, puede utilizar CloudTrail Lake para buscar, consultar y analizar los datos que se registran de las aplicaciones.

Las integraciones también pueden registrar eventos en los almacenes de datos de eventos de más de una docena de socios de CloudTrail. 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 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.

Para obtener más información sobre las integraciones, consulte [Crear una integración con un origen de eventos externo a AWS](#).

## Recursos adicionales

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)
- [Analizar los registros de actividad con AWS CloudTrail Lake y Amazon Athena](#) (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](#)
- [AWS CloudTrail Referencia de la API de](#)
- [AWS CloudTrail Referencia de la API de datos de](#)
- [AWS CloudTrail Guía de incorporación de socios de](#)

## 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 |

| Nombre de la región       | Región         |
|---------------------------|----------------|
| Oeste de EE. UU. (Oregón) | us-west-2      |
| África (Ciudad del Cabo)  | af-south-1     |
| Asia-Pacífico (Hong Kong) | ap-east-1      |
| Asia-Pacífico (Hyderabad) | ap-south-2     |
| Asia-Pacífico (Yakarta)   | ap-southeast-3 |
| Asia-Pacífico (Melbourne) | ap-southeast-4 |
| Asia-Pacífico (Bombay)    | ap-south-1     |
| Asia-Pacífico (Osaka)     | ap-northeast-3 |
| Asia-Pacífico (Seúl)      | ap-northeast-2 |
| Asia-Pacífico (Singapur)  | ap-southeast-1 |
| Asia-Pacífico (Sídney)    | ap-southeast-2 |
| Asia-Pacífico (Tokio)     | ap-northeast-1 |
| Canadá (centro)           | ca-central-1   |
| Europa (Fráncfort)        | eu-central-1   |
| Europa (Irlanda)          | eu-west-1      |
| Europa (Londres)          | eu-west-2      |
| Europa (Milán)            | eu-south-1     |
| Europa (París)            | eu-west-3      |
| Europa (España)           | eu-south-2     |
| Europa (Estocolmo)        | eu-north-1     |

| Nombre de la región            | Región        |
|--------------------------------|---------------|
| Europa (Zúrich)                | eu-central-2  |
| Israel (Tel Aviv)              | il-central-1  |
| Medio Oriente (Baréin)         | me-south-1    |
| Medio Oriente (EAU)            | me-central-1  |
| América del Sur (São Paulo)    | sa-east-1     |
| AWS GovCloud (Este de EE. UU.) | us-gov-east-1 |
| AWS GovCloud (Oeste de EE.UU.) | us-gov-west-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 el uso de CloudTrail en las AWS GovCloud (US) Regions, consulte [Service Endpoints](#) 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](#)
- [Paneles](#)

## 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 CloudTrail](#) (eventos de administración, de datos y de actividad de la red), 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 los eventos de administración, eventos de datos y eventos de actividad de la red, puede utilizar selectores de eventos avanzados para filtrar los 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

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 Administración de los costos de CloudTrail Lake](#).

## 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.

## Protección de finalización

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 [Cambio de la protección contra la terminación con la consola](#).

# 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 [AWS CloudTrailEjemplos de políticas basadas en recursos de](#) .



## Consultas

Las consultas de CloudTrail Lake se crean en SQL. Puede crear una consulta en la pestaña Editor de CloudTrail Lake mediante la escritura de la consulta en SQL desde cero, la apertura de una consulta guardada o de muestra y su edición, o mediante el generador de consultas para crear una consulta a partir de una petición redactada en inglés. Para obtener más información, consulte [Creación o edición de una consulta con la consola de CloudTrail](#) y [Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural](#).

CloudTrail Lake admite todas las funciones e instrucciones SELECT de Trino válidas. Para obtener más información acerca de los operadores y funciones SQL compatibles, consulte [Funciones y operadores](#) en el sitio web de documentación de Trino.

## Paneles

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 Servicios de AWS, usuarios y errores principales. Para obtener más información, consulte [Paneles de CloudTrail Lake](#).

### Tipos de paneles

CloudTrail Lake ofrece los siguientes tipos de paneles:

- **Paneles administrados:** puede ver un panel administrado para ver las tendencias de eventos de un almacén de datos de eventos que recopila eventos de administración, de datos o de Insights. Estos paneles están disponibles de manera automática y CloudTrail Lake los administra. CloudTrail ofrece 14 paneles administrados entre los que puede elegir. Puede actualizar de manera manual los paneles administrados. No puede modificar, agregar ni eliminar los widgets de estos paneles; sin embargo, puede guardar un panel administrado como un panel personalizado si quiere modificar los widgets o establecer un programa de actualización.
- **Paneles personalizados:** estos le permiten consultar eventos en cualquier tipo de almacén de datos de eventos. Puede agregar hasta 10 widgets a un panel personalizado. Puede actualizar de manera manual un panel personalizado o puede establecer un programa de actualización.
- **Paneles destacados:** habilite el panel de aspectos destacados para ver un resumen rápido de la actividad recopilada de AWS por los almacenes de datos de eventos de la cuenta. CloudTrail administra el panel de aspectos destacados e incluye widgets que son pertinentes para la cuenta. Los widgets que se muestran en el panel de aspectos destacados son únicos para cada cuenta. Estos widgets podrían mostrar la actividad anormal o las anomalías detectadas.

Por ejemplo, en el panel de aspectos destacados se podría incluir el Widget de acceso entre cuentas total, que muestra si hay un aumento en la actividad anormal entre cuentas. CloudTrail actualiza el panel de aspectos destacados cada 6 horas. En el panel se muestran los datos de las últimas 24 horas de la última actualización.

## Widgets

Los widgets son los componentes que forman parte de un panel y ofrecen una visualización, como un gráfico de líneas o de barras. Cada widget corresponde a una consulta SQL. Cuando se actualiza un panel, CloudTrail ejecuta una consulta para cada widget del panel a fin de completar los datos del widget.

## Almacenes de datos de eventos de CloudTrail Lake

Cuando crea un almacén de datos de eventos en CloudTrail Lake, elige el tipo de eventos que desea incluir en él. Puede crear un almacén de datos de eventos para que incluya los eventos de CloudTrail (eventos de administración, de datos o de actividad de la red), los eventos de CloudTrail Insights, los elementos de configuración de AWS Config o los eventos ajenos a AWS. Cada tipo de almacén de datos de eventos solo puede contener categorías de eventos específicas (por ejemplo, elementos de configuración de AWS Config), ya que el esquema de eventos de cada categoría es único. 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                                                                                                                                                                                                                                                       |
|--------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eventos de CloudTrail    | Management          | Este tipo de almacén de datos de eventos puede recopilar eventos de administración, de datos de actividad de la red de CloudTrail. Para obtener más información, consulte <a href="#">Creación de un almacén de datos de eventos para eventos de CloudTrail</a> . |
|                          | Data                |                                                                                                                                                                                                                                                                   |
|                          | NetworkActivity     |                                                                                                                                                                                                                                                                   |

| Tipo de evento (consola)       | eventCategory (API) | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eventos de CloudTrail Insights | Insight             | Este tipo de almacén de datos de eventos puede recopilar eventos de CloudTrail Insights. Para recibir eventos de Insights, necesita un <a href="#">almacén de datos de eventos de origen</a> que registre los eventos de administración de CloudTrail y habilite Insights. Para obtener información sobre la creación de los almacenes de datos de eventos de origen y destino, consulte <a href="#">Creación de un almacén de datos de eventos para eventos de CloudTrail Insights</a> . |
| Elementos de configuración     | ConfigurationItem   | Este tipo de almacén de datos de eventos puede recopilar elementos de configuración de AWS Config. Para obtener más información, consulte <a href="#">Creación de un almacén de datos de eventos para los elementos de configuración de AWS Config</a> .                                                                                                                                                                                                                                  |
| Eventos de integración         | ActivityAuditLog    | Este tipo de almacén de datos de eventos puede recopilar eventos que no son de AWS de integraciones. Para obtener más información, consulte <a href="#">Creación de un almacén de datos de eventos para eventos externos a AWS</a> .                                                                                                                                                                                                                                                      |

También puede crear un almacén de datos de eventos para evidencia de AWS Audit Manager mediante la consola de Audit Manager. Para obtener más información sobre cómo agregar evidencia en CloudTrail Lake con Audit Manager, consulte [Cómo funciona el buscador de evidencia con CloudTrail Lake](#) en la Guía del usuario de AWS Audit Manager.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

Las siguientes secciones describen cómo crear, actualizar y eliminar almacenes de datos de eventos.

## Temas

- [Creación, actualización y administración de almacenes de datos de eventos con la consola](#)
- [Creación, actualización y administración de almacenes de datos de eventos con la AWS CLI](#)
- [Administración de los ciclos de vida de los almacenes de datos de eventos](#)
- [Copiar eventos de registro de seguimiento en un almacén de datos de eventos](#)
- [Federar un almacén de datos de eventos](#)
- [Descripción de los almacenes de datos de eventos de la organización](#)

## Creación, actualización y administración de almacenes de datos de eventos con la consola

Puede usar la consola de CloudTrail para crear, actualizar, eliminar y restaurar almacenes de datos de eventos.

Puede actualizar la siguiente configuración mediante la consola de CloudTrail:

- Puede cambiar la [opción de precio](#) de precio de retención de siete años a un precio de retención ampliable por un año.
- Puede actualizar 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.
- Puede convertir un almacén de datos de eventos multirregión en un almacén de datos de eventos de una sola región o viceversa.
- La cuenta de administración de una organización de AWS Organizations puede convertir un almacén de datos de eventos a nivel de cuenta en un almacén de datos de eventos de la organización o viceversa. Esta configuración no está disponible en los almacenes de datos de eventos que recopilan eventos externos a AWS.
- Puede activar o desactivar la [federación de consultas de Lake](#). La federación de un almacén de datos de eventos le permite consultar los datos de sus eventos desde Amazon Athena.

- Puede agregar o editar la política basada en recursos de un almacén de datos de eventos para ofrecer acceso entre cuentas al almacén de datos de eventos. Para obtener más información, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).
- Puede [detener la ingesta de eventos](#) y reiniciarla en los almacenes de datos de eventos que recopilan eventos de datos y de administración de CloudTrail o elementos de configuración de AWS Config.
- Puede habilitar o deshabilitar la [protección contra la terminación](#). Habilitar la protección contra la terminación impide que un almacén de datos de eventos se elimine accidentalmente. La protección contra la terminación está habilitada de forma predeterminada.
- Puede [restaurar](#) un almacén de datos de eventos que esté pendiente de eliminación.
- Puede agregar o eliminar 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.
- Puede agregar una clave de KMS para cifrar su almacén de datos de eventos. No puede eliminar una clave de KMS de un almacén de datos de eventos.

El uso de la consola de CloudTrail para crear o actualizar un almacén de datos de eventos ofrece las siguientes ventajas:

- Si va a configurar un almacén de datos de eventos para recopilar eventos de datos, usar la consola de CloudTrail le permite ver los tipos de recursos de eventos de datos disponibles. Para obtener más información, consulte [Registro de eventos de datos](#).
- Si está configurando un almacén de datos de eventos para recopilar los eventos de actividad de la red, usar la consola de CloudTrail le permite ver los orígenes de los eventos para los que puede registrar los eventos de actividad de la red. Para obtener más información, consulte [Registro de eventos de actividad de la red](#).
- En caso de que esté configurando un almacén de datos de eventos para recopilar los eventos externos a AWS, la consola de CloudTrail le permite ver información acerca de los socios disponibles. Para obtener más información, consulte [Creación de un almacén de datos de eventos para eventos externos a AWS con la consola](#).

## Temas

- [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#)
- [Creación de un almacén de datos de eventos para los eventos de Insights con la consola](#)
- [Creación de un almacén de datos de eventos para los elementos de configuración con la consola](#)

- [Creación de un almacén de datos de eventos para eventos externos a AWS con la consola](#)
- [Actualización de un almacén de datos de eventos con la consola](#)
- [Detención e inicio de la ingesta de eventos con la consola](#)
- [Cambio de la protección contra la terminación con la consola](#)
- [Eliminar un almacén de datos de eventos con la consola](#)
- [Restaurar un almacén de datos de eventos con la consola](#)

## Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola

Los almacenes de datos de eventos para eventos de CloudTrail pueden incluir eventos de administración de CloudTrail, eventos de datos y eventos de actividad de la red. 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.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

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

Utilice este procedimiento para crear un almacén de datos de eventos que registre los eventos de administración de CloudTrail, los eventos de datos o los eventos de actividad de la red.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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. 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.

 Note

Si está copiando eventos de registros de seguimiento en este almacén de datos de eventos, CloudTrail no copiará un evento si el valor de `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 conservar los eventos en el almacén de datos de eventos (periodo de retención = *el evento más antiguo en días* más *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.

7. (Opcional) Para habilitar el cifrado con AWS Key Management Service, elija Utilizar clave de AWS KMS key propia. Elija New (Nueva) si desea que se cree una AWS KMS key para usted, o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de claves para permitir que se cifre y descifre el almacén de datos de eventos de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.
11. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
12. En la página Elegir eventos, elija Eventos de AWS y, a continuación, Eventos de CloudTrail.
13. En CloudTrail events (Eventos de CloudTrail), elija al menos un tipo de evento. De forma predeterminada, se selecciona la opción Management events (Eventos de administración). Puede agregar [eventos de administración](#), [eventos de datos](#) y [eventos de actividad de red](#) a su almacén de datos de eventos.
14. (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](#).
15. 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.

16. Expanda la opción Configuración adicional para elegir si desea que su almacén de datos de eventos recopile los eventos de todas las Regiones de AWS o solo las Región de AWS actuales, y elija si desea que el almacén de datos de eventos ingiera 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.
17. 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 entre la Recopilación de eventos simple o la Recopilación de eventos avanzada:
    - Elija la Recopilación de eventos simple si desea registrar todos los eventos, registrar solo los eventos de lectura o solo los eventos de escritura. También tiene la opción de elegir excluir los eventos de AWS Key Management Service y la API de datos de Amazon RDS.
    - Elija la Recopilación avanzada de eventos si desea incluir o excluir los eventos de administración en función de los valores de los campos del selector de eventos avanzado, como los campos eventName, eventType, eventSource, sessionCredentialFromConsole y userIdentity.arn.
  - b. Si seleccionó la Recopilación de eventos simple, elija si quiere registrar todos los eventos, registrar solo los eventos de lectura o registrar solo los eventos de escritura. También tiene la opción de elegir excluir los eventos de AWS KMS y la API de datos de Amazon RDS.
  - c. Si seleccionó la Recopilación de eventos avanzada, realice las siguientes selecciones:

- i. En la Plantilla de selector de registros, elija una plantilla predefinida o Personalizada para crear una configuración personalizada basada en los valores de los campos del selector de eventos avanzado.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
  - Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
  - Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
  - Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
  - Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).
- ii. (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 administración de las sesiones de la Consola de administración de AWS”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
  - iii. Si eligió Personalizado, en los Selectores de eventos avanzados cree una expresión basada en los valores de los campos del selector de eventos avanzado.

 Note

Los selectores no admiten el uso de caracteres comodín como `*`. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

A. Elija uno de los siguientes campos.

- **readOnly**: readOnly se puede establecer en igual a un valor true o false. Cuando se establece en false, el almacén de datos de eventos registra los eventos de administración de solo escritura. Los eventos de administración de solo lectura son eventos que no cambian el estado de un recurso, como los eventos Get\* o Describe\*. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos Put\*, Delete\* o Write\*. Para registrar los eventos de Lectura y Escritura, no agregue un selector de readOnly.
  - **eventName** – eventName puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de administración, como CreateAccessPoint o GetAccessPoint.
  - **userIdentity.arn**: incluya o excluya los eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
  - **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de Consola de administración de AWS. Este campo se puede establecer como igual o no igual con un valor true.
  - **eventSource**: puede usarlo para incluir o excluir los orígenes de eventos específicos. El eventSource suele ser una forma abreviada del nombre del servicio sin espacios más .amazonaws.com. Por ejemplo, podría establecer el valor eventSource igual a ec2.amazonaws.com para registrar solo los eventos de administración de Amazon EC2.
  - **eventType**: el [Tipo de evento](#) que se va a incluir o excluir. Por ejemplo, puede establecer este campo en no igual a AwsServiceEvent para excluir los [eventos de Servicio de AWS](#).
- B. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- C. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
- iv. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
- d. Seleccione Habilitar la captura de eventos de Insights para activar 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. 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.
18. Para incluir eventos de datos en su almacén de datos de eventos, haga lo siguiente.
- a. Elija un tipo de recurso. Este es el Servicio de AWS y el recurso en los que se registran los eventos de datos.

- b. En la Plantilla de selección de registros, elija una plantilla predefinida o una Personalizada para definir sus propias condiciones de recopilación de eventos en función de los valores de los campos del selector de eventos avanzado.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
  - Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
  - Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
  - Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
  - Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).
- 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. Si seleccionó Personalizado, en los selectores de eventos avanzados cree una expresión basada en los valores de los campos del selector de eventos avanzado.

 Note

Los selectores no admiten el uso de caracteres comodín como `*`. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

- i. Elija uno de los siguientes campos.

- **readOnly**: `readOnly` se puede establecer en `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 utilizarlo para incluir o excluir cualquier evento de datos registrado en CloudTrail, como `PutBucket`, `GetItem` o `GetSnapshotBlock`.
- **eventSource**: el origen del evento que se va a incluir o excluir. Este campo puede utilizar cualquier operador.
- **eventType**: el tipo de evento que se va a incluir o excluir. Por ejemplo, puede establecer este campo en `not equal to AwsServiceEvent` para excluir [Servicio de AWSEventos de](#) . Para obtener una lista de los tipos de eventos, consulte [eventType](#) en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).
- **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de la Consola de administración de AWS. Este campo se puede establecer como `equal to` o `not equal to` con un valor `true`.
- **userIdentity.arn**: incluya o excluya los eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- **resources.ARN**: puede utilizar cualquier operador con `resources.ARN`, pero si utiliza `equal to` o `not equal to`, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo especificado en la plantilla como el valor de `resources.type`.

 **Note**

No puede usar el campo `resources.ARN` para filtrar los tipos de recursos que no tienen ARN.



Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte [Acciones, recursos y claves de condición para los Servicios de AWS](#) en la Referencia de autorizaciones de servicio.

- ii. 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 eventos de datos de dos buckets de S3 de los eventos de datos registrados en su almacén de datos de eventos, puede establecer el campo en resources.ARN, configurar el operador en no comienza por y, a continuación, pegar un ARN de bucket 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.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- iii. 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.
- e. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
  - f. Para agregar otro tipo de recurso en el que registrar eventos de datos, elija Agregar tipo de evento de datos. Repita los pasos hasta este paso a fin de configurar los selectores de eventos avanzados para el tipo de recursos.
19. Para incluir eventos de actividad de la red en su almacén de datos de eventos, haga lo siguiente.
- a. En Origen de eventos de actividad de la red, seleccione el origen de los eventos de actividad de la red.

- b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede optar por registrar todos los eventos de actividad de la red, registrar todos los eventos de acceso denegado a la actividad de la red o seleccionar Personalizar para crear un selector de registro personalizado que filtre por varios campos, como `eventName` y `vpcEndpointId`.
  - c. (Opcional) Escriba un nombre para identificar el selector. El nombre del selector aparece como Nombre en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
  - d. En Selectores de eventos avanzados, cree expresiones mediante la selección de valores para Campo, Operador y Valor. Puede omitir este paso si utiliza una plantilla de registro predefinida.
    - i. Para excluir o incluir eventos de actividad de la red, puede elegir entre los siguientes campos de la consola.
      - **eventName** – puede utilizar cualquier operador con `eventName`. Puede utilizarlo para incluir o excluir cualquier evento, como `CreateKey`.
      - **errorCode** – puede usarlo para filtrar por un código de error. Actualmente, el único `errorCode` que se admite es `VpceAccessDenied`.
      - **vpcEndpointId** – identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con `vpcEndpointId`.
    - ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.
    - iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
  - e. Para agregar otro origen de eventos de actividad de la red que quiera registrar, seleccione Agregar selector de eventos de actividad de la red.
  - f. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
20. 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 los eventos de CloudTrail contenidos en el prefijo `CloudTrail` del bucket de S3 y los prefijos dentro del prefijo `CloudTrail` y no comprueba los prefijos de otros servicios

de AWS. Si desea copiar los eventos de CloudTrail contenidos en otro prefijo, elija Enter S3 URI (Introducir la URI de S3) y, a continuación, elija Browse S3 (Examinar S3) para buscar el prefijo. Si el bucket de S3 de origen para el registro de seguimiento usa una clave de KMS para el cifrado de datos, verifique que la política de la clave de KMS permite a CloudTrail descifrar los datos. Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave de manera que permitan a CloudTrail descifrar los datos en el 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 registro para comprobar que el nombre contenga una fecha situada entre la fecha de inicio y la fecha de finalización elegidas antes de intentar copiar los eventos del registro 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 registros de seguimiento que tengan un valor de `eventTime` dentro del periodo de retención del almacén de datos de eventos. Por ejemplo, si el periodo de retención de un almacén de datos de eventos es de 90 días, CloudTrail no copiará ningún evento de registro de seguimiento con un valor de `eventTime` anterior a 90 días.

- Si elige Intervalo relativo, puede elegir si desea copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un intervalo personalizado. CloudTrail copia los eventos registrados dentro del periodo seleccionado.
  - Si selecciona Absolute range (Intervalo absoluto), puede elegir fechas de inicio y de finalización específicas. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y de finalización seleccionadas.
- 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 **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.
  - Seleccione **Usar 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.
  - Elija un rol de IAM existente de la lista desplegable.
21. Elija **Siguiente** para enriquecer los eventos si agrega claves de etiquetas de recurso y claves de condición global de IAM.
22. En **Eventos enriquecidos** agregue hasta 50 claves de etiqueta de recurso y 50 claves de condición global de IAM para ofrecer metadatos adicionales sobre los eventos. Esto le ayuda a clasificar y agrupar los eventos relacionados.

Si agrega claves de etiqueta de recurso, CloudTrail incluirá las claves de las etiquetas seleccionadas asociadas a los recursos que han participado en la llamada a la API. Los eventos de la API relacionados con recursos eliminados no tendrán etiquetas de recurso.

Si agrega claves de condición global de IAM, CloudTrail incluirá información sobre las claves de condición seleccionadas que se evaluaron durante el proceso de autorización, como detalles adicionales sobre la entidad principal, la sesión, la red y la propia solicitud.

La información sobre las claves de etiqueta de recurso y las claves de condición global de IAM se muestra en el campo `eventContext` del evento. Para obtener más información, consulte [Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM](#).

 **Note**

Si un evento contiene un recurso que no pertenece a la región del evento, CloudTrail no completará las etiquetas de este recurso porque la recuperación de etiquetas se limita a la región del evento.

23. Seleccione **Expandir el tamaño del evento** para ampliar la carga útil del evento de 256 KB a 1 MB. Esta opción se activa de manera automática al agregar claves de etiqueta de recurso o

claves de condición global de IAM para garantizar que todas las claves agregadas se incluyan en el evento.

Ampliar el tamaño del evento es útil para analizar y solucionar problemas de eventos, ya que permite ver el contenido completo de los siguientes campos siempre que la carga útil del evento sea inferior a 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Para obtener más información sobre estos campos, consulte [Contenido de los registros de CloudTrail](#).

24. Elija Next (Siguiente) para revisar las opciones seleccionadas.
25. 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).
26. 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 con la consola de CloudTrail](#).

También puede ver los [paneles administrados](#) o [crear paneles personalizados](#) para visualizar las tendencias de los eventos. Para obtener más información acerca de los paneles de Lake, consulte [Paneles de CloudTrail Lake](#).

## Creación de un almacén de datos de eventos para los eventos de Insights con la consola

AWS CloudTrail Insights ayuda a los usuarios de AWS a identificar y responder a la actividad inusual asociada a las tasas de llamada 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 tasas de llamada a la API y tasas de error de la API, también conocido como valor de referencia, y genera eventos de Insights cuando el volumen de llamadas o tasa de error se encuentra fuera de los patrones normales. Los eventos de Insights en las tasas de llamada a la API se generan para las API de administración de `write` y los eventos de Insights en la tasa de errores de la 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 almacén de datos de eventos de origen que habilite Insights y registre los eventos de administración.

### Note

Para registrar los eventos de Insights sobre las tasas de llamada 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 las tasas de errores de la API, el almacén de datos de eventos de origen debe registrar los eventos de administración de `read` o `write`.

Si ha habilitado CloudTrail Insights en un almacén de datos de eventos de origen y CloudTrail detecta actividad inusual, CloudTrail entrega los eventos de Insights en el almacén de datos de eventos de destino. A diferencia de otros tipos de eventos capturados en un almacén de datos de eventos 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.

Después de habilitar CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual durante ese tiempo.

CloudTrail Insights analiza los eventos de administración que se producen en cada región para el almacén de datos de eventos y genera un evento de Insights cuando se detecta una actividad inusual que se desvía del valor de referencia. El evento de CloudTrail Insights se genera en la misma región en la que se genera el evento de administración correspondiente.

En el caso de un almacén de datos de eventos de la organización, CloudTrail Insights analiza los eventos de administración de cada cuenta de miembro en la organización para cada región y genera un evento de Insights cuando se detecta una actividad inusual que se desvía del valor de referencia de la cuenta y la región.

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 los almacenes de datos de eventos de CloudTrail Lake. Para obtener información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## 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 Consola de administración de AWS y abra la consola de CloudTrail 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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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 con AWS Key Management Service, elija Utilizar clave de AWS KMS key propia. Elija New (Nueva) si desea que se cree una AWS KMS key para usted, o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de claves para permitir que se cifre y descifre el



almacén de datos de eventos de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar

qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.

11. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
12. En la página Elegir eventos, elija Eventos de AWS y, a continuación, Eventos de CloudTrail Insights.
13. En 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 organización de AWS Organizations.
  - 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.
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.
17. 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 Consola de administración de AWS y abra la consola de CloudTrail 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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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. 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.

7. (Opcional) Para habilitar el cifrado con AWS Key Management Service, elija Utilizar clave de AWS KMS key propia. Elija New (Nueva) si desea que se cree una AWS KMS key para usted, o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de claves para permitir que se cifre y descifre el almacén de datos de eventos de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de

datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.
11. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
12. En la página Elegir eventos, elija Eventos de AWS y, a continuación, Eventos de CloudTrail.
13. En Eventos de CloudTrail, deje seleccionados los Eventos de administración.

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). Debe iniciar sesión en la cuenta de administración de la organización para crear un almacén de datos de eventos que habilite Insights.
15. Expanda la opción **Configuración adicional** para elegir si desea que su almacén de datos de eventos recopile los eventos de todas las Regiones de AWS o solo las Región de AWS actuales, y elija si desea que el almacén de datos de eventos ingiera 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.
16. Elija entre la **Recopilación de eventos simple** o la **Recopilación de eventos avanzada**:
  - Elija la **Recopilación de eventos simple** si desea registrar todos los eventos, registrar solo los eventos de lectura o solo los eventos de escritura. También tiene la opción de elegir excluir los eventos de AWS Key Management Service y la API de datos de Amazon RDS.
  - Elija la **Recopilación avanzada de eventos** si desea incluir o excluir los eventos de administración en función de los valores de los campos del selector de eventos avanzado, como los campos `eventName`, `eventType`, `eventSource`, `sessionCredentialFromConsole` y `userIdentity.arn`.
17. Si seleccionó la **Recopilación de eventos simple**, elija si quiere registrar todos los eventos, registrar solo los eventos de lectura o registrar solo los eventos de escritura. También tiene la opción de elegir excluir los eventos de AWS KMS y la API de datos de Amazon RDS.
18. Si seleccionó la **Recopilación de eventos avanzada**, realice las siguientes selecciones:
  - a. En la **Plantilla de selección de registros**, elija una plantilla predefinida o una **Personalizada** para escribir sus propias condiciones de recopilación de eventos en función de los valores de los campos del selector de eventos avanzado.

Puede elegir entre las siguientes plantillas predefinidas:

- **Registrar todos los eventos**: elija esta plantilla para registrar todos los eventos.



- Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
  - Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
  - Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
  - Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).
- b. (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 administración de las sesiones de la Consola de administración de AWS”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
- c. Si eligió Personalizado, en los Selectores de eventos avanzados cree una expresión basada en los valores de los campos del selector de eventos avanzado.

 Note

Los selectores no admiten el uso de caracteres comodín como `*`. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

- i. Elija uno de los siguientes campos.
- **readOnly**: `readOnly` se puede establecer en igual a un valor `true` o `false`. Cuando se establece en `false`, el almacén de datos de eventos registra los eventos de administración de solo escritura. Los eventos de administración de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`. Para registrar los eventos de Lectura y Escritura, no agregue un selector de `readOnly`.

- **eventName** – eventName puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de administración, como CreateAccessPoint o GetAccessPoint.
  - **userIdentity.arn**: incluya o excluya los eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
  - **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de Consola de administración de AWS. Este campo se puede establecer como igual o no igual con un valor true.
  - **eventSource**: puede usarlo para incluir o excluir los orígenes de eventos específicos. El eventSource suele ser una forma abreviada del nombre del servicio sin espacios más .amazonaws.com. Por ejemplo, podría establecer el valor eventSource igual a ec2.amazonaws.com para registrar solo los eventos de administración de Amazon EC2.
  - **eventType**: el [Tipo de evento](#) que se va a incluir o excluir. Por ejemplo, puede establecer este campo en no igual a AwsServiceEvent para excluir los [eventos de Servicio de AWS](#).
- ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
- d. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.

## 19. Seleccione Habilitar la captura de eventos de Insights.

20. 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](#).
21. 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.
22. Elija Siguiente para enriquecer los eventos si agrega claves de etiquetas de recurso y claves de condición global de IAM.
23. En Enriquecer eventos agregue hasta 50 claves de etiqueta de recurso y 50 claves de condición global de IAM para ofrecer metadatos adicionales sobre los eventos. Esto le ayuda a clasificar y agrupar los eventos relacionados.

Si agrega claves de etiqueta de recurso, CloudTrail incluirá las claves de las etiquetas seleccionadas asociadas a los recursos que han participado en la llamada a la API. Los eventos de la API relacionados con recursos eliminados no tendrán etiquetas de recurso.

Si agrega claves de condición global de IAM, CloudTrail incluirá información sobre las claves de condición seleccionadas que se evaluaron durante el proceso de autorización, como detalles adicionales sobre la entidad principal, la sesión, la red y la propia solicitud.

La información sobre las claves de etiqueta de recurso y las claves de condición global de IAM se muestra en el campo eventContext del evento. Para obtener más información, consulte [Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM](#).

 Note

Si un evento contiene un recurso que no pertenece a la región del evento, CloudTrail no completará las etiquetas de este recurso porque la recuperación de etiquetas se limita a la región del evento.

24. Seleccione Expandir el tamaño del evento para ampliar la carga útil del evento de 256 KB a 1 MB. Esta opción se activa de manera automática al agregar claves de etiqueta de recurso o

claves de condición global de IAM para garantizar que todas las claves agregadas se incluyan en el evento.

Ampliar el tamaño del evento es útil para analizar y solucionar problemas de eventos, ya que permite ver el contenido completo de los siguientes campos siempre que la carga útil del evento sea inferior a 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Para obtener más información sobre estos campos, consulte [Contenido de los registros de CloudTrail](#).

25. Elija Next (Siguiente) para revisar las opciones seleccionadas.
26. 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).
27. 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. Después de habilitar CloudTrail Insights por primera vez en el almacén de datos de eventos de origen, CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual durante ese tiempo.

También puede ver el panel de CloudTrail Lake para ver los eventos de Insights del almacén de datos de eventos de destino. Para obtener más información acerca de los paneles de Lake, consulte [Paneles de CloudTrail Lake](#).

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](#).

## Creación de un almacén de datos de eventos para los elementos de configuración con la consola

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 vista puntual en el tiempo de los atributos de un recurso compatible de AWS que existe en su cuenta. AWS Config crea un elemento de configuración cada vez que detecta un cambio en un tipo de recurso que registra. AWS Config también crea elementos de configuración cuando se captura una instantánea de configuración.

Puede usar tanto AWS Config como CloudTrail Lake para ejecutar consultas en sus elementos de configuración. Puede utilizar AWS Config para consultar el estado de configuración actual de los recursos de AWS en función de las propiedades de configuración de una sola Cuenta de AWS y Región de AWS o de varias cuentas y regiones. Por el contrario, puede usar CloudTrail Lake para consultar diversos orígenes de datos, como eventos de CloudTrail, elementos de configuración y evaluaciones de reglas. Las consultas de CloudTrail Lake cubren todos los elementos de configuración de AWS Config, incluidos la configuración de los recursos y el historial de cumplimiento.

La creación de un almacén de datos de eventos para los elementos de configuración no afecta a las consultas avanzadas de AWS Config existentes ni a ningún agregador configurado de AWS Config. Puede seguir ejecutando consultas avanzadas con AWS Config. AWS Config continuará enviando archivos de historial a los buckets de S3.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

## 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 su almacén de datos de eventos, configure el registro de AWS Config para todas sus cuentas y regiones. Puede usar [Quick Setup](#), una capacidad de AWS Systems Manager, para crear rápidamente un registrador de configuraciones basado en AWS Config.

### Note

Se le cobrarán las tarifas de uso del servicio cuando AWS Config comience a registrar 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 desea que utilice AWS Config para evaluar la información de conformidad para los tipos de recursos registrados. Varias de las consultas de muestra de CloudTrail Lake para AWS Config requieren que Reglas de AWS Config evalúe el estado de cumplimiento de sus recursos de AWS. Para obtener más información sobre Reglas de AWS Config, consulte [Evaluación de recursos con Reglas de AWS Config](#) en la Guía para desarrolladores de AWS Config.

Para crear un almacén de datos de eventos para elementos de configuración

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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. 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.

7. (Opcional) Para habilitar el cifrado con AWS Key Management Service, elija Utilizar clave de AWS KMS key propia. Elija New (Nueva) si desea que se cree una AWS KMS key para usted, o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de claves para permitir que se cifre y descifre el almacén de datos de eventos de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.
11. Elija Siguiente.
12. En la página Elegir eventos, elija Eventos de AWS y, a continuación, Elementos de configuración.
13. CloudTrail almacena el recurso del almacén de datos de eventos en la región en la que usted lo crea, pero, de forma predeterminada, los elementos de configuración recopilados en el almacén de datos son de todas las regiones de su cuenta que tienen habilitado el registro. 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.
14. Para que su almacén de datos de eventos recopile elementos de configuración 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 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.
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.

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.

## 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 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 registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

- [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          | Obligatorio | La versión del formato del evento de AWS.                                                            |
| eventCategory    | cadena          | Obligatorio | La categoría del evento. Para los elementos de configuración, el valor válido es ConfigurationItem . |

| Nombre del campo   | Tipo de entrada | Requisito   | Descripción                                                                                                                                                                                                   |
|--------------------|-----------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| eventType          | cadena          | Obligatorio | Tipo de evento. Para los elementos de configuración, el valor válido es <code>AwsConfigurationItem</code> .                                                                                                   |
| eventID            | cadena          | Obligatorio | El ID único de un evento.                                                                                                                                                                                     |
| eventTime          | cadena          | Obligatorio | La marca de tiempo del evento, en formato <code>yyyy-MM-DDTHH:mm:ss</code> , en Hora Universal Coordinada (UTC).                                                                                              |
| awsRegion          | cadena          | Obligatorio | La Región de AWS a la que se debe asignar un evento.                                                                                                                                                          |
| recipientAccountId | cadena          | Obligatorio | Representa el ID de la Cuenta de AWS que recibió este evento.                                                                                                                                                 |
| addendum           | addendum        | Opcional    | Muestra información 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                      | -               | Obligatorio | Los elementos de configuración proporcionan los campos de eventData .                                                                                          |
| • configurationItemVersion     | cadena          | Opcional    | La versión del elemento de configuración desde su origen.                                                                                                      |
| • configurationItemCaptureTime | 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 identificador de 12 dígitos de la Cuenta de AWS asociado al recurso.                                                                                        |
| • resourceType                 | cadena          | Opcional    | Tipo de recurso de AWS. Para obtener                                                                                                                           |

| Nombre del campo       | Tipo de entrada | Requisito | Descripción                                                                                                                                   |
|------------------------|-----------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|                        |                 |           | más información acerca de los tipos de recursos válidos, consulte <a href="#">ConfigurationItem</a> en la referencia de la API de AWS Config. |
| • 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  | La Región de AWS donde está ubicado 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.                                                                                              |
| • configuration        | JSON            | Opcional  | La descripción de la configuración del recurso.                                                                                               |

| Nombre del campo             | Tipo de entrada | Requisito | Descripción                                                                                                                                                    |
|------------------------------|-----------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • supplementaryConfiguration | JSON            | Opcional  | Atributos de configuración que devuelve AWS Config para que ciertos tipos de recursos complementen la información devuelta para el parámetro de configuración. |
| • relatedEvents              | cadena          | Opcional  | La lista de ID de eventos de CloudTrail.                                                                                                                       |
| • relationships              | -               | Opcional  | La lista de los recursos de AWS relacionados.                                                                                                                  |
| • • nombre                   | cadena          | Opcional  | El tipo de relación con el recurso relacionado.                                                                                                                |
| • • resourceType             | cadena          | Opcional  | El tipo del recurso relacionado.                                                                                                                               |
| • • resourceId               | cadena          | Opcional  | El ID del recurso relacionado (por ejemplo, sg- <b>xxxxxx</b> ).                                                                                               |
| • • resourceName             | cadena          | Opcional  | El nombre personalizado del recurso relacionado, si está disponible.                                                                                           |

| Nombre del campo | Tipo de entrada | Requisito | Descripción                                                                    |
|------------------|-----------------|-----------|--------------------------------------------------------------------------------|
| • 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
}
}
```

## Creación de un almacén de datos de eventos para eventos externos a AWS con la consola

Puede crear un almacén de datos de eventos para incluir eventos externos a AWS y luego, utilizar CloudTrail Lake para buscar, consultar y analizar los datos que se registran desde las aplicaciones.

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.

Cuando crea un almacén de datos de eventos para una integración, también crea un canal y asocia una política de recursos al canal.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

Para crear un almacén de datos de eventos para eventos externos a AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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. 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.

7. (Opcional) Para habilitar el cifrado con AWS Key Management Service, elija Utilizar clave de AWS KMS key propia. Elija New (Nueva) si desea que se cree una AWS KMS key para usted,

o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de claves para permitir que se cifre y descifre el almacén de datos de eventos de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.

11. Elija Next (Siguiente) para configurar el almacén de datos de eventos.
12. En la página Choose events (Elegir eventos), elija Events from integrations (Eventos de integraciones).
13. En Events from integration (Eventos de integraciones), elija el origen para enviar eventos al almacén de datos de eventos.
14. 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.
15. 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.

**External ID**

Enter the unique account identifier provided by Nordcloud. [How to find this?](#) 

 **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 cada cuenta de AWS que se agregará como entidad principal en la política.
16. Elija *Next* (Siguiendo) para revisar las opciones seleccionadas.
17. 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).
18. El nuevo almacén de datos de eventos aparece en la tabla *Almacenes de datos de eventos* de la página *Almacenes de datos de eventos*.
19. 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 ingerir eventos de socios en CloudTrail a través del canal de la integración cuando usted, el socio o las aplicaciones asociadas llaman a la API `PutAuditEvents` del canal.

## Actualización de un almacén de datos de eventos con la consola

En esta sección, se describe cómo actualizar la configuración de un almacén de datos de eventos mediante la Consola de administración de AWS. Para obtener información acerca de cómo actualizar

un almacén de datos de eventos con la 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 en la Consola de administración de AWS y abra la consola de CloudTrail 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 [Administración de los costos de CloudTrail Lake](#).

 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 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.

- 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, CloudTrail cifra todos los eventos que se encuentran en un almacén de datos de eventos. 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 organización de AWS Organizations, seleccione Activar en 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 para el almacén de datos de eventos es Eventos de CloudTrail 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. [La habilitación de la federación de consultas de Lake](#) le permite ver los metadatos del almacén de datos de eventos en el [Catálogo de datos de AWS Glue](#) y ejecutar consultas SQL en los datos del evento mediante Amazon Athena. [La deshabilitación de la federación de consultas de Lake](#) 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 CloudTrail Lake.



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. Cuando crea un nuevo rol, CloudTrail crea automáticamente uno 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. En la **Política de recursos**, elija **Editar** para agregar o revisar la política basada en recursos para el almacén de datos de eventos.

Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

7. Edite cualquier configuración adicional específica del Tipo de evento del almacén de datos de eventos.

### Configuración de eventos de CloudTrail

- Para cambiar los eventos que registra su almacén de datos de eventos, seleccione Editar en Eventos de CloudTrail.
- En Eventos de administración, elija Editar para cambiar la configuración de registro de eventos de administración. Para obtener más información, consulte [Actualización de la configuración de eventos de administración de un almacén de datos de eventos existente](#).
- En Eventos de datos, elija Editar para cambiar la configuración de los eventos de datos. Puede elegir qué tipos de recursos quiere registrar y elegir la plantilla de selección de registros que quiere usar. Para obtener más información, consulte [Actualizar un almacén de datos de eventos existente para registrar los eventos de datos mediante la consola](#).
- En Eventos de actividad de la red, seleccione Editar para modificar la configuración de los eventos de actividad de la red. Puede elegir qué tipo de evento de actividad de la red quiere registrar y elegir la plantilla del selector de registros que quiere usar. Para obtener más información, consulte [Actualización de un almacén de datos de eventos existente para registrar los eventos de actividad de red](#).
- En Enriquecer eventos, ampliar el tamaño del evento, elija Editar para agregar o eliminar las etiquetas de recursos y las claves de condición global de IAM, y amplíe el tamaño del evento.

En Enriquecer eventos agregue hasta 50 claves de etiqueta de recurso y 50 claves de condición global de IAM para ofrecer metadatos adicionales sobre los eventos. Esto le ayuda a clasificar y agrupar los eventos relacionados.

Si agrega claves de etiqueta de recurso, CloudTrail incluirá las claves de las etiquetas seleccionadas asociadas a los recursos que han participado en la llamada a la API. Los eventos de la API relacionados con recursos eliminados no tendrán etiquetas de recurso.

Si agrega claves de condición global de IAM, CloudTrail incluirá información sobre las claves de condición seleccionadas que se evaluaron durante el proceso de autorización, como detalles adicionales sobre la entidad principal, la sesión, la red y la propia solicitud.

La información sobre las claves de etiqueta de recurso y las claves de condición global de IAM se muestra en el campo `eventContext` del evento. Para obtener más información, consulte [Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM](#).

 Note

Si un evento contiene un recurso que no pertenece a la región del evento, CloudTrail no completará las etiquetas de este recurso porque la recuperación de etiquetas se limita a la región del evento.

Seleccione Expandir el tamaño del evento para ampliar la carga útil del evento de 256 KB a 1 MB. Esta opción se activa de manera automática al agregar claves de etiqueta de recurso o claves de condición global de IAM para garantizar que todas las claves agregadas se incluyan en el evento.

Ampliar el tamaño del evento es útil para analizar y solucionar problemas de eventos, ya que permite ver el contenido completo de los siguientes campos siempre que la carga útil del evento sea inferior a 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`

- `requestParameters`
- `errorMessage`

Para obtener más información sobre estos campos, consulte [Contenido de los registros de CloudTrail](#).

Cuando haya finalizado, elija Guardar cambios.

## Configuración de los eventos a partir de la integración

En Integraciones, elija su integración. Luego elija Editar, para cambiar la siguiente configuración:

- 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 socio de CloudTrail con la consola](#).

8. 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.

## Detención e inicio de la ingesta de eventos con la consola

De forma predeterminada, los almacenes de datos de eventos están configurados para ingerir eventos. Puede evitar que un almacén de datos de eventos ingiera eventos mediante la consola, la AWS CLI o las API.

Las opciones Iniciar ingesta y Detener ingesta solo están disponibles en los almacenes de datos de eventos que contienen eventos de CloudTrail (eventos de administración, de datos y de actividad de la red) o elementos de configuración de AWS Config.

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 registros de seguimiento en el almacén de datos de eventos (si solo contiene eventos de CloudTrail).

Para evitar que un almacén de datos de eventos ingiera eventos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 Consola de administración de AWS y abra la consola de CloudTrail 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.

## Cambio de la protección contra la terminación con la consola

De forma predeterminada, los almacenes de datos de eventos en AWS CloudTrail Lake están configurados con la protección contra la 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 contra la terminación mediante la Consola de administración de AWS, AWS CLI u operaciones de la API.

Para desactivar la protección contra la terminación

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 Save. Ahora puede [eliminar el almacén de datos de eventos](#).

Para activar la protección contra la terminación

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 Save.

## Eliminar un almacén de datos de eventos con la consola

En esta sección, se describe cómo eliminar un almacén de datos de eventos mediante la consola de CloudTrail. Para obtener información acerca de cómo eliminar un almacén de datos de eventos con la AWS CLI, consulte [Eliminar 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 contra la 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 obtener 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 en la Consola de administración de AWS y abra la consola de CloudTrail 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, seleccione 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. Los almacenes de datos de eventos que están pendientes de eliminación se tienen en cuenta para la cuota de almacenes de datos de eventos que pueden existir en una Región de AWS.

## Restaurar un almacén de datos de eventos con la consola

Después de eliminar un almacén de datos de eventos en AWS CloudTrail Lake, su estado cambia a `PENDING_DELETION` y permanece en ese estado durante 7 días. Durante este tiempo, puede restaurar el almacén de datos de eventos mediante Consola de administración de AWS, AWS CLI o la operación [RestoreEventDataStore](#) de la API.

En esta sección, se describe cómo restaurar un almacén de datos de eventos mediante la consola. Para obtener información acerca de cómo restaurar un almacén de datos de eventos con la AWS CLI, consulte [Restaurar un almacén de datos de eventos con la AWS CLI](#).

### Para restaurar un almacén de datos de eventos

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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.

## Creación, actualización y administración de almacenes de datos de eventos con la AWS CLI

En esta sección se describen los comandos de la AWS CLI que puede usar para crear, actualizar y administrar sus almacenes de datos de eventos de CloudTrail Lake.

Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la Región de AWS 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.

### Comandos disponibles para los almacenes de datos de eventos

Los comandos para crear y actualizar almacenes de datos de eventos en CloudTrail Lake son:

- [create-event-data-store](#) para crear un almacén de datos de eventos.
- [get-event-data-store](#) para devolver información acerca del almacén de datos de eventos, incluidos los selectores de eventos avanzados configurados para dicho almacén.
- [update-event-data-store](#) para cambiar la configuración de un almacén de datos de eventos existente.
- [list-event-data-stores](#) para enumerar los almacenes de datos de eventos.
- [delete-event-data-store](#) para eliminar un almacén de datos de eventos.
- [restore-event-data-store](#) para restaurar un almacén de datos de eventos que está pendiente de eliminación.
- [start-import](#) para iniciar una importación de eventos de registro de seguimiento en un almacén de datos de eventos, o volver a intentar realizar una importación errónea.
- [get-import](#) para devolver información acerca de una importación específica.
- [stop-import](#) para detener una importación de eventos de registro de seguimiento a un almacén de datos de eventos.
- [list-imports](#) para devolver información sobre todas las importaciones o un conjunto seleccionado de importaciones realizadas por `ImportStatus` o `Destination`.
- [list-import-failures](#) para enumerar los errores de la importación especificada.
- [stop-event-data-store-ingestion](#) para detener la ingesta de eventos en un almacén de datos de eventos.



- [start-event-data-store-ingestion](#) para reiniciar la ingesta de eventos en un almacén de datos de eventos.
- [enable-federation](#) para permitir la federación en un almacén de datos de eventos y consultarlo en Amazon Athena.
- [disable-federation](#) para deshabilitar la federación en un almacén de datos de eventos. Tras deshabilitar la federación, ya no podrá consultar los datos del almacén de datos de eventos en Amazon Athena. Puede seguir realizando consultas en CloudTrail Lake.
- [put-insight-selectors](#) para agregar o modificar selectores de eventos de Insights para un almacén de datos de eventos existente, y habilitar o deshabilitar los eventos de Insights.
- [get-insight-selectors](#) para devolver información sobre los selectores de eventos de Insights configurados para un almacén de datos de eventos.
- [add-tags](#) para agregar una o varias etiquetas (pares clave-valor) a un almacén de datos de eventos existente.
- [remove-tags](#) para eliminar una o varias etiquetas de un almacén de datos de eventos.
- [list-tags](#) para devolver una lista de etiquetas asociadas a un almacén de datos de eventos.
- [get-event-configuration](#) para devolver las claves de etiqueta de recursos y las claves de condición global de IAM configuradas para el almacén de datos de eventos. El comando también indica si el almacén de datos de eventos está configurado para recopilar eventos de tamaño Standard o eventos de tamaño Large.
- [put-event-configuration](#) para ampliar el tamaño del evento y agregar o eliminar claves de etiqueta de recursos y claves de condición global de IAM. Para obtener más información, consulte [Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM](#).
- [put-resource-policy](#) para asociar una política basada en recursos a un almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).
- [get-resource-policy](#) para asociar la política basada en recursos a un almacén de datos de eventos.
- [delete-resource-policy](#) para eliminar la política basada en recursos a un almacén de datos de eventos.

Para obtener una lista de los comandos disponibles para las consultas de CloudTrail Lake, consulte [Comandos disponibles para consultas de CloudTrail Lake](#).

Para obtener una lista de los comandos disponibles para los paneles de CloudTrail Lake, consulte [Comandos disponibles para los paneles](#).

Para obtener una lista de los comandos disponibles para las integraciones de CloudTrail Lake, consulte [Comandos disponibles para las integraciones de CloudTrail Lake](#).

## Crear un almacén de datos de eventos con la AWS CLI

En esta sección se describe cómo usar el comando [create-event-data-store](#) para crear un almacén de datos de eventos y se ofrecen ejemplos de los distintos tipos de almacenes de datos de eventos que se pueden crear.

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 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.

Ejemplos:

- [Crear un almacén de datos de eventos para eventos de datos de S3 con la AWS CLI](#)
- [Creación de un almacén de datos de eventos para eventos de actividad de la red de KMS 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"
}

```

Creación de un almacén de datos de eventos para eventos de actividad de la red de KMS con la AWS CLI

En el ejemplo siguiente, se muestra cómo crear un almacén de datos de eventos para que incluya eventos de actividad de la red `VpceAccessDenied` para AWS KMS. En este ejemplo, se establece el campo `errorCode` igual a los eventos `VpceAccessDenied` y el campo `eventSource` igual a `kms.amazonaws.com`.

```

aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",

```

```

        "Equals": ["VpceAccessDenied"]
      }
    ]
  }
]'

```

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": "Audit AccessDenied AWS KMS events over a VPC endpoint",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "NetworkActivity"
          ]
        },
        {
          "Field": "eventSource",
          "Equals": [
            "kms.amazonaws.com"
          ]
        },
        {
          "Field": "errorCode",
          "Equals": [
            "VpceAccessDenied"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "RetentionPeriod": 366,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",

```

```
"UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Para obtener más información sobre los eventos de actividad de la red, consulte [Registro de eventos de actividad de la red](#).

Crear un almacén de datos de eventos para los elementos de configuración de AWS 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 habilitar CloudTrail Insights por primera vez en un almacén de datos de eventos, CloudTrail puede tardar hasta 7 días en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual durante ese tiempo.

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

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, cómo importar los eventos a ese almacén de datos de eventos mediante el comando [start-import](#). Para obtener más información acerca de cómo importar eventos de registro de seguimiento, consulte [Copiar eventos de registro de seguimiento en un almacén de datos de eventos](#).

### Cómo 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 comando [list-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
```

## Actualizar un almacén de datos de eventos con la AWS CLI

En esta sección, se ofrecen ejemplos que muestran cómo actualizar la configuración de un almacén de datos de eventos mediante la ejecución del comando `update-event-data-store` de la AWS CLI.

Ejemplos:

- [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 [Administración de los costos de CloudTrail Lake](#).

### 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"
}
```

## Administración de almacenes de datos de eventos con la AWS CLI

En esta sección se describen otros comandos que puede ejecutar para obtener información sobre los almacenes de datos de eventos, iniciar y detener la ingesta en un almacén de datos de eventos y habilitar y deshabilitar la [federación](#) en un almacén de datos de eventos.

### Temas

- [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](#)
- [Agregue claves de etiqueta de recurso y claves de condición global de IAM y amplíe el tamaño del evento.](#)
- [Obtenga la configuración de eventos de un almacén de datos de eventos](#)
- [Obtenga la política basada en recursos para un almacén de datos de eventos con el AWS CLI](#)
- [Asocie una política basada en recursos a un almacén de datos de eventos con el AWS CLI](#)
- [Elimine la política basada en recursos asociada a un almacén de datos de eventos con el 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](#)
- [Restaurar un almacén de datos de eventos con la AWS CLI](#)

## 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:::amzn-s3-demo-bucket"
          ]
        }
      ]
    }
  ]
}
```



```

        ]
      },
      {
        "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"
    }
  ]
}

```

Agregue claves de etiqueta de recurso y claves de condición global de IAM y amplíe el tamaño del evento.

Ejecute el comando AWS CLI `put-event-configuration` para ampliar el tamaño máximo del evento y agregue hasta 50 claves de etiqueta de recurso y 50 claves de condición global de IAM para ofrecer metadatos adicionales sobre los eventos.

El comando `put-event-configuration` acepta los argumentos siguientes:

- `--event-data-store`: especifique el ARN del almacén de datos de eventos o el sufijo de ID del ARN. Este parámetro es obligatorio.
- `--max-event-size`: configúrelo en `Large` para establecer el tamaño máximo del evento en 1 MB. De manera predeterminada, el valor es `Standard`, que especifica un tamaño máximo de evento de 256 KB.

#### Note

Para agregar claves de etiqueta de recurso o claves de condición global de IAM, debe establecer el tamaño del evento en `Large` para garantizar que todas las claves agregadas se incluyan en el evento.

- `--context-key-selectors`: especifique el tipo de claves que quiere incluir en los eventos recopilados por el almacén de datos de eventos. Puede incluir claves de etiquetas de recursos y claves de condición global de IAM. La información sobre las etiquetas de recurso agregadas y las

claves de condición global de IAM se muestra en el campo `eventContext` en el evento. Para obtener más información, consulte [Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM](#).

- Defina el `Type` a `TagContext` para pasar una matriz de hasta 50 claves de etiqueta de recurso. Si agrega etiquetas de recurso, los eventos de CloudTrail incluirán las claves de las etiquetas seleccionadas asociadas a los recursos que han participado en la llamada a la API. Los eventos de la API relacionados con recursos eliminados no tendrán etiquetas de recurso.
- Configure el `Type` a `RequestContext` para pasar una matriz de hasta 50 claves de condición global de IAM. Si agrega claves de condición global de IAM, los eventos de CloudTrail incluirán información sobre las claves de condición seleccionadas que se evaluaron durante el proceso de autorización, como detalles adicionales sobre la entidad principal, la sesión, la red y la propia solicitud.

En el siguiente ejemplo, se establece el tamaño máximo del evento en `Large` y se agregan dos claves de etiqueta de recurso `myTagKey1` y `myTagKey2`.

```
aws cloudtrail put-event-configuration \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE \  
--max-event-size Large \  
--context-key-selectors '[{"Type":"TagContext", "Equals":["myTagKey1","myTagKey2"]}']'
```

En el siguiente ejemplo, se establece el tamaño máximo del evento en `Large` y se agrega una clave de condición global de IAM (`aws:MultiFactorAuthAge`).

```
aws cloudtrail put-event-configuration \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE \  
--max-event-size Large \  
--context-key-selectors '[{"Type":"RequestContext", "Equals":  
["aws:MultiFactorAuthAge"]}']'
```

El último ejemplo elimina todas las claves de etiqueta de recurso y las claves de condición global de IAM y establece el tamaño máximo del evento en `Standard`.

```
aws cloudtrail put-event-configuration \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE \  
--max-event-size Standard
```

```
--max-event-size Standard \  
--context-key-selectors
```

Obtenga la configuración de eventos de un almacén de datos de eventos

Ejecute el comando AWS CLI `get-event-configuration` para regresar a la configuración de eventos de un almacén de datos de eventos que recopila los eventos de CloudTrail. Este comando regresa el tamaño máximo del evento y muestra las claves de etiqueta de recurso y las claves de condición global de IAM (si las hubiera) que se incluyen en los eventos de CloudTrail.

```
aws cloudtrail get-event-configuration \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Obtenga la política basada en recursos para un almacén de datos de eventos con el AWS CLI

En el siguiente ejemplo se ejecuta el comando `get-resource-policy` en un almacén de datos de eventos de la organización.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-  
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

Como el comando se ejecutó en un almacén de datos de eventos de la organización, el resultado mostrará tanto la política basada en recursos que se brindó como la [DelegatedAdminResourcePolicy](#) generada para las cuentas de los administradores delegados.

Asocie una política basada en recursos a un almacén de datos de eventos con el AWS CLI

Para ejecutar las consultas en un panel durante una actualización manual o programada, debe asociar una política basada en recursos a cada almacén de datos de eventos que esté asociado a un widget en el panel. Esto permite a CloudTrail Lake ejecutar las consultas en su nombre. Para obtener más información sobre la política basada en recursos, consulte [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#).

En el siguiente ejemplo, se asocia una política basada en recursos a un almacén de datos de eventos que permite a CloudTrail ejecutar consultas en un panel cuando se lo actualiza. La política se crea en un archivo independiente, *policy.json*, con el siguiente ejemplo de declaración de la política:

## JSON

```
{ "Version": "2012-10-17",      "Statement": [{ "Sid": "EDSPolicy", "Effect":
    "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
event_data_store_ID",
    "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
    { "AWS:SourceArn":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE",
    "AWS:SourceAccount": "123456789012" } } } ] }
```

Reemplace *123456789012* por su ID de cuenta, *arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/event\_data\_store\_ID* con el ARN de un almacén de datos de eventos para el que CloudTrail ejecutará las consultas, y *arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE* con el ARN del panel.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy file://policy.json
```

Lo que sigue es un ejemplo de respuesta.

```
{ "ResourceArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE", "ResourcePolicy": "policy-statement" }
```

Para obtener otros ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Elimine la política basada en recursos asociada a un almacén de datos de eventos con el AWS CLI

En los siguientes ejemplos se elimina la política basada en recursos asociada a un almacén de datos de eventos. Reemplace *eds-arn* por el ARN del almacén de datos de eventos.

```
aws cloudtrail delete-resource-policy --resource-arn eds-arn
```

Este comando no genera ningún resultado si se utiliza correctamente.

## 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.

## 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.

## Eliminar un almacén de datos de eventos con la AWS CLI

En esta sección, se muestra cómo eliminar un almacén de datos de eventos mediante la ejecución del comando `delete-event-data-store` de la AWS CLI

Para eliminar un almacén de datos de eventos, indique el ARN del almacén de datos de eventos o el sufijo de ID del ARN para especificar el `--event-data-store`. 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. Cuando está pendiente de eliminación, el almacén de datos de eventos no se tiene en cuenta para el máximo de 10 almacenes de datos de eventos de la Región de AWS.

### Note

No puede eliminar un almacén de datos de eventos si `--termination-protection-enabled` está configurado o si `FederationStatus` está `ENABLED`.

Para eliminar un almacén de datos de eventos con una `eventCategory` de `ActivityAuditLog`, primero debe eliminar el canal de la integración. Puede eliminar el canal mediante el comando `aws cloudtrail delete-channel`. Para obtener más información, consulte [Eliminar un canal para eliminar una integración con la AWS CLI](#).

```
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.

## 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.

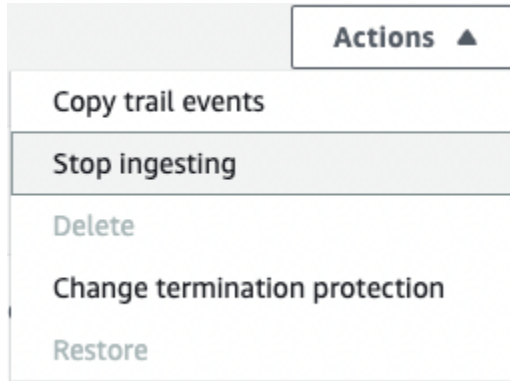
Solo puede eliminar un almacén de datos de eventos si la protección contra terminación y federación está desactivada. Protección contra terminación evita que el almacén de datos de eventos se elimine accidentalmente. De forma predeterminada, la protección contra la terminación está activada en los almacenes 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. Sin embargo, los almacenes de datos de eventos que están pendientes de

eliminación se tienen en cuenta para la cuota de almacenes de datos de eventos que pueden existir en una Región de AWS.

### 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 Copiar eventos de registros de seguimiento solo está disponible en los almacenes de datos de eventos que contienen eventos de CloudTrail. Las opciones Iniciar ingesta y Detener ingesta solo están disponibles en los almacenes de datos de eventos que contienen eventos de CloudTrail (eventos de administración y datos) o elementos de configuración de AWS Config.

## Copiar eventos de registro de seguimiento en un almacén de datos de eventos

Puede copiar los eventos de registro de seguimiento en un almacén de datos de eventos de CloudTrail Lake para crear una instantánea puntual de los eventos del registro de seguimiento. 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 registros de seguimiento en un almacén de datos de eventos existente configurado para los eventos de CloudTrail, o puede crear un nuevo almacén de datos de eventos de CloudTrail y seleccionar la opción Copiar eventos de los registros de seguimiento como parte de la creación del almacén 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 [Copia de eventos de registro de seguimiento a un almacén de datos de eventos existente con la consola](#). Para obtener más información acerca de la creación de un nuevo almacén de datos

de eventos, consulte [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

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.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

Cuando copia los eventos de registros de seguimiento en un almacén de datos de eventos de CloudTrail Lake, genera cargos según la cantidad de datos de eventos que ingiera el almacén de datos de eventos.

Al copiar eventos de registros de seguimiento en CloudTrail Lake, CloudTrail descomprime los registros que están almacenados en formato gzip (comprimido) y, a continuación, 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 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 [Administración de los costos de CloudTrail Lake](#).

## 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?                                                                                                 |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Analizar y consultar eventos de registros de seguimiento | Cree un <a href="#">nuevo almacén de datos de eventos</a> y seleccione la opción Copiar eventos de registros de seguimiento como parte |

| Escenario                                                                                            | ¿Cómo puedo lograr esto en la consola?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| históricos en CloudTrail Lake sin ingerir nuevos eventos                                             | 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 el registro de seguimiento existente por un almacén de datos de eventos de CloudTrail Lake | <p>Cree un almacén de datos de eventos con los mismos selectores 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.</p> <p>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.</p> <p>Después de crear el almacén de datos de eventos, puede desactivar el registro del registro de seguimiento para evitar cargos adicionales.</p> |

## Temas

- [Consideraciones para copiar eventos de registros de seguimiento](#)
- [Permisos necesarios para copiar eventos de registro de seguimiento](#)
- [Copia de eventos de registro de seguimiento a un almacén de datos de eventos existente con la consola](#)
- [Copia de eventos de registro de seguimiento a un nuevo almacén de datos de eventos con la consola](#)
- [Visualización de detalles de la copia de eventos con la consola de 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 registros de seguimiento, CloudTrail utiliza la operación de la API [GetObject](#) de S3 para recuperar los eventos de registros de seguimiento en el bucket 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.
- Cuando copia eventos de registros de seguimiento en un almacén de datos de eventos, CloudTrail copia todos los eventos de registros de seguimiento, independientemente de la configuración de los tipos de eventos, los selectores de eventos avanzados o la Región de AWS del almacén de datos de eventos de destino.
- 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](#).
  - Periodo de retención: el periodo de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos de eventos. CloudTrail solo copia los eventos de registros de seguimiento que tengan un valor de `eventTime` dentro del periodo de retención del almacén de datos de eventos. 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 conservar los eventos en el almacén de datos de eventos (periodo de retención = *el evento más antiguo en días* más *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.
- 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 registro de seguimiento de los archivos de registros comprimidos Gzip que están en el bucket de S3 de origen. CloudTrail no copia los eventos de registro de seguimiento de los archivos de registros sin comprimir ni de los archivos de registros 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 los eventos de CloudTrail contenidos en el prefijo CloudTrail del bucket de S3 y los prefijos dentro del prefijo CloudTrail y no comprueba los prefijos de otros servicios de AWS. Si desea copiar los eventos de CloudTrail contenidos en otro prefijo, debe elegir el prefijo al copiar los eventos del registro 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 registro de seguimiento, asegúrese de tener todos los permisos necesarios para su rol 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 elige crear un nuevo rol de IAM, CloudTrail proporciona todos los permisos necesarios para el rol.

Si el bucket de S3 de origen usa una clave de KMS para el cifrado de datos, verifique que la política de la clave de KMS permite a CloudTrail descifrar datos en el bucket. Si el bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave de manera que permitan a CloudTrail descifrar datos en el 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. Cuando elige un nuevo rol de IAM, CloudTrail crea un rol de IAM con los permisos necesarios y no se requiere ninguna acción adicional de su parte.

Si elige un rol existente, asegúrese de que las políticas de roles de IAM permitan a CloudTrail copiar los eventos de registro de seguimiento desde el bucket de S3 de origen. Esta sección proporciona ejemplos de las políticas de confianza y de permisos necesarias para el rol de IAM.

El siguiente ejemplo muestra la política de permisos, que permite a CloudTrail copiar los eventos de registro de seguimiento en el bucket de S3 de origen. Reemplace *amzn-s3-demo-bucket*, *myAccountID*, *region*, *prefix* y *eventDataStoreId* por los valores adecuados para la configuración. *myAccountID* es el ID de la cuenta de AWS utilizado para CloudTrail Lake, que puede no ser el ID de la cuenta de AWS del bucket de S3.

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:::amzn-s3-demo-bucket"
      ],
      "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:::amzn-s3-demo-bucket/prefix",
      "arn:aws:s3:::amzn-s3-demo-bucket/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 muestra la política de confianza de IAM, que permite a CloudTrail asumir un rol de IAM para copiar los eventos de registro de seguimiento del bucket de S3. Complete *myAccountID* (ID de la cuenta), *region* (Región) y *eventDataStoreArn* (ARN del almacén de datos de eventos) con los valores apropiados para la configuración. *myAccountID* es el ID de la Cuenta de AWS que se usa para CloudTrail Lake, que puede no ser igual al ID de la cuenta de AWS 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 registro de seguimiento, debe actualizar la política de buckets de S3 para permitir que CloudTrail copie los eventos de registro de seguimiento en el bucket de S3.

Puede agregar la siguiente instrucción a la política de buckets de S3 para conceder estos permisos. Sustituya *roleArn* y *amzn-s3-demo-bucket* por los valores apropiados para la configuración.

```

{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3::amzn-s3-demo-bucket",
    "arn:aws:s3::amzn-s3-demo-bucket/*"
  ]
},

```

## Política de claves KMS para descifrar datos en el bucket de S3 de origen

Si el bucket de S3 de origen usa una clave de KMS para el cifrado de datos, verifique que la política de claves de KMS proporcione a CloudTrail los permisos necesarios `kms:Decrypt` y `kms:GenerateDataKey` para copiar eventos de registros de seguimiento de un bucket de S3 con el cifrado SSE-KMS activado. Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave. Actualizar la política de la clave de KMS permite a CloudTrail descifrar los datos en el bucket de S3 de origen, ejecutar comprobaciones de validación para garantizar que los eventos cumplan los estándares de CloudTrail y copiar los eventos en el almacén de datos de eventos de CloudTrail Lake.

El siguiente ejemplo muestra la política de la clave de KMS, la cual permite a CloudTrail descifrar los datos en el bucket de S3 de origen. Reemplace *roleArn*, *amzn-s3-demo-bucket*, *myAccountID*, *region* y *eventDataStoreId* por los valores adecuados para la configuración. *myAccountID* es el ID de la cuenta de AWS utilizado para CloudTrail Lake, que puede no ser el ID de la cuenta de AWS del bucket de S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
        "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

## Copia de eventos de registro de seguimiento a un almacén de datos de eventos existente con la consola

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 [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

### 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](#).
- Periodo de retención: el periodo de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos de eventos. CloudTrail solo copia los eventos de registros de seguimiento que tengan un valor de eventTime dentro del periodo de retención del almacén de datos de eventos. 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 conservar los eventos en el almacén de datos de eventos (periodo de retención = *el evento más antiguo en días* más *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.

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

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 los eventos de CloudTrail contenidos en el prefijo CloudTrail del bucket de S3 y los prefijos dentro del prefijo CloudTrail y no comprueba los prefijos de otros servicios de AWS. Si desea copiar los eventos de CloudTrail contenidos en otro prefijo, elija Enter S3 URI (Introducir la URI de S3) y, a continuación, elija Browse S3 (Examinar S3) para buscar el prefijo. Si el bucket de S3 de origen para el registro de seguimiento usa una clave de KMS para el cifrado de datos, verifique que la política de la clave de KMS permite a CloudTrail descifrar los datos. Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave de manera que permitan a CloudTrail descifrar los datos en el 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 de buckets de S3 debe conceder acceso a CloudTrail para copiar los eventos de registro 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 intervalo de tiempo de eventos, seleccione el intervalo de tiempo de copia de los eventos. CloudTrail comprueba el prefijo y el nombre del registro para comprobar que el nombre contenga una fecha situada entre la fecha de inicio y la fecha de finalización elegidas antes de intentar copiar los eventos del registro 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 registros de seguimiento que tengan un valor de eventTime dentro del periodo de retención del almacén de datos de eventos. Por ejemplo, si el periodo de retención de un almacén de datos de eventos es de 90 días, CloudTrail no copiará ningún evento de registro de seguimiento con un valor de eventTime anterior a 90 días.

- Si elige Intervalo relativo, puede elegir si desea copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un intervalo personalizado. CloudTrail copia los eventos registrados dentro del periodo seleccionado.

- Si selecciona Absolute range (Intervalo absoluto), puede elegir fechas de inicio y de finalización específicas. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y de finalización seleccionadas.
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.
    - Seleccione Usar 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.
    - 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 de la copia 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). Cuando vuelva a realizar la copia, CloudTrail reanuda la copia 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 [Visualización de detalles de la copia de eventos con la consola de CloudTrail](#).

## Copia de eventos de registro de seguimiento a un nuevo almacén de datos de eventos con la consola

En este tutorial se explica cómo copiar eventos de registro de seguimiento en un nuevo almacén de datos de eventos de CloudTrail Lake para hacer un 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](#).

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

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 *my-management-events-eds*. Como práctica recomendada, utilice un nombre que identifique rápidamente el propósito del almacén de datos de eventos. Para obtener más información acerca de los requisitos de nomenclatura de CloudTrail, consulte [Requisitos de nomenclatura de los recursos de CloudTrail, los buckets de S3 y las claves de KMS](#).
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 [Administración de los costos de CloudTrail Lake](#).

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 extendida está disponible a precio de pago por uso. 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. 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.

 Note

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 conservar los eventos en el almacén de datos de eventos (periodo de retención = *el evento más antiguo en días* más *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.

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

Para habilitar el cifrado con su propia clave de KMS, seleccione Usar mi propia AWS KMS key. Elija New (Nueva) si desea que se cree una AWS KMS key para usted, o elija Existing (Existente) para usar una clave de KMS existente. En Enter KMS alias (Ingresar alias de KMS), especifique un alias con el formato `alias/MyAliasName`. El uso de su propia clave de KMS requiere que edite la política de la clave para permitir que se cifren y descifren los registros de CloudTrail. Para obtener más información, consulte [Configurar políticas de clave de AWS KMS para CloudTrail](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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.

Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. 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 cifrado de AWS Key Management Service del almacén de datos de eventos de una organización, debe utilizar una clave de 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 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](#).

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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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) Elija Habilitación de política de recursos para agregar una política basada en recursos a este almacén de datos de eventos. Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Por ejemplo, puede agregar una política basada en recursos para permitir a los usuarios raíz de otras cuentas consultar el almacén de datos de eventos y ver los resultados de las consultas. Para ver ejemplos de políticas, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

Una política basada en recursos incluye una o más instrucciones. Cada instrucción de la política define las [entidades principales](#) a las que se les permite o deniega el acceso al almacén de datos de eventos y las acciones que las entidades principales pueden realizar en el recurso del almacén de datos de eventos.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

10. (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 eventos de CloudTrail. 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 costos definidas por el usuario para 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 más información sobre cómo usar las etiquetas en AWS, consulte [Tagging your AWS resources](#) en la Guía del usuario para el etiquetado de recursos de AWS.

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

**Event type** [Info](#)  
Choose the type of events you want to add to your event data store. [Additional charges apply](#)

**Choose event types**

☒ **AWS events**  
Capture operations performed on or within your AWS resources.

☐ **Events from integrations**  
Create an integration to get events that are logged by applications outside of your AWS resources.

**Specify the type of AWS events**

☒ **CloudTrail events**  
CloudTrail events provide a record of activity in an AWS account.

☐ **CloudTrail Insights events**  
Insights events help identify unusual activity, errors, or user behavior in your account. You will be charged separately if you enable Insights for both trails and event data stores.

☐ **Configuration items**  
Configuration items show changes made to the configuration of a resource, and show the resource's compliance status.

13. En Eventos de CloudTrail, dejaremos seleccionado Eventos de administración y seleccionaremos Copiar eventos de los registros 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.

**CloudTrail events** [Info](#)

☒ **Management events**  
Capture management operations performed on your AWS resources.

☐ **Data events**  
Log the resource operations performed on or within a resource.

☐ **Network activity events**  
Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.

☒ **Copy trail events**  
Copy CloudTrail events logged in your trails or from S3 buckets.

☐ **Enable for all accounts in my organization**  
To review accounts in your organization, open AWS Organizations. [See all accounts](#) [↗](#)

**► Additional settings**

14. 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.

15. 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 eventos de todas las Regiones de AWS y comienza a ingerir eventos cuando se crea.
16. En Eventos de administración, dejaremos la configuración predeterminada.
17. En el área Copiar eventos de registros de seguimiento, complete los siguientes pasos.
- 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 los eventos de CloudTrail contenidos en el prefijo CloudTrail del bucket de S3 y los prefijos dentro del prefijo CloudTrail y no comprueba los prefijos de otros servicios de AWS. Si desea copiar los eventos de

CloudTrail contenidos en otro prefijo, elija Enter S3 URI (Introducir la URI de S3) y, a continuación, elija Browse S3 (Examinar S3) para buscar el prefijo. Si el bucket de S3 de origen para el registro de seguimiento usa una clave de KMS para el cifrado de datos, verifique que la política de la clave de KMS permite a CloudTrail descifrar los datos. Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave de manera que permitan a CloudTrail descifrar los datos en el 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 un intervalo de tiempo para copiar los eventos. CloudTrail comprueba el prefijo y el nombre del registro para comprobar que el nombre contenga una fecha situada entre la fecha de inicio y la fecha de finalización elegidas antes de intentar copiar los eventos del registro 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 elige Intervalo relativo, puede elegir si desea copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un intervalo personalizado. CloudTrail copia los eventos registrados dentro del periodo seleccionado.
  - Si selecciona Absolute range (Intervalo absoluto), puede elegir fechas de inicio y de finalización específicas. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y de finalización seleccionadas.

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

The screenshot shows the AWS CloudTrail console's date range selection interface. At the top, there are two tabs: 'Relative range' and 'Absolute range', with 'Absolute range' being the active tab. Below the tabs, there are two calendar views for May 2024 and June 2024. The date range is set from May 1, 2024, to May 31, 2024. The start time is 00:00:00 and the end time is 23:59:59. The 'Apply' button is highlighted.

- 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 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.
  - Seleccione Usar 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.
  - 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**.

### Copy existing trail events Info

Choose trail event source

management-events

S3 location of CloudTrail data (S3 URI)

s3://aws-cloudtrail-logs- /AWSLogs/ /CloudTr

Specify a time range of events

2023-06-01T00:00:00-05:00 — 2023-06-30T23:59:59-05:00

All CloudTrail events in your event source are imported, regardless of your event data store's configuration.

Choose IAM role

Create a new role (recommended)

Enter IAM role name

The new role name is prepended with CloudTrailLake-us-east-1-

copy-trail-events

► **Permission policies**

18. Elija Next (Siguiente) para revisar las opciones seleccionadas.
19. 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).
20. El nuevo almacén de datos de eventos aparece en la tabla Almacenes de datos de eventos de la página Almacenes de datos de eventos.

| Event data stores (3)    |         |             |              |                   |  | <div><div></div></div> | Copy trail events | Create event data store |
|--------------------------|---------|-------------|--------------|-------------------|--|------------------------|-------------------|-------------------------|
| Name                     | Status  | All regions | All accounts | Event type        |  |                        |                   |                         |
| my-management-events-eds | Enabled | Yes         | No           | CloudTrail events |  |                        |                   |                         |

21. 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.

|                                            |                                                      |             |         |                                     |                                     |  |         |
|--------------------------------------------|------------------------------------------------------|-------------|---------|-------------------------------------|-------------------------------------|--|---------|
| Event copy status (1) <a href="#">Info</a> |                                                      |             |         |                                     |                                     |  | Actions |
| < 1 >                                      |                                                      |             |         |                                     |                                     |  |         |
|                                            | Event log S3 location                                | Copy status | Copy ID | Created time                        | Finish time                         |  |         |
|                                            | s3://aws-cloudtrail-logs-.../AWSLogs/.../CloudTrail/ | Completed   | ...     | July 18, 2023, 15:50:06 (UTC-05:00) | July 18, 2023, 15:53:07 (UTC-05:00) |  |         |

22. 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 [Visualización de detalles de la copia de eventos con la consola de CloudTrail](#).

CloudTrail

>

Lake

>

Event data stores

>

my-management-events-trail-events

>

Copy ID

Actions

Copy details

info

Event log S3 location

s3://aws-cloudtrail-logs-

-

/AWSLogs/

/CloudTrail/

Copy ID

Prefixes copied

817/817 prefixes copied (0 failures)

Copy status

Completed

Created time

July 18, 2023, 15:50:06 (UTC-05:00)

Finish time

July 18, 2023, 16:04:51 (UTC-05:00)

Copy failures (0)

Retry copying prefixes that failed to copy.

<

1

>

Event location

▼

Error message

▼

Error type

▼

No failures

There are currently no copy failures.

23. 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). Cuando vuelva a realizar la copia, CloudTrail reanuda la copia en la ubicación en la que se produjo el error.

## Visualización de detalles de la copia de eventos con la consola de CloudTrail

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 Consola de administración de AWS 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.

## Federar un almacén de datos de eventos

La federación de un almacén de datos de eventos le permite ver los metadatos asociados al almacén de datos de eventos en el [Catálogo de datos de AWS Glue](#), registrar el catálogo de datos con AWS Lake Formation y ejecutar consultas SQL sobre los datos de sus 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.

Puede habilitar la federación mediante la consola de CloudTrail, AWS CLI o la operación [EnableFederation](#) de la API. 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 datos de AWS Glue. El ID del almacén de datos de eventos se utiliza para el nombre de la tabla. CloudTrail registra el ARN del rol de federación y el almacén de datos de eventos en [AWS Lake Formation](#), el servicio responsable de permitir un control de acceso detallado de los recursos federados del catálogo de datos de 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 rol nuevo mediante la consola de CloudTrail, CloudTrail crea 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 consola de CloudTrail, AWS CLI o la operación [DisableFederation](#) de la API. 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.

No se cobran cargos de CloudTrail por federar un almacén de datos de eventos de CloudTrail Lake. Realizar consultas en Amazon Athena tiene costos. Para obtener más información acerca de los precios de Athena, consulte la [Precios de Amazon Athena](#).

## [Análisis de los registros de actividad con AWS CloudTrail Lake y 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](#)
- [Cómo administrar 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:

- No se cobran cargos de CloudTrail por federar un almacén de datos de eventos de CloudTrail Lake. 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 elimina el rol de federación o revoca los permisos a los recursos de Lake Formation o AWS Glue, no puede ejecutar consultas desde Athena. Para obtener más información sobre el uso de Lake Formation, consulte [Cómo administrar 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 administrada de AWS: [AmazonAthenaFullAccess](#) permite 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 `aws:cloudtrail` CloudTrail administra la base de datos.
- Para crear un conjunto de datos en Amazon Quick Suite, 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 elige crear un nuevo rol de IAM mediante la consola de CloudTrail, 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. Cuando elige un nuevo rol de IAM, CloudTrail crea un rol de IAM con los permisos necesarios y no se requiere ninguna acción adicional de 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFederationEDSDataAccess",
      "Effect": "Allow",
      "Action": "cloudtrail:GetEventDataStoreData",
      "Resource": "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
    },
    {
      "Sid": "LakeFederationKMSTDecryptAccess",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111111111111: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.

## JSON

```
{
  "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 a CloudTrail habilitar la federación en el almacén de datos de eventos, a AWS Glue crear los recursos federados en el catálogo de datos de AWS Glue y a AWS Lake Formation administrar el registro de recursos.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudTrailEnableFederation",
      "Effect": "Allow",
      "Action": "cloudtrail:EnableFederation",
      "Resource": "arn:aws:cloudtrail:us-  
east-1:111111111111:eventdatastore/eds-id"
    },
    {
      "Sid": "FederationRoleAccess",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "iam:GetRole"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:iam::111122223333:role/federation-role-name"
  },
  {
    "Sid": "GlueResourceCreation",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:CreateTable",
      "glue:PassConnection"
    ],
    "Resource": [
      "arn:aws:glue:us-east-1:111111111111:catalog",
      "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
      "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-
id",
      "arn:aws:glue:us-east-1:111111111111:connection/aws:cloudtrail"
    ]
  },
  {
    "Sid": "LakeFormationRegistration",
    "Effect": "Allow",
    "Action": [
      "lakeformation:RegisterResource",
      "lakeformation:DeregisterResource"
    ],
    "Resource":
      "arn:aws:lakeformation:region:111111111111:catalog:111111111111"
  }
]
}

```

## 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 permite a CloudTrail deshabilitar la federación en el almacén de datos del evento, a AWS Glue eliminar la tabla federada administrada del catálogo de datos de AWS Glue y a Lake Formation anular el registro del recurso federado.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudTrailDisableFederation",
      "Effect": "Allow",
      "Action": "cloudtrail:DisableFederation",
      "Resource": "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
    },
    {
      "Sid": "GlueTableDeletion",
      "Effect": "Allow",
      "Action": "glue:DeleteTable",
      "Resource": [
        "arn:aws:glue:us-east-1:111111111111:catalog",
        "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
        "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-id"
      ]
    },
    {
      "Sid": "LakeFormationDeregistration",
      "Effect": "Allow",
      "Action": "lakeformation:DeregisterResource",
      "Resource": "arn:aws:lakeformation:us-east-1:111111111111:catalog:111111111111"
    }
  ]
}
```

## Habilitación de la federación de consultas de Lake

Puede habilitar la federación de consultas de Lake mediante la consola de CloudTrail, AWS CLI o la operación de [EnableFederation](#) de la API. 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 datos de AWS Glue. El ID del almacén de datos de eventos se utiliza para el nombre de la tabla. CloudTrail registra el ARN del rol de federación y el almacén de datos de eventos en [AWS Lake Formation](#), el servicio responsable de



permitir un control de acceso detallado de los recursos federados del catálogo de datos de AWS Glue.

En esta sección, se describe cómo habilitar la federación mediante la consola de CloudTrail y la 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 Consola de administración de AWS y abra la consola de CloudTrail 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. Cuando crea un nuevo rol, CloudTrail crea automáticamente uno 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. Seleccione Save changes (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 consola de CloudTrail, AWS CLI o la operación [DisableFederation](#) de la API. 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 con la consola de CloudTrail 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 Consola de administración de AWS y abra la consola de CloudTrail 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. Seleccione Save changes (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.

## Cómo administrar los recursos de la federación de CloudTrail Lake con AWS Lake Formation

Al federar un almacén de datos de eventos, CloudTrail registra el ARN del rol de federación y el almacén de datos de eventos en AWS Lake Formation, el servicio responsable de permitir un control de acceso detallado de los recursos federados del catálogo de datos de AWS Glue. En esta sección, se describe cómo puede utilizar Lake Formation para administrar los recursos de la federación de CloudTrail Lake.

Al habilitar la federación, CloudTrail crea los siguientes recursos en el catálogo de datos de AWS Glue.

- **Base de datos administrada:** CloudTrail crea 1 base de datos con el nombre `aws:cloudtrail` de cada cuenta. CloudTrail administra la base de datos. No puede eliminar ni modificar la base de datos en AWS Glue.
- **Tabla federada administrada:** CloudTrail crea 1 tabla para cada almacén de datos de eventos federado y utiliza el ID del almacén 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 funciona AWS Glue con IAM, consulte [Cómo funciona AWS Glue 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](#). Para obtener más información, consulte [Securing data lakes with row-level access control](#) en la Guía para desarrolladores de AWS Lake Formation.
  - 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 administrada y una tabla federada gestionada con la configuración del lago de datos de Lake Formation.

Una vez que CloudTrail habilite la federación, puede comprobar qué método de permisos utiliza para la base de datos administrada y la tabla federada administrada al comprobar 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 un recurso del catálogo de datos se comparte con su Cuenta de AWS y su cuenta no pertenece a la misma organización de AWS que la cuenta que lo comparte, acepte la invitación para compartir recursos de AWS Resource Access Manager (AWS RAM). Para obtener más información, consulte [Aceptación de una invitación para compartir un recurso de AWS RAM](#).

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 un recurso del catálogo de datos se comparte con su Cuenta de AWS y su cuenta no pertenece a la misma organización de AWS que la cuenta que lo comparte, 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 [Aceptación de una invitación para compartir un recurso de AWS RAM](#).
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.

## Descripción de los 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 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. No se puede utilizar el almacén de datos de eventos de la organización para recopilar eventos fuera de AWS.

Puede [crear un almacén de datos de eventos de la organización](#) mediante la cuenta de administración o la cuenta del 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 almacén 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 funciones de la cuenta de administración y las cuentas de administrador delegado dentro de la organización de AWS Organizations.

| Capacidades                                                                                                                         | Cuenta de administración | Cuenta de administrador delegado |
|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------|
| Registrar o eliminar las cuentas de administrador delegado.                                                                         | Sí                       | No                               |
| Crear un almacén de datos de eventos de una organización para eventos de AWS CloudTrail o elementos de configuración de AWS Config. | 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 <sup>1</sup>                  |
| Iniciar o detener la ingesta de eventos en un almacén de datos de eventos de la organización.                                       | Sí                       | Sí                               |
| Habilitar la federación de consultas de Lake en un almacén de datos de eventos de la organización. <sup>2</sup>                     | 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                               |

| Capacidades                                                                                                 | Cuenta de administración | Cuenta de administrador delegado |
|-------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------|
| Consultar el panel administrado de un almacén de datos de eventos de la organización.                       | Sí                       | No                               |
| Habilitar el panel de aspectos destacados para los almacenes de datos de eventos de la organización.        | Sí                       | No                               |
| Crear un widget para un panel personalizado que consulte un almacén de datos de eventos de la organización. | Sí                       | No                               |

<sup>1</sup>Solo la cuenta de administración puede convertir un almacén de datos de eventos de la organización en un almacén de datos de eventos a nivel de cuenta, o convertir un almacén de datos de eventos a nivel de cuenta en un almacén 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 almacén de datos de eventos de la organización se convierte en un almacén de datos de eventos a nivel de cuenta, solo la cuenta de administración tiene acceso al almacén de datos de eventos. Del mismo modo, solo un almacén de datos de eventos a nivel de cuenta que esté en la cuenta de administración se puede convertir en un almacén de datos de eventos de la organización.

<sup>2</sup>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.

## Creación de un almacén de datos de eventos de la organización

La cuenta de administración o la cuenta del administrador delegado de una organización puede crear un almacén de datos de eventos de la organización para recopilar eventos de CloudTrail (eventos de administración o de datos) o elementos de configuración de AWS Config.



**Note**

Solo la cuenta de administración de la organización puede copiar eventos de registro de seguimiento en un almacén de datos de eventos.

## CloudTrail console

Creación de un almacén de datos de eventos de la organización mediante la consola

1. Siga los pasos del procedimiento [Creación de un almacén de datos de eventos para eventos de CloudTrail](#) para crear un almacén de datos de eventos de la organización para los eventos de datos o de administración de CloudTrail.

OR

Siga los pasos del procedimiento [Creación de un almacén de datos de eventos para los elementos de configuración de AWS Config](#) para crear un almacén de datos de eventos de la organización para los elementos de configuración de AWS Config.

2. En la página Elegir eventos, elija Habilitar para todas las cuentas de mi organización.

## AWS CLI

Para crear un almacén de datos de eventos de la organización, ejecute el comando [create-event-data-store](#) e incluya la opción `--organization-enabled`.

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. Como CloudTrail registra los eventos de administración de forma predeterminada, no es necesario especificar selectores de eventos avanzados si el almacén 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 comando de ejemplo `create-event-data-store` de la AWS CLI crea un almacén de datos de eventos de la organización denominado `config-items-org-eds` que recopila elementos de configuración de AWS Config. Para recopilar los elementos de configuración, especifique que el campo `eventCategory` iguale a `ConfigurationItem` en 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"] }
    ]
  }
]'

```

## Aplicación de un almacén de datos de eventos a nivel de cuenta a una organización

La cuenta de administración de la organización puede convertir un almacén de datos de eventos a nivel de cuenta para aplicarlo a una organización.

### CloudTrail console

Actualización de un almacén de datos de eventos a nivel de cuenta mediante la consola

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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), elija Edit (Editar).
5. Seleccione Habilitar para todas las cuentas de mi organización.
6. Seleccione Save changes (Guardar cambios).

Para obtener información adicional acerca de la actualización de un almacén de datos de eventos, consulte [Actualización de un almacén de datos de eventos con la consola](#).

### AWS CLI

Para actualizar un almacén de datos de eventos a nivel de cuenta para aplicarlo a una organización, ejecute el comando [update-event-data-store](#) e incluya la opción `--organization-enabled`.

```
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
```

## Política predeterminada de recursos para administradores delegados

CloudTrail crea de manera automática una política de recursos denominada `DelegatedAdminResourcePolicy` para los [almacenes de datos de eventos de la organización](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en

los almacenes de datos de eventos de la organización. Los permisos que se encuentran en `DelegatedAdminResourcePolicy` se obtienen de los permisos del administrador delegado en AWS Organizations.

El objetivo de la `DelegatedAdminResourcePolicy` es garantizar que las cuentas del administrador delegado puedan administrar el almacén de datos de eventos de la organización en nombre de la organización y no se les niegue involuntariamente el acceso al almacén de datos de eventos de la organización cuando se asocia una política basada en recursos que permite o impide a las entidades principales realizar una acción en el almacén de datos de eventos de la organización.

CloudTrail evalúa `DelegatedAdminResourcePolicy` en conjunto con cualquier política basada en recursos que se ofrezca para el almacén de datos de eventos de la organización. Solo se negaría el acceso a las cuentas de administrador delegado si la política basada en recursos que se brinda incluyera una declaración en la que se impidiera de manera explícita a las cuentas de administrador delegado realizar una acción en el almacén de datos de eventos de la organización que, de otro modo, las cuentas de administrador delegado podrían realizar.

Esta política `DelegatedAdminResourcePolicy` se actualiza de manera automática cuando sucede lo siguiente:

- La cuenta de administración convierte un almacén de datos de eventos de la organización en un almacén de datos de eventos a nivel de cuenta, o convierte un almacén de datos de eventos a nivel de cuenta en un almacén de datos de eventos de la organización.
- Existen cambios en la organización. Por ejemplo, la cuenta de administración registra o elimina una cuenta de administrador delegado de CloudTrail.

Puede consultar la política actualizada en la sección de Políticas de recursos del administrador delegado de la consola CloudTrail o mediante la ejecución del comando AWS CLI `get-resource-policy` y el paso del ARN del almacén de datos de eventos de la organización.

En el siguiente ejemplo se ejecuta el comando `get-resource-policy` en un almacén de datos de eventos de la organización.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

El resultado de este comando mostrará la política basada en recursos y la política `DelegatedAdminResourcePolicy` generada para las cuentas del administrador delegado.

## Recursos adicionales

- [Administrador delegado de la organización](#)
- [Cómo agregar un administrador delegado de CloudTrail](#)
- [Cómo eliminar un administrador delegado de CloudTrail](#)

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

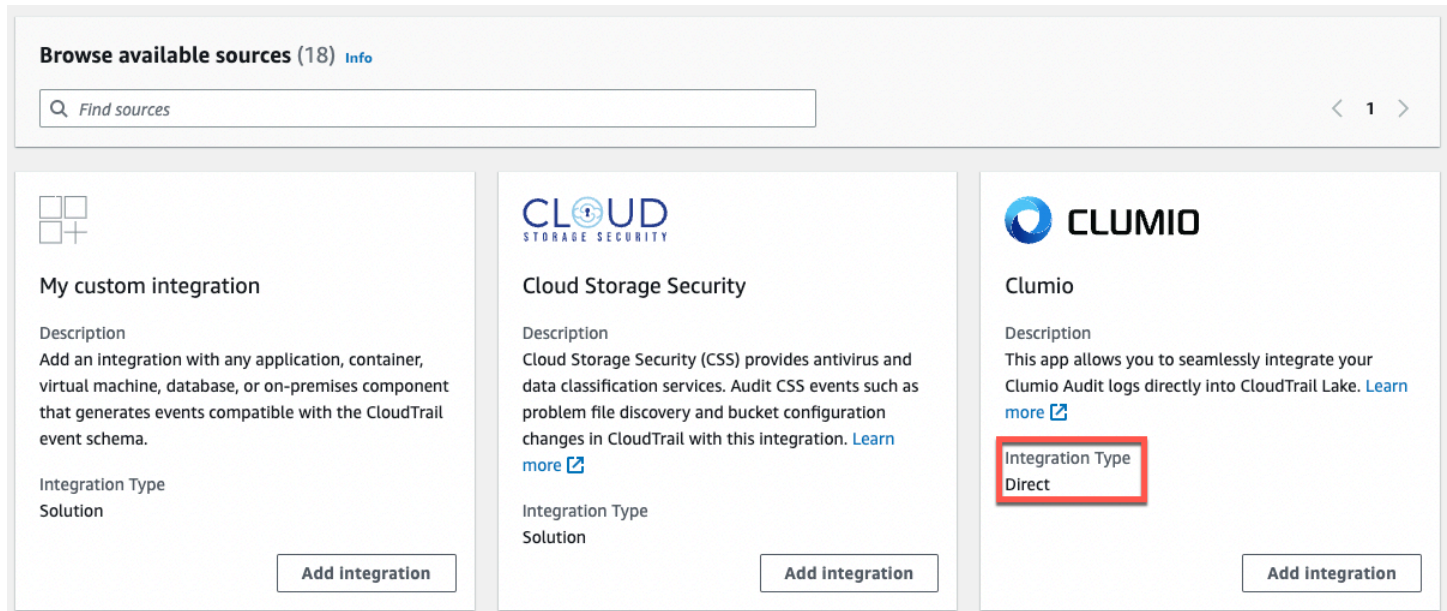
Puede utilizar CloudTrail para registrar y almacenar datos de actividad de los usuarios desde cualquier origen en los entornos híbridos, como aplicaciones internas o de SaaS alojadas en las instalaciones o en la nube, máquinas virtuales o contenedores. Puede almacenar, acceder y analizar los datos, solucionar 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.



**Browse available sources (18)** [Info](#)

Find sources

**My custom integration**

Description  
Add an integration with any application, container, virtual machine, database, or on-premises component that generates events compatible with the CloudTrail event schema.

Integration Type  
Solution

**Add integration**

**Cloud Storage Security**

Description  
Cloud Storage Security (CSS) provides antivirus and data classification services. Audit CSS events such as problem file discovery and bucket configuration changes in CloudTrail with this integration. [Learn more](#)

Integration Type  
Solution

**Add integration**

**Clumio**

Description  
This app allows you to seamlessly integrate your Clumio Audit logs directly into CloudTrail Lake. [Learn more](#)

Integration Type  
Direct

**Add integration**

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 con la consola](#)
- [Creación de una integración personalizada con la consola](#)
- [Creación, actualización y administración de las integraciones de CloudTrail Lake con la AWS CLI](#)
- [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 con la consola

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 Consola de administración de AWS 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 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.

**External ID**

Enter the unique account identifier provided by Nordcloud. [How to find this?](#) 

**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 con la consola

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 Consola de administración de AWS 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 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 Precio de retención ampliable por un año, o hasta 2557 días (unos 7 años) si elige la opción 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","\nUID\\":\\"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.

```
EXAMPLEHjkI8iehvCUCWTIAbNYk0g0/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`.

## Creación, actualización y administración de las integraciones de CloudTrail Lake con la AWS CLI

En esta sección se describen los comandos que puede usar para crear, actualizar y administrar sus integraciones de CloudTrail Lake mediante la AWS CLI.

Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la Región de AWS 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.

## Comandos disponibles para las integraciones de CloudTrail Lake

Comandos para crear, actualizar y administrar integraciones en CloudTrail Lake:

- [create-event-data-store](#) para crear un almacén de datos de eventos para eventos externos a AWS.
- [delete-channel](#) para eliminar un canal usado para una integración.
- [delete-resource-policy](#) para eliminar la política de recursos asociada a un canal de una integración de CloudTrail Lake.
- [get-channel](#) para devolver información acerca de un canal de CloudTrail.
- [get-resource-policy](#) para recuperar el texto JSON del documento de la política basada en recursos asociado al canal CloudTrail.
- [list-channels](#) para enumerar los canales de la cuenta actual y sus nombres de origen.
- [put-audit-events](#) para ingerir los eventos de su aplicación en CloudTrail Lake. Un parámetro obligatorio, `auditEvents`, acepta los registros JSON (también denominados carga útil) de los eventos que desea que CloudTrail ingiera. Puede agregar hasta 100 de estos eventos(o hasta 1 MB) por solicitud `PutAuditEvents`.
- [put-resource-policy](#) para adjuntar una política de permisos basada en recursos a un canal de CloudTrail que se utilice para la integración con un origen de eventos ajeno a AWS. Para más información sobre las políticas basadas en los recursos, consulte los [ejemplos de políticas de AWS CloudTrail basadas en recursos](#).
- [update-channel](#) para actualizar un canal especificado mediante un ARN o UUID de canal necesario.

Para obtener una lista de los comandos disponibles para los almacenes de datos de eventos de CloudTrail Lake, consulte [Comandos disponibles para los almacenes de datos de eventos](#).

Para obtener una lista de los comandos disponibles para las consultas de CloudTrail Lake, consulte [Comandos disponibles para consultas de CloudTrail Lake](#).

Para obtener una lista de los comandos disponibles para los paneles de CloudTrail Lake, consulte [Comandos disponibles para los paneles](#).

## Crear una integración para registrar eventos externos a AWS con la AWS CLI

En esta sección se describe cómo puede usar la AWS CLI para crear una integración de CloudTrail Lake para registrar eventos externos a AWS.

En la AWS CLI, puede crear una integración 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 [AWS CloudTrailEjemplos de políticas basadas en recursos de](#) .

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.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYk0g0/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`.

## Actualizar un canal con la AWS CLI

En esta sección, se describe cómo usar la AWS CLI para actualizar un canal que se utiliza para una integración de CloudTrail Lake. Puede ejecutar el comando `update-channel` para actualizar el nombre del canal o para especificar un otro almacén de datos de eventos de destino. No se puede actualizar el origen de un canal.

Al ejecutar el comando, el parámetro `--channel` es obligatorio.

A continuación, se muestra un ejemplo de cómo actualizar el nombre y el destino del canal.

```
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

En esta sección, se describe cómo ejecutar el comando `delete-channel` para eliminar el canal de una integración de CloudTrail Lake. El canal se elimina cuando quiere detener la ingesta de eventos de socios u otros eventos de actividad externos a AWS. Se requiere el ARN o el ID (el sufijo ARN) del canal que desea eliminar.

En el ejemplo siguiente, se muestra cómo eliminar el canal.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

## 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             |
| Netskope                   | NetskopeCloudExchange       | solución            |
| Nordcloud, an IBM Company  | IBMMulticloud               | directa             |
| MontyCloud                 | MontyCloud                  | directa             |
| Okta                       | OktaSystemLogEvents         | solución            |
| One Identity               | OneLogin                    | solución            |
| Shoreline.io               | Shoreline                   | solución            |

| Nombre del socio (consola) | Nombre del origen (API) | Tipo de integración |
|----------------------------|-------------------------|---------------------|
| 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 Consola de administración de AWS 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 registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

- [Campos que proporciona CloudTrail después de la ingesta de datos](#)
- [Campos que proporcionan los eventos](#)

CloudTrail proporciona los siguientes campos después de la ingesta de datos:

| Nombre del campo | Tipo de entrada | Requisito   | Descripción            |
|------------------|-----------------|-------------|------------------------|
| eventVersion     | cadena          | Obligatorio | La versión del evento. |



| Nombre del campo   | Tipo de entrada | Requisito   | Descripción                                                                                                                                  |
|--------------------|-----------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| eventCategory      | cadena          | Obligatorio | La categoría del evento. Para los eventos que no son de AWS, el valor es <code>ActivityAuditLog</code> .                                     |
| eventType          | cadena          | Obligatorio | Tipo de evento. Para los eventos que no son de AWS, el valor válido es <code>ActivityLog</code> .                                            |
| eventId            | cadena          | Obligatorio | El ID único de un evento.                                                                                                                    |
| eventTime          | cadena          | Obligatorio | Marca de tiempo del evento, en formato <code>yyyy-MM-DDTHH:mm:ss</code> , en tiempo universal coordinado (UTC).                              |
| awsRegion          | cadena          | Obligatorio | La Región de AWS donde la llamada <code>PutAuditEvents</code> se realizó.                                                                    |
| recipientAccountId | cadena          | Obligatorio | Representa el ID de cuenta que recibió este evento. CloudTrail completa este campo mediante el cálculo a partir de la carga útil del evento. |

| Nombre del campo | Tipo de entrada | Requisito | Descripción                                                                                                                                                                                                                     |
|------------------|-----------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| addendum         | -               | Opcional  | Muestra información 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. |
| • razón          | 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 proporciona si el motivo es <code>UPDATED_DATA</code> .                                                                                     |
| • originalUID    | cadena          | Opcional  | El UID del evento original del origen. Esto solo se proporciona si el motivo es <code>UPDATED_DATA</code> .                                                                                                                     |

| Nombre del campo  | Tipo de entrada | Requisito   | Descripción                                                                                                            |
|-------------------|-----------------|-------------|------------------------------------------------------------------------------------------------------------------------|
| • originalEventID | cadena          | Opcional    | El ID del evento original. Esto solo se proporciona si el motivo es UPDATED_DATA .                                     |
| metadatos         | -               | Obligatorio | Información acerca del canal que utilizó el evento.                                                                    |
| • ingestionTime   | cadena          | Obligatorio | La marca de tiempo en que se procesó el evento, en formato yyyy-MM-DDTHH:mm:ss , en tiempo universal coordinado (UTC). |
| • channelARN      | cadena          | Obligatorio | El ARN del canal que utilizó el evento.                                                                                |

Los eventos de clientes proporcionan los siguientes campos:

| Nombre del campo | Tipo de entrada | Requisito   | Descripción                                                                      |
|------------------|-----------------|-------------|----------------------------------------------------------------------------------|
| eventData        | -               | Obligatorio | Los datos de auditoría enviados a CloudTrail en una llamada PutAuditEvents .     |
| • versión        | cadena          | Obligatorio | La versión del evento desde el origen.<br><br>Limitaciones de longitud: longitud |

| Nombre del campo | Tipo de entrada | Requisito   | Descripción                                                                                                           |
|------------------|-----------------|-------------|-----------------------------------------------------------------------------------------------------------------------|
|                  |                 |             | máxima de 256 caracteres.                                                                                             |
| • userIdentity   | -               | Obligatorio | Información acerca del usuario que realizó una solicitud.                                                             |
| • • tipo         | cadena          | Obligatorio | El tipo de identidad de usuario.<br><br>Limitaciones de longitud: longitud máxima de 128 caracteres.                  |
| • • principalId  | cadena          | Obligatorio | Un identificador único para el actor del evento.<br><br>Limitaciones de longitud: longitud máxima de 1024 caracteres. |
| • • Detalles     | Objeto JSON     | Opcional    | Información adicional acerca de la identidad .                                                                        |
| • userAgent      | cadena          | Opcional    | El agente que realizó la solicitud.<br><br>Limitaciones de longitud: longitud máxima de 1024 caracteres.              |

| Nombre del campo           | Tipo de entrada | Requisito   | Descripción                                                                                                                                                                      |
|----------------------------|-----------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • <code>eventSource</code> | cadena          | Obligatorio | <p>Este es el origen de eventos asociado o la aplicación personalizada en que se registran los eventos.</p> <p>Limitaciones de longitud: longitud máxima de 1024 caracteres.</p> |
| • <code>eventName</code>   | cadena          | Obligatorio | <p>La acción solicitada, una de las acciones de la API para la aplicación o el servicio de origen.</p> <p>Limitaciones de longitud: longitud máxima de 1024 caracteres.</p>      |
| • <code>eventTime</code>   | cadena          | Obligatorio | <p>Marca de tiempo del evento, en formato <code>yyyy-MM-DDTHH:mm:ss</code> , en tiempo universal coordinado (UTC).</p>                                                           |

| Nombre del campo                                                  | Tipo de entrada | Requisito   | Descripción                                                                                                                                                                                                      |
|-------------------------------------------------------------------|-----------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>UID</li></ul>               | cadena          | Obligatorio | <p>El valor de UID que identifica la solicitud . El servicio o la aplicación que se llama genera este valor.</p> <p>Limitaciones de longitud: longitud máxima de 1024 caracteres.</p>                            |
| <ul style="list-style-type: none"><li>requestParameters</li></ul> | 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.                                                     |
| <ul style="list-style-type: none"><li>responseElements</li></ul>  | Objeto JSON     | Opcional    | El elemento de respuesta de las acciones que realizaron cambios (acciones de creación, actualización 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.<br><br>Limitaciones de longitud: longitud máxima de 256 caracteres.                        |
| • errorMessage       | cadena          | Opcional    | La descripción del error.<br><br>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          | Obligatorio | 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                                                                                                                                                                       |
|---------------------------------------------------------------------|-----------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>additionalEventData</li></ul> | 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
    }
}
```

## Paneles de CloudTrail Lake

Puede usar los paneles de CloudTrail Lake para consultar las tendencias de eventos de los almacenes de datos de eventos de la cuenta. CloudTrail Lake ofrece los siguientes tipos de paneles:

- **Paneles administrados:** puede ver un panel administrado para ver las tendencias de eventos de un almacén de datos de eventos que recopila eventos de administración, de datos o de Insights. Estos paneles están disponibles de manera automática y CloudTrail Lake los administra. CloudTrail ofrece 14 paneles administrados entre los que puede elegir. Puede actualizar de manera manual los paneles administrados. No puede modificar, agregar ni eliminar los widgets de estos paneles; sin embargo, puede guardar un panel administrado como un panel personalizado si quiere modificar los widgets o establecer un programa de actualización.
- **Paneles personalizados:** estos le permiten consultar eventos en cualquier tipo de almacén de datos de eventos. Puede agregar hasta 10 widgets a un panel personalizado. Puede actualizar de manera manual un panel personalizado o puede establecer un programa de actualización.

- **Paneles destacados:** habilite el panel de aspectos destacados para ver un resumen rápido de la actividad recopilada de AWS por los almacenes de datos de eventos de la cuenta. CloudTrail administra el panel de aspectos destacados e incluye widgets que son pertinentes para la cuenta. Los widgets que se muestran en el panel de aspectos destacados son únicos para cada cuenta. Estos widgets podrían mostrar la actividad anormal o las anomalías detectadas. Por ejemplo, en el panel de aspectos destacados se podría incluir el Widget de acceso entre cuentas total, que muestra si hay un aumento en la actividad anormal entre cuentas. CloudTrail actualiza el panel de aspectos destacados cada 6 horas. En el panel se muestran los datos de las últimas 24 horas de la última actualización.

Cada panel consta de uno o más widgets y cada uno brinda una representación gráfica de los resultados de una consulta SQL. Para ver la consulta de un widget, elija Ver y editar consultas a fin de abrir el editor de consultas.

Cuando se actualiza un panel, CloudTrail Lake ejecuta las consultas para completar los widgets del panel. Dado que la ejecución de consultas genera costos, CloudTrail le solicita que confirme los costos asociados a la ejecución de consultas. Para obtener más información acerca de los precios de CloudTrail, consulte [Precios de CloudTrail](#).

## Temas

- [Requisitos previos](#)
- [Limitaciones](#)
- [Compatibilidad de regiones](#)
- [Permisos necesarios](#)
- [Consulta de un panel administrado con la consola de CloudTrail](#)
- [Habilitación del panel de aspectos destacados con la consola de CloudTrail](#)
- [Desactivación del panel de aspectos destacados con la consola de CloudTrail](#)
- [Cree un panel personalizado con la consola de CloudTrail](#)
- [Establezca un programa de actualización de un panel personalizado con la consola de CloudTrail](#)
- [Deshabilite un programa de actualización de un panel personalizado con la consola de CloudTrail](#)
- [Cambio de la protección contra la terminación con la consola de CloudTrail](#)
- [Eliminación de un panel personalizado con la consola de CloudTrail](#)
- [Crear, actualizar y administrar los paneles con la AWS CLI](#)

## Requisitos previos

Para usar los paneles de CloudTrail 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 [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#). Para obtener información acerca de cómo crear un almacén de datos de eventos mediante la AWS CLI, consulte [Crear un almacén de datos de eventos con la AWS CLI](#).
- Debe tener los permisos adecuados para ver, crear y actualizar los paneles. Para obtener más información, consulte [Permisos necesarios](#).

## Limitaciones

Las siguientes limitaciones se aplican a los paneles de CloudTrail Lake:

- Solo puede habilitar el panel de aspectos destacados para los almacenes de datos de eventos que existan en la cuenta.
- Solo puede ver el panel administrados para los almacenes de datos de eventos que existan en la cuenta.
- En el caso de los paneles personalizados, solo puede agregar los widgets de muestra o crear nuevos que consulten los almacenes de datos de eventos que existen en su cuenta.
- Los administradores delegados de una organización AWS Organizations no pueden ver ni administrar los paneles que sean propiedad de la cuenta de administración.

## Compatibilidad de regiones

Los paneles de CloudTrail Lake son compatibles en todas las Regiones de AWS en las que se admite CloudTrail Lake.

El widget de Resumen de actividades del panel de Aspectos destacados es compatible con las siguientes regiones:

- Región Asia-Pacífico (Tokio) (ap-northeast-1)
- Este de EE. UU. (Norte de Virginia) (us-east-1)

- Región EE. UU. Oeste (Oregón) (us-west-1)

Todos los demás widgets son compatibles en todas las Regiones de AWS en las que se admite CloudTrail Lake.

Para obtener más información sobre las regiones que son compatibles con CloudTrail Lake, consulte [Regiones en las que se admite CloudTrail Lake](#).

## Permisos necesarios

En esta sección se describen los permisos necesarios para los paneles de CloudTrail Lake y se analizan dos tipos de políticas de IAM:

- Las políticas basadas en la identidad que le permiten realizar acciones para crear, administrar y eliminar paneles.
- Las políticas basadas en recursos que permiten a CloudTrail ejecutar consultas en el almacén de datos de eventos cuando se actualiza el panel y realizar actualizaciones programadas de los paneles personalizados y del panel de aspectos destacados en su nombre. Cuando crea paneles con la consola de CloudTrail, tiene la opción de asociar las políticas basadas en recursos. También puede ejecutar el comando AWS CLI [put-resource-policy](#) para agregar una política basada en recursos a los almacenes de datos de eventos o paneles.

### Requisitos de la política basada en la identidad

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. 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.

Para ver y administrar los paneles de CloudTrail Lake, necesita una de las siguientes políticas:

- La política administrada de [CloudTrailFullAccess](#).
- La política administrada de [AdministratorAccess](#).
- Una política personalizada que incluya uno o más de los permisos específicos que se describen en las secciones que se encuentran a continuación.

## Temas

- [Permisos necesarios para crear los paneles](#)
- [Permisos necesarios para actualizar los paneles](#)
- [Permisos necesarios para actualizar los paneles](#)

### Permisos necesarios para crear los paneles

El siguiente ejemplo de política ofrece los permisos mínimos necesarios para crear paneles.

Reemplace *partition*, *region*, *account-id* y *eds-id* por los valores de su configuración.

- El permiso `StartQuery` solo es necesario si la solicitud contiene widgets. Proporcione permisos `StartQuery` para todos los almacenes de datos de eventos incluidos en una consulta de widgets.
- El permiso `StartDashboardRefresh` solo es necesario si el panel tiene un programa de actualización.
- Para el panel de aspectos destacados, el remitente debe tener el permiso `StartQuery` a fin de acceder a todos los almacenes de datos de eventos de la cuenta.

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:CreateDashboard",
        "cloudtrail:StartDashboardRefresh",
        "cloudtrail:StartQuery"
      ],
      "Resource": [
        "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
        "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
      ]
    }
  ]
}
```

## Permisos necesarios para actualizar los paneles

El siguiente ejemplo de política ofrece los permisos mínimos necesarios para actualizar paneles. Reemplace *partition*, *region*, *account-id* y *eds-id* por los valores de su configuración.

- El permiso `StartQuery` solo es necesario si la solicitud contiene widgets. Proporcione permisos `StartQuery` para todos los almacenes de datos de eventos incluidos en una consulta de widgets.
- El permiso `StartDashboardRefresh` solo es necesario si el panel tiene un programa de actualización.
- Para el panel de aspectos destacados, el remitente debe tener el permiso `StartQuery` a fin de acceder a todos los almacenes de datos de eventos de la cuenta.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:UpdateDashboard",
        "cloudtrail:StartDashboardRefresh",
        "cloudtrail:StartQuery"
      ],
      "Resource": [
        "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
        "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
      ]
    }
  ]
}
```

## Permisos necesarios para actualizar los paneles

El siguiente ejemplo de política ofrece los permisos mínimos necesarios para actualizar los paneles. Reemplace *partition*, *region*, *account-id*, *dashboard-name* y *eds-id* por los valores de su configuración.

- Para los paneles personalizados y los paneles de aspectos destacados, el remitente debe disponer de `cloudtrail:StartDashboardRefresh` permissions.
- En el caso de los paneles administrados, el remitente debe tener el permiso `cloudtrail:StartDashboardRefresh` y los permisos `cloudtrail:StartQuery` para el almacén de datos de eventos implicado en la actualización.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "cloudtrail:StartDashboardRefresh",
        "cloudtrail:StartQuery"
      ],
      "Resource": [
        "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/dashboard-  
name",
        "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
      ]
    }
  ]
}
```

## Políticas basadas en recursos para paneles y almacenes de datos de eventos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. 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.

Para ejecutar consultas en un panel durante una actualización manual o programada, debe asociar una política basada en recursos a cada almacén de datos de eventos que esté asociado a un widget del panel. Esto permite a CloudTrail Lake ejecutar las consultas en su nombre. Cuando crea un

panel personalizado o habilita el panel de aspectos destacados mediante la consola de CloudTrail, esta le ofrece la opción de elegir a qué almacenes de datos de eventos quiere aplicar los permisos. Para obtener más información sobre la política basada en recursos, consulte [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#).

A fin de establecer un programa de actualización para un panel, debe asociar una política basada en recursos al panel para permitir que CloudTrail Lake actualice el panel en su nombre. Cuando establece un programa de actualización para un panel personalizado o habilita el panel de aspectos destacados mediante la consola de CloudTrail, esta le ofrece la opción de asociar una política basada en recursos al panel. Para ver una política de ejemplo, consulte [Ejemplo de política basada en recursos para un panel](#).

Puede asociar una política basada en recursos mediante la consola de CloudTrail, el [AWS CLI](#) o la operación de la API [PutResourcePolicy](#).

## Permisos clave de KMS para descifrar los datos de un almacén de datos de eventos

Si el almacén de datos de eventos que se está consultando está cifrado con una clave de KMS, asegúrese que la política de claves de KMS permite a CloudTrail descifrar los datos en el almacén de datos de eventos. El siguiente ejemplo de instrucción de política permite que la entidad principal del servicio CloudTrail descifre el almacén de datos de eventos.

```
{
  "Sid": "AllowCloudTrailDecryptAccess",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

## Consulta de un panel administrado con la consola de CloudTrail

CloudTrail Lake ofrece paneles administrados que muestran las tendencias de eventos para los almacenes de datos de eventos que recopilan eventos administrados, de datos y de Insights. CloudTrail Lake administra estos paneles. No puede modificar, agregar ni eliminar los widgets de estos paneles; sin embargo, puede guardar un panel administrado como un panel personalizado si quiere modificar los widgets o establecer un programa de actualización.



 Note

Solo puede ver el panel administrados para los almacenes de datos de eventos que existan en la cuenta.

Para ver un panel administrado

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En Paneles administrados, elija el panel que desea consultar. Para obtener más información, consulte [Paneles administrados disponibles](#).

 Note

El menú desplegable muestra solo los almacenes de datos de eventos pertinentes para el panel seleccionado. Por ejemplo, si elige paneles centrados en los eventos de datos, como los eventos de datos de S3, el menú desplegable solo mostrará los almacenes de datos de eventos que estén configurados a fin de recopilar eventos de datos.

5. Elija el almacén de datos de eventos para el panel. CloudTrail ejecutará consultas en este panel cuando se lo actualice.
6. Para ver la consulta de un widget, elija Ver y editar consulta en la parte inferior del widget.
7. 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](#).

8. Elija el icono de actualización para completar los gráficos de los widgets del panel. Cada widget indica el estado de la actualización.

## Guarde un panel administrado como un panel personalizado

No puede modificar un panel administrado, pero puede guardar una copia como panel personalizado. Esto le permite establecer un programa de actualización para el panel y modificar los widgets.

### Guardar un panel administrado como un panel personalizado

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. Elija el panel administrado para el que desea crear una copia.
5. Elija Guardar como panel nuevo.
6. Asigne un nombre para identificar el panel.
7. (Opcional) En la sección Etiquetas, puede agregar hasta 50 pares de claves de etiquetas para que lo ayuden a identificar y clasificar el panel. Para obtener más información sobre cómo usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.
8. En Permisos, elija los almacenes de datos de eventos a los que quiere aplicar los permisos. Como CloudTrail ejecuta consultas para completar los datos de los widgets de un panel, necesita permisos para ejecutar consultas en el almacén de datos de eventos asociado a los widgets del panel. Para cada almacén de datos de eventos seleccionado en este paso, CloudTrail asocia una política basada en recursos al almacén de datos de eventos que permite a CloudTrail ejecutar consultas. Puede quitar la selección un almacén de datos de eventos si no quiere conceder permisos.
9. Elija Crear panel.

Después de crear el panel personalizado, puede [agregar widgets](#) y [eliminar widgets](#), y [establecer un programa de actualización](#) para el panel.

## Paneles administrados disponibles

La sección ofrece información sobre los paneles administrados disponibles y sobre los widgets que aparecen en cada panel.

Paneles administrados disponibles:

- [Panel de supervisión de seguridad](#)
- [Panel de actividad de IAM](#)
- [Panel de actividad del usuario](#)
- [Panel de eventos enriquecidos](#)
- [Panel de análisis de errores](#)
- [Panel de actividad de EC2](#)
- [Panel de actividad de las organizaciones](#)
- [Panel de cambios de recursos](#)
- [Panel de información general sobre eventos de datos](#)
- [Panel de eventos de datos de Lambda](#)
- [Panel de eventos de datos de DynamoDB](#)
- [Panel de eventos de datos de S3](#)
- [Panel de eventos de Insights](#)
- [Panel de eventos de administración](#)
- [Panel de información general](#)

### Panel de supervisión de seguridad

Este panel ofrece una vista centralizada de los widgets fundamentales centrados en la seguridad, como los eventos principales de acceso denegado, los intentos erróneos de inicio de sesión de la consola y sus direcciones IP asociadas, los intentos de inicio de sesión de la consola del usuario raíz, las acciones destructivas, el acceso entre cuentas y otros widgets fundamentales centrados en la seguridad. Brinda una detección y una respuesta rápidas a los incidentes para mejorar la postura de seguridad general.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

## Eventos principales de acceso denegado

Realiza un seguimiento de los eventos de acceso denegado que suceden con más frecuencia, agrupados por API.

## Intentos de ConsoleLogin erróneos

Realiza un seguimiento de la tendencia de intentos erróneos de inicio de sesión en la consola a lo largo del tiempo, con desgloses entre los remitentes autenticados de MFA y de no MFA.

## Intentos de ConsoleLogin erróneos por dirección IP

Realiza un seguimiento de las direcciones IP asociadas a los intentos erróneos de inicio de sesión de la consola y muestra las direcciones IP más infractoras según el recuento de inicios de sesión erróneos.

## Intentos de ConsoleLogin del usuario raíz

Realiza un seguimiento de la frecuencia de los intentos de inicio de sesión de la consola realizados por los usuarios raíz a lo largo del tiempo.

## Acciones destructivas

Realiza un seguimiento de la frecuencia de las operaciones de eliminación a lo largo del tiempo.

## Acceso entre cuentas principal

Realiza un seguimiento de la actividad principal entre cuentas según el ID de cuenta del remitente y la acción.

## Usuarios que han desactivado la MFA

Realiza un seguimiento de los usuarios más recientes que desactivaron la MFA.

## Cambios recientes de EC2 SecurityGroup y NetworkAcl

Realiza un seguimiento de los cambios más recientes de EC2 SecurityGroup y NetworkAcl.

## Cambios recientes de EC2 SecurityGroup que permiten el acceso público

Realiza un seguimiento de los grupos de seguridad de EC2 más recientes que tienen reglas que permiten el acceso público (0.0.0.0/0).

## Posibles acciones de desactivación de CloudTrail

Realiza un seguimiento de las acciones recientes que corren el riesgo de interrumpir el registro de CloudTrail.

## Panel de actividad de IAM

Este panel ofrece visibilidad de las API de IAM más utilizadas, los errores de API, los cambios en las entidades de IAM y las direcciones IP de los principales remitentes, lo que permite identificar las acciones de IAM no deseadas y los problemas de cumplimiento.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

### API de IAM principales

Realiza un seguimiento de las API de IAM utilizadas con más frecuencia.

### Remitentes de IAM principales

Realiza un seguimiento de los remitentes de la API de IAM más frecuentes.

### Tendencia de éxito frente a error de IAM

Realiza un seguimiento de la tendencia del éxito y de las llamadas erróneas a la API de IAM a lo largo del tiempo.

### Errores principales de la API de IAM

Realiza un seguimiento de los errores más frecuentes al llamar a las API de IAM.

### API de IAM principales de AccessDenied

Realiza un seguimiento de las llamadas a la API de IAM más frecuentes que produjeron errores de acceso denegado.

### Direcciones IP principales de las llamadas de IAM

Realiza un seguimiento de las principales direcciones IP de origen desde las que se realizaron las llamadas a la API de IAM.

### Cambios recientes en la política de IAM

Realiza un seguimiento de los cambios más recientes en las políticas de IAM, clasificados según la operación específica de la API de IAM que facilitó el cambio, el recurso de IAM (usuario, rol o grupo) asociado al cambio de política y el nombre de la política o ARN que se utilizó.

### Cambios recientes de usuario de IAM

Realiza un seguimiento de los cambios más recientes de los usuarios de IAM, clasificados según la API de IAM específica que facilita la administración de los usuarios, el usuario de IAM afectado por el cambio y la hora del evento.

## Roles de IAM asumidos principales

Realiza un seguimiento de los roles de IAM asumidos con más frecuencia.

### Panel de actividad del usuario

Este panel ofrece visibilidad de las tendencias de actividad de los usuarios, información sobre áreas clave como los principales usuarios activos, los patrones de tráfico de los usuarios, los usuarios con errores de acceso denegado, las operaciones recientes de los usuarios, los usuarios que realizaron actividades destructivas y los cambios en las políticas de IAM, así como las acciones de los usuarios privilegiados. Ayuda a detectar las acciones no deseadas de los usuarios y los riesgos de seguridad.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

#### Tendencias de actividad de los usuarios por ARN de usuario

Realiza un seguimiento de la tendencia de la actividad del usuario a lo largo del tiempo por ARN del usuario.

#### Tendencias de actividad de los usuarios por API

Realiza un seguimiento de la tendencia de la actividad de los usuarios a lo largo del tiempo por API.

#### Actividad del usuario más reciente

Realiza un seguimiento de las acciones más recientes de los usuarios.

#### Usuarios principales con errores

Realiza un seguimiento de los usuarios que tienen la mayor cantidad de errores.

#### Usuarios principales con errores de AccessDenied

Realiza un seguimiento de los usuarios que tienen la mayor cantidad de errores de AccessDenied.

#### Usuarios principales que realizan acciones destructivas

Realiza un seguimiento de los usuarios que realizan la mayor cantidad de acciones destructivas.

#### Usuarios principales que cambian las políticas de IAM

Realiza un seguimiento de los usuarios de IAM que realizan cambios frecuentes en las políticas de IAM.

## Acciones principales realizadas por posibles usuarios privilegiados de IAM

Realiza un seguimiento de las acciones más frecuentes de los usuarios de IAM con muchos privilegios, como los administradores.

### Panel de eventos enriquecidos

Este panel de eventos enriquecidos ofrece información sobre las tendencias de los recursos etiquetados, las actividades de entidades principales y las claves de condición global de AWS. Esta información le ayuda a analizar las distribuciones de recursos y de etiquetas de entidades principales más frecuentes, así como las claves de condición global que se utilizan con más frecuencia en las sesiones de roles, las solicitudes y las entidades principales en el contexto de las solicitudes.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

#### Eventos enriquecidos a lo largo del tiempo

Realiza un seguimiento del recuento de eventos enriquecidos a lo largo del tiempo.

#### Pares de valor de claves de etiquetas de recurso más frecuentes

Muestra los pares de valor de claves de etiquetas de recurso más utilizados en los eventos enriquecidos.

#### Pares de valor de claves de etiquetas de recurso más frecuentes con los recursos y usuarios asociados

Muestra los pares de valor de claves de etiquetas de recurso más utilizados e indica qué recursos utilizan estas etiquetas y qué usuarios están asociados a ellas.

#### Pares de valor de claves de etiquetas de entidad principal más frecuentes

Muestra los pares de valor de claves de etiquetas de entidad principal más utilizados en los eventos enriquecidos.

#### Acciones de acceso denegado más frecuentes agrupadas por pares de valor de etiquetas de entidad principal

Muestra las acciones de acceso denegado más frecuentes agrupadas por pares de valor de etiquetas de entidad principal.

## Propiedades de entidad principal más frecuentes en las claves de condición global de IAM

Muestra las claves de condición global de IAM utilizadas con más frecuencia para las propiedades de entidad principal, con sus pares valor de claves y sus recuentos en todos los eventos.

## Propiedades de solicitud más frecuentes en las claves de condición global de IAM

Muestra las claves de condición global de IAM utilizadas con más frecuencia para las propiedades de solicitud, con sus pares valor de claves y sus recuentos en todos los eventos.

## Propiedades de sesión de roles más frecuentes en las claves de condición global de IAM

Muestra las claves de condición global de IAM utilizadas con más frecuencia para las propiedades de sesión de roles, con sus pares valor de claves y sus recuentos en todos los eventos.

## Panel de análisis de errores

Este panel ofrece información completa sobre las tendencias de error en los servicios, las API, los usuarios, los códigos de error y las API limitadas. La visibilidad permite la identificación de petición y la solución de problemas de disponibilidad potenciales para un rendimiento óptimo del sistema.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

### Recuento de errores por servicio

Realiza un seguimiento del recuento de errores de las actividades por servicio.

### Recuento de errores por API

Realiza un seguimiento del recuento de errores de las actividades por API.

### Errores principales por código de error

Realiza un seguimiento de los errores más frecuentes por código de error.

### Errores principales por mensaje de error

Realiza un seguimiento de los errores más frecuentes por mensaje de error.

### Errores principales de AccessDenied por API

Realiza un seguimiento de las API con los errores de acceso denegado notificados con más frecuencia.



## Errores principales limitados por API

Realiza un seguimiento de las API con los errores de limitación notificados con más frecuencia.

## Usuarios principales con errores

Realiza un seguimiento de los usuarios con los errores notificados con más frecuencia.

## Panel de actividad de EC2

Este panel ofrece una visibilidad completa de las actividades de administración de EC2, como las tendencias de las API, los errores de acceso, los lanzadores de instancias principales, los cambios de seguridad y las modificaciones de la red. La información ayuda a identificar los riesgos de seguridad y los problemas operativos.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

### Información general de la actividad de administración de instancias de EC2

Supervisa la información general de las actividades de administración de instancias de EC2 durante un tiempo específico y destaca las operaciones clave, como los lanzamientos, las detenciones y las terminaciones.

### Tendencias de éxito frente a error de las API de EC2

Realiza un seguimiento de la tendencia del éxito y de las llamadas erróneas a la API de EC2 a lo largo del tiempo.

### Errores principales de EC2

Realiza un seguimiento de los códigos de error más frecuentes que se producen durante las llamadas a la API de EC2.

### Eventos principales de AccessDenied de EC2

Realiza un seguimiento de las API de EC2 con la mayor cantidad de errores de acceso denegado.

### Usuarios principales que lanzan instancias de EC2

Realiza un seguimiento de los usuarios más activos en el lanzamiento de nuevas instancias de EC2.

## Cambios recientes en EC2 SecurityGroup y NetworkInterface

Realiza un seguimiento de los cambios más recientes en el grupo de seguridad y la interfaz de red de EC2.

## Cambios recientes en la tabla de enrutamiento y administración de VPC

Realiza un seguimiento de las actividades de administración de VPC más recientes y de los cambios en la tabla de enrutamiento.

## Acciones recientes de EC2 por parte del usuario raíz

Realiza un seguimiento de las acciones de EC2 más recientes realizadas por los usuarios raíz con permisos muy privilegiados.

## Panel de actividad de las organizaciones

Diseñado para los almacenes de datos de eventos de la organización, este panel ofrece visibilidad de las actividades y tendencias de la organización, incluida la información sobre los miembros activos, la administración de cuentas, los patrones de acceso, los cambios de las políticas y los principales servicios y API utilizados.

Este panel está disponible para los almacenes de datos de eventos de la organización e incluye los siguientes widgets:

### Tendencia de actividad en la organización

Realiza un seguimiento de la tendencia general de actividad en toda la organización de AWS Organizations a lo largo del tiempo, lo que ofrece visibilidad de los periodos de niveles de actividad altos o bajos.

### Resumen de administración de la cuenta de miembro

Realiza un seguimiento de la distribución de las actividades de administración de la cuenta de miembro dentro de la organización, clasificadas según los recuentos de cada tipo de actividad.

### Servicios más utilizados en toda la organización

Realiza un seguimiento de los Servicios de AWS que más se utilizaron en la organización.

### Cuentas más activas por servicio

Realiza un seguimiento de las cuentas más activas mediante el uso de un Servicio de AWS en toda la organización.

## API más utilizadas en toda la organización

Destaca las API de AWS que se invocaron con más frecuencia en toda la organización.

## Cuentas de miembros más activas

Realiza un seguimiento de las cuentas de los miembros de la organización que mostraron la mayor cantidad de actividad.

## Tendencia de errores de acceso denegado en toda la organización

Realiza un seguimiento del patrón de errores de acceso denegado que se producen en la organización a lo largo del tiempo.

## Cuentas con la mayoría de los errores de acceso denegado

Realiza un seguimiento de las cuentas de la organización que sufrieron la mayor cantidad de errores de acceso denegado.

## Cambios recientes de la política de control de servicios

Realiza un seguimiento de los cambios más recientes realizados en las políticas de control de servicios (SCP) dentro de la organización.

## Panel de cambios de recursos

Este panel ofrece una visión integral de las actividades de administración de recursos y supervisa las tendencias en el aprovisionamiento, la eliminación y las modificaciones en los servicios. Destaca los cambios fundamentales, incluidos los realizados a través de CloudFormation, de forma manual y en políticas como el bucket de S3 y el acceso a KMS.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

### Tendencias de creación y eliminación de recursos

Realiza un seguimiento de la creación y eliminación de recursos dentro de la cuenta a lo largo del tiempo.

### Usuarios principales que realizan la creación de recursos

Realiza un seguimiento de los usuarios que crean nuevos recursos de forma más activa.

## API principales utilizadas para la creación de recursos

Realiza un seguimiento de las API que se utilizan con más frecuencia para crear nuevos recursos en la cuenta.

## API principales utilizadas para la eliminación de recursos

Realiza un seguimiento de las API que se utilizan con más frecuencia para eliminar recursos en la cuenta.

## Recursos más recientes creados fuera de CloudFormation

Realiza un seguimiento de los nuevos recursos creados fuera del gobierno de CloudFormation y hace hincapié en los cambios que no se gestionan mediante las plantillas de CloudFormation.

## Cambios de recursos más recientes realizados con la consola

Realiza un seguimiento de los cambios más recientes realizados en los recursos a través de Consola de administración de AWS.

## Cambios más recientes en el acceso al bucket de S3

Realiza un seguimiento de los cambios de acceso al bucket de S3 más recientes.

## Cambios de acceso a claves de KMS más recientes

Realiza un seguimiento de los cambios más recientes de la política de claves de KMS.

## Panel de información general sobre eventos de datos

Este panel ofrece una vista centralizada de los eventos de datos en el almacén de datos de eventos, incluidas las tendencias generales de actividad, los servicios principales, las API, las regiones, las API de planos de datos limitados y los usuarios principales del plano de datos. Este panel le ayuda a supervisar la actividad de la API del plano de datos para realizar auditorías y solucionar problemas.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos e incluye los siguientes widgets:

### Tendencia general de eventos de datos

Realiza un seguimiento de la tendencia de los eventos de datos generales que se producen en la cuenta a lo largo del tiempo.

## Servicios principales que generan eventos de datos

Realiza un seguimiento de los servicios que generan la mayor cantidad de actividad de datos dentro de la cuenta.

## API principales que generan eventos de datos

Realiza un seguimiento de las API que generan la mayor cantidad de actividad de datos dentro de la cuenta.

## Regiones principales que generan eventos de datos

Realiza un seguimiento de las regiones que generan la mayor cantidad de actividad de datos en la cuenta.

## API de plano de datos más limitadas

Realiza un seguimiento de las API del plano de datos que sufren frecuentes limitaciones en la cuenta.

## Usuarios principales de las API de plano de datos

Realiza un seguimiento de los usuarios principales que más utilizan las API del plano de datos en la cuenta.

## Panel de eventos de datos de Lambda

Este panel ofrece visibilidad de la actividad de la API del plano de datos de Lambda, incluidos los usuarios principales, las funciones que se invocan con frecuencia y los errores comunes de la API. Esta información le ayuda a auditar el uso de Lambda, detectar anomalías y mitigar los riesgos operativos o de seguridad.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos de Lambda e incluye los siguientes widgets:

### Actividad de la API del plano de datos de Lambda

Realiza un seguimiento de la tendencia de la actividad de la API del plano de datos de Lambda dentro de la cuenta a lo largo del tiempo.

### Tendencia de éxito frente a fracaso de las invocaciones de Lambda

Realiza un seguimiento de la tendencia de éxito y de las invocaciones erróneas de Lambda a lo largo del tiempo.

## Usuarios principales de invocaciones de Lambda

Realiza un seguimiento de los usuarios que más veces invocan funciones de Lambda en la cuenta.

## Principales funciones de Lambda invocadas

Realiza un seguimiento de las funciones de Lambda que se invocan con más frecuencia en la cuenta.

## Los 10 errores principales de la API de invocación de Lambda

Realiza un seguimiento de los 10 errores principales encontrados durante las llamadas a la API de invocación de Lambda.

## Usuarios más limitados de las invocaciones de Lambda

Realiza un seguimiento de los usuarios que experimentan la mayor cantidad de eventos de limitación para las invocaciones de Lambda.

## Panel de eventos de datos de DynamoDB

Este panel ofrece visibilidad de la actividad de las API del plano de datos de DynamoDB, incluidas las tendencias de uso, las API principales y los patrones de limitación relacionados con los usuarios y las tablas. Esta información le ayuda a auditar el uso de DynamoDB, detectar anomalías y mitigar los riesgos operativos o de seguridad.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos de DynamoDB e incluye los siguientes widgets:

### Actividad de datos de la cuenta de DynamoDB

Realiza un seguimiento de la tendencia de los eventos de datos de DynamoDB que se producen en la cuenta a lo largo del tiempo.

### Tendencia de éxito o fracaso de las API del plano de datos de DynamoDB

Realiza un seguimiento de la tendencia del éxito y de las llamadas erróneas a la API del plano de datos de DynamoDB a lo largo del tiempo.

### Las 10 API principales de plano de datos de DynamoDB

Muestra las 10 llamadas a la API principales del plano de datos de DynamoDB.

## Usuarios principales de las API de plano de datos de DynamoDB

Realiza un seguimiento de los usuarios que realizan la mayor cantidad de llamadas a las API del plano de datos de DynamoDB dentro de la cuenta.

## Los 10 errores principales de la API del plano de datos de DynamoDB

Realiza un seguimiento de los 10 errores principales al llamar a las API del plano de datos de DynamoDB.

## Los usuarios más limitados de las API de plano de datos de DynamoDB

Realiza un seguimiento de los usuarios con limitaciones más frecuentes al llamar a las API del plano de datos de DynamoDB.

## API de plano de datos de DynamoDB más limitadas

Realiza un seguimiento de las API del plano de datos de DynamoDB que sufren frecuentes limitaciones en la cuenta.

## Tablas de DynamoDB más limitadas

Realiza un seguimiento de las tablas de DynamoDB que presentan las tasas de limitación más altas de la cuenta.

## Panel de eventos de datos de S3

Este panel ofrece visibilidad de la actividad de la API del plano de datos de S3, incluidas las tendencias de uso, los objetos de S3 a los que más se accede, los usuarios principales de S3 y las acciones principales de S3. Esta información le ayuda a auditar el uso de S3, detectar anomalías y mitigar los riesgos operativos o de seguridad.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de datos de Amazon S3 e incluye los siguientes widgets:

### Actividad de la cuenta de S3

Realiza un seguimiento de la actividad de la cuenta de S3.

### Objetos a los que más se accede

Muestra los objetos de S3 a los que más se accede.

### Usuarios principales de S3

Realiza un seguimiento de los usuarios principales de S3.

## Acciones principales de S3

Realiza un seguimiento de las acciones principales de S3.

## Panel de eventos de Insights

Este panel ofrece visibilidad del desglose general de los eventos de Insights por tipo, así como de los usuarios principales y servicios que generan estos tipos de eventos. Además, muestra el recuento diario de eventos de Insights y una vista histórica de 30 días de las métricas 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.
- 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`.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de Insights e incluye los siguientes widgets:

### Tipos de Insight

Realiza un seguimiento de los eventos por tipo de Insights.

### Insights por fecha

Realiza un seguimiento de los eventos de Insights por fecha.

### Insights de tasa de llamada a la API por origen de eventos

Realiza un seguimiento de Insights de tasa de llamada a la API por origen de eventos. Para ver los datos de este widget, el almacén de datos de eventos de Insights debe estar configurado para recopilar información sobre la tasa de llamada a la API.



## Insights de tasa de errores de la API por origen de eventos

Realiza un seguimiento de Insights de tasa de errores de la API por origen de eventos. Para ver este widget, el almacén de datos de eventos de Insights debe estar configurado para recopilar información sobre la tasa de errores de la API.

## Insights de los usuarios principales

Muestra los usuarios principales con solicitudes que generan eventos de Insights.

## Eventos de Insights

Muestra los eventos recientes de Insights.

## Panel de eventos de administración

Este panel destaca la información sobre los eventos de acceso denegado, las acciones destructivas, los eventos de inicio de sesión de la consola, los errores principales por usuario, el uso de la versión de TLS y las llamadas de TLS desactualizadas por parte del usuario.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

### Eventos principales de acceso denegado

Realiza un seguimiento de los eventos principales que provocaron errores de acceso denegado.

### Errores principales por usuario

Realiza un seguimiento de los errores principales por usuario.

### Eventos de inicio de sesión de la consola

Muestra los eventos de inicio de sesión de la consola.

### Acciones destructivas

Realiza un seguimiento de las acciones que dieron lugar a acciones destructivas.

### Versión de TLS

Muestra las versiones de TLS.

### Llamadas de TLS desactualizadas por parte del usuario

Realiza un seguimiento de las llamadas que utilizan versiones de TLS desactualizadas por usuario.

## Panel de información general

Este panel destaca la información sobre los eventos de acceso denegado, las acciones destructivas, los eventos de inicio de sesión de la consola, los errores principales por usuario, el uso de la versión de TLS y las llamadas de TLS desactualizadas por parte del usuario.

Este panel está disponible para los almacenes de datos de eventos que recopilan eventos de administración e incluye los siguientes widgets:

### Actividad de la cuenta

Realiza un seguimiento de la actividad de lectura y escritura de la cuenta.

### Errores principales

Muestra los errores más frecuentes.

### Regiones más activas

Muestra las Regiones de AWS más activas.

### Servicios principales

Muestra los servicios principales.

### Eventos más limitados

Muestra los eventos más limitados.

### Usuarios principales

Muestra los usuarios principales.

## Habilitación del panel de aspectos destacados con la consola de CloudTrail

Habilite el panel de aspectos destacados para ver un resumen rápido de la actividad de AWS recopilada por los almacenes de datos de eventos de la cuenta. CloudTrail administra el panel de aspectos destacados e incluye widgets que son pertinentes para la cuenta. Los widgets que se muestran en el panel de aspectos destacados son únicos para cada cuenta. Estos widgets podrían mostrar la actividad anormal o las anomalías detectadas. Por ejemplo, en el panel de aspectos destacados se podría incluir el Widget de acceso entre cuentas total, que muestra si hay un aumento en la actividad anormal entre cuentas.

CloudTrail actualiza el panel de aspectos destacados cada 6 horas. En el panel se muestran los datos de las últimas 24 horas de la última actualización.

 Note

Solo puede habilitar el panel de aspectos destacados para los almacenes de datos de eventos que existan en la cuenta.

No puede establecer un programa de actualización para el panel de aspectos destacados ni agregar o eliminar widgets.

## Habilitar el panel de aspectos destacados

Utilice el procedimiento que se encuentra a continuación para habilitar el panel de aspectos destacados.

1. Inicie sesión en la Consola de administración de AWS 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. Seleccione la pestaña Aspectos destacados.
4. Como la ejecución de consultas genera cargos de CloudTrail, CloudTrail le solicita que revise la información de los costos antes de habilitar el panel de aspectos destacados. Para obtener información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

Seleccione Aceptar y habilitar los aspectos destacados para activar el panel de aspectos destacados.

5. En Permisos, elija los almacenes de datos de eventos a los que quiere aplicar los permisos. CloudTrail necesita estos permisos para ejecutar consultas en los almacenes de datos de eventos y actualizar el panel en su nombre. Para ofrecer los permisos, CloudTrail asocia una política basada en recursos predeterminada a cada almacén de datos de eventos seleccionado en este paso a fin de permitir a CloudTrail ejecutar las consultas en el almacén de datos de eventos. CloudTrail asocia una política basada en recursos al panel para permitir que CloudTrail actualice el panel cada 6 horas.

Puede modificar la política basada en recursos de un almacén de datos de eventos desde la página de detalles. Para modificar la política basada en recursos de un panel, seleccione Editar política en el menú Acciones del panel.

## 6. Elija Confirmar.

Al activar el panel de aspectos destacados, la protección contra la terminación se activa de manera automática. La protección contra la terminación protege un panel de una eliminación accidental. Si quiere desactivar el panel, tendrá que desactivar la protección contra la terminación.

## Desactivación del panel de aspectos destacados con la consola de CloudTrail

En esta sección se describe cómo deshabilitar el panel de aspectos destacados. Como la protección contra la terminación se habilita de manera automática en el panel de aspectos destacados, primero tendrá que desactivar la protección contra la terminación y, luego, el panel de aspectos destacados.

### Desactivar del panel de aspectos destacados

1. Inicie sesión en la Consola de administración de AWS 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. Seleccione la pestaña Aspectos destacados.
4. En Acciones, elija Cambiar protección contra la terminación.
5. Elija Deshabilitar.
6. Seleccione Save.
7. En Acciones, seleccione Desactivar los aspectos destacados.

## Cree un panel personalizado con la consola de CloudTrail

Puede crear paneles personalizados y agregar hasta 10 widgets a cada uno. Puede elegir agregar widgets de muestra o crear nuevos a partir de consultas SQL.

Cuando haya terminado de agregar widgets, puede actualizar de manera manual el panel o establecer un programa de actualización.

### Para crear un panel personalizado

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. Seleccione Crear mi propio panel.
5. Asigne un nombre al panel para identificarlo.
6. En Permisos, elija los almacenes de datos de eventos a los que quiere aplicar los permisos. Como CloudTrail ejecuta consultas para completar los datos de los widgets de un panel, CloudTrail necesita permisos para ejecutar consultas en los almacenes de datos de eventos asociados a los widgets del panel. Para cada almacén de datos de eventos seleccionado en este paso, CloudTrail asocia una política basada en recursos al almacén de datos de eventos que permite a CloudTrail ejecutar consultas en el almacén de datos de eventos para este panel.
7. (Opcional) En la sección Etiquetas, puede agregar hasta 50 pares de claves de etiquetas para que lo ayuden a identificar y clasificar el panel. Para obtener más información sobre cómo usar las etiquetas en AWS, consulte [Etiquetado de los recursos de AWS](#) en la Guía del usuario para el etiquetado de recursos de AWS.
8. Elija Crear panel.

A continuación, puede agregar widgets y [establecer un programa de actualización](#).

## Temas

- [Agregue un widget de muestra con la consola de CloudTrail](#)
- [Creación de un widget nuevo a partir de una consulta SQL con la consola de CloudTrail](#)
- [Eliminar un widget de un panel con la consola de CloudTrail](#)

## Agregue un widget de muestra con la consola de CloudTrail

En esta sección se describe cómo agregar un widget de muestra a su panel. Puede agregar un máximo de 10 widgets a un panel personalizado.

### Note

Los widgets de muestra se limitan a un solo almacén de datos de eventos que existe en su cuenta. Para realizar consultas en varios almacenes de datos de eventos de su cuenta, [cree un widget nuevo](#).

## Agregar un widget de muestra a un panel

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En Paneles personalizados, elija el panel al que quiere agregar un widget.
5. En Acciones, elija Editar el panel.
6. En Acciones, elija Agregar widget de muestra.
7. Elija el almacén de datos de eventos en el que quiere ejecutar la consulta. Solo puede elegir almacenes de datos de eventos que existen en su cuenta.
8. Elija el widget de muestra que quiera agregar. De manera predeterminada, se muestran todos los widgets de muestra. Puede filtrar por tipo de widget (por ejemplo, widgets de IAM).
9. Seleccione Ver consulta para ver la consulta del widget seleccionado.
10. Elija Agregar al panel para agregar el widget al panel.
11. Elija Guardar para guardar el panel.

## Creación de un widget nuevo a partir de una consulta SQL con la consola de CloudTrail

En esta sección se describe cómo crear un widget nuevo al escribir o pegar una consulta SQL y elegir un tipo de gráfico. Puede agregar un máximo de 10 widgets a un panel personalizado.

### Crear de un widget nuevo a partir de una consulta SQL

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En Paneles personalizados, elija el panel para el que desea crear un widget.
5. En Acciones, elija Editar el panel.
6. En Acciones, elija Crear widget nuevo.

7. Elija el almacén de datos de eventos en el que quiere ejecutar la consulta. Puede realizar consultas en varios almacenes de datos de eventos siempre que los almacenes de datos de eventos existan en su cuenta.
8. Escribir o copiar la consulta SQL.

También puede ofrecer una petición en lenguaje natural en inglés y elegir Generar consulta para generar una consulta SQL a partir de la petición. Para obtener más información, consulte [Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural](#).

9. Elija Ejecutar para ejecutar la consulta y obtener una vista previa de los resultados de la consulta.

 Note

Cuando ejecuta consultas, incurre en cargos según la cantidad de datos optimizados y comprimidos que se escanean. Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales `eventTime` de inicio y finalización a las consultas.

10. Elija la pestaña Visualizador para seleccionar el tipo de gráfico para el widget. Puede elegir entre estos tipos de gráficos: tabla, gráfico de barras, gráfico de líneas y gráfico circular.
11. Elija Agregar al panel para agregar el widget al panel.
12. Elija Guardar para guardar el panel.

## Eliminar un widget de un panel con la consola de CloudTrail

En esta sección se describe cómo eliminar un widget de un panel personalizado.

### Eliminar un widget desde un panel

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En Paneles personalizados, elija el panel del que quiera eliminar un widget.
5. En Acciones, elija Editar el panel.

6. En el widget que quiere eliminar, elija el icono de eliminar



)

y, luego, elija Eliminar.

7. Elija Guardar para guardar el panel.

## Establezca un programa de actualización de un panel personalizado con la consola de CloudTrail

En esta sección se describe cómo establecer un programa de actualización del panel. Puede configurar un programa de actualización para permitir que CloudTrail Lake actualice un panel cada 1 hora, 6 horas, 12 horas o 24 horas (1 día).

Cuando configura un programa de actualización mediante la consola de CloudTrail, CloudTrail asocia una política basada en recursos al panel que le permite actualizar el panel en su nombre.

### Establecer un programa de actualización

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En Paneles personalizados, elija el panel para el que desea establecer un programa de actualización.
5. Elija la frecuencia de actualización en la lista desplegable.
6. A fin de crear un programa de actualización, CloudTrail asocia una política basada en recursos al panel para permitir que CloudTrail actualice el panel en su nombre. Amplíe la política de recursos del panel para ver la política basada en recursos que CloudTrail asociará al panel.
7. Como la ejecución de consultas implica costos, CloudTrail le solicita que confirme que quiere ejecutar las consultas con la frecuencia programada. Elija Confirmar para establecer un programa de actualización.

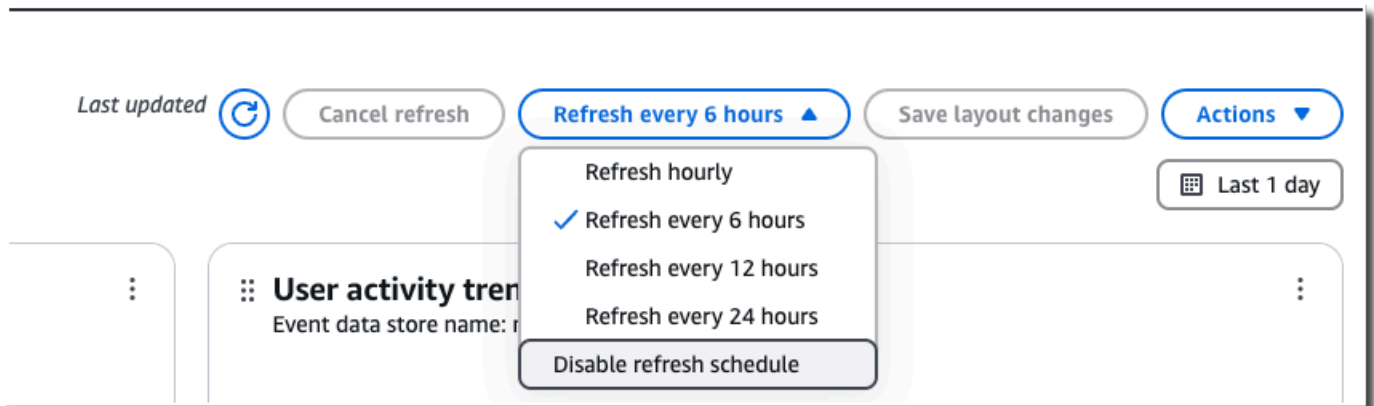


## Deshabilite un programa de actualización de un panel personalizado con la consola de CloudTrail

Puede desactivar el programa de actualización si ya no quiere que CloudTrail actualice de manera automática su panel y, en cambio, quiere actualizarlo de forma manual.

### Desactivar un programa de actualización

1. Inicie sesión en la Consola de administración de AWS 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 la pestaña Paneles administrados y personalizados.
4. En Paneles personalizados, elija el panel para el que quiere deshabilitar un programa de actualización.
5. Seleccione Deshabilitar el programa de actualización en la lista desplegable.



## Cambio de la protección contra la terminación con la consola de CloudTrail

La protección contra la terminación evita que un panel se elimine accidentalmente. Si quiere eliminar un panel personalizado o deshabilitar el panel de aspectos destacados, debe deshabilitar la protección contra la terminación.

### Para desactivar la protección contra la terminación

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija Lake y, luego, Panel.

3. Elija el tipo de panel para el que quiere deshabilitar la protección contra la terminación.
4. En Acciones, elija Cambiar protección contra la terminación.
5. Elija Deshabilitar.
6. Seleccione Save.

Para activar la protección contra la terminación

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija Lake y, luego, Panel.
3. Elija el tipo de panel para el que quiere habilitar la protección contra la terminación.
4. En Acciones, elija Cambiar protección contra la terminación.
5. Para habilitar la protección de terminación, elija Habilitada.
6. Seleccione Save.

## Eliminación de un panel personalizado con la consola de CloudTrail.

En esta sección, se describe cómo eliminar un panel mediante CloudTrail.

### Note

No puede eliminar un almacén de datos de eventos si la [protección contra la terminación](#) está habilitada.

### Eliminación de un panel

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija Lake y, luego, Panel.
3. Elija la pestaña Paneles administrados y personalizados.
4. Elija el panel personalizado que quiere eliminar.
5. En Acciones, seleccione Eliminar.

6. Elija Eliminar para confirmar que quiere eliminar el panel.

## Crear, actualizar y administrar los paneles con la AWS CLI

En esta sección se describen los comandos de AWS CLI que puede usar para crear, actualizar y administrar los paneles de CloudTrail Lake.

Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la Región de AWS 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.

### Comandos disponibles para los paneles

Los comandos para crear y actualizar paneles en CloudTrail Lake son los siguientes:

- `create-dashboard` para crear un panel personalizado o habilitar el panel de aspectos destacados.
- `update-dashboard` para actualizar un panel personalizado o el panel de aspectos destacados.
- `delete-dashboard` para eliminar un panel personalizado o el panel de aspectos destacados.
- `get-dashboard` devuelve información sobre el panel especificado.
- `list-dashboards` muestra todos los paneles de su Cuenta de AWS o del filtro especificado.
- `start-dashboard-refresh` inicia una actualización del panel.
- `get-resource-policy` asocia la política basada en recursos al panel.
- `put-resource-policy` asocia una política basada en recursos a un panel para permitir a CloudTrail actualizar el panel de forma asíncrona en su nombre. También se asocia una política basada en recursos a un almacén de datos de eventos para permitir que CloudTrail ejecute consultas en el almacén de datos de eventos para completar los datos de los widgets del panel.
- `delete-resource-policy` elimina la política basada en recursos asociada a un panel.
- `add-tags` agrega etiquetas para identificar el panel.
- `remove-tags` elimina las etiquetas de un panel.
- `list-tags` hace una lista de etiquetas de un panel.

Para obtener una lista de los comandos disponibles para los almacenes de datos de eventos de CloudTrail Lake, consulte [Comandos disponibles para los almacenes de datos de eventos](#).

Para obtener una lista de los comandos disponibles para las consultas de CloudTrail Lake, consulte [Comandos disponibles para consultas de CloudTrail Lake](#).

Para obtener una lista de los comandos disponibles para las integraciones de CloudTrail Lake, consulte [Comandos disponibles para las integraciones de CloudTrail Lake](#).

Temas:

- [Creación de un panel con el AWS CLI](#)
- [Administre los paneles con el AWS CLI](#)
- [Eliminación de un panel con el AWS CLI](#)

## Creación de un panel con el AWS CLI

En esta sección se describe cómo utilizar el comando `create-dashboard` para crear un panel personalizado o el panel de aspectos destacados.

Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la Región de AWS 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.

CloudTrail ejecuta consultas para completar los widgets del panel durante una actualización manual o programada. Se deben conceder permisos a CloudTrail para ejecutar la operación `StartQuery` en cada almacén de datos de eventos asociado a un widget de panel. A fin de brindar permisos, ejecute el comando `put-resource-policy` para asociar una política basada en recursos a cada almacén de datos de eventos o edite la política del almacén de datos de eventos en la consola de CloudTrail. Para ver una política de ejemplo, consulte [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#).

A fin de establecer un programa de actualización, CloudTrail debe tener permisos para ejecutar la operación `StartDashboardRefresh` de actualización del panel en su nombre. A fin de brindar permisos, ejecute la operación `put-resource-policy` para asociar una política basada en recursos al panel o edite la política del panel en la consola de CloudTrail. Para ver una política de ejemplo, consulte [Ejemplo de política basada en recursos para un panel](#).

Ejemplos:

- [Creación de un panel personalizado con el AWS CLI](#)
- [Habilitación del panel de aspectos destacados con el AWS CLI](#)

- [Consulte las propiedades de los widgets](#)

## Creación de un panel personalizado con el AWS CLI

El siguiente procedimiento indica cómo crear un panel personalizado, asociar las políticas basadas en recursos necesarias a los almacenes de datos de eventos y al panel, y actualizar el panel para establecer y habilitar un programa de actualización.

### 1. Ejecutar `create-dashboard` para crear un panel

Al crear un panel personalizado, puede incluir una matriz con hasta 10 widgets. Un widget ofrece una representación gráfica de los resultados de una consulta. Cada widget consta de `ViewProperties`, `QueryStatement` y `QueryParameters`.

- `ViewProperties`: especifica las propiedades del tipo de vista. Para obtener más información, consulte [Consulte las propiedades de los widgets](#).
- `QueryStatement`: la consulta de CloudTrail se ejecuta cuando se actualiza el panel. Puede realizar consultas en varios almacenes de datos de eventos siempre que los almacenes de datos de eventos existan en su cuenta.
- `QueryParameters`: los siguientes valores de `QueryParameters` son compatibles con los paneles personalizados: `$Period$`, `$StartTime$` y `$EndTime$`. Para utilizar los `QueryParameters`, coloque a `?` en el lugar `QueryStatement` donde quiera sustituir el parámetro. CloudTrail completará los parámetros al ejecutar la consulta.

En el siguiente ejemplo se crea un panel con cuatro widgets, uno de cada tipo de vista.

#### Note

En este ejemplo, `?` está rodeado de comillas simples porque se utiliza con `eventTime`. Según el sistema operativo que utilice, es posible que necesite poner comillas de escape entre las comillas simples. Para obtener más información, consulte [Uso de entrecorillado y literales con cadenas en la AWS CLI](#).

```
aws cloudtrail create-dashboard --name AccountActivityDashboard \  
--widgets '[  
  {
```

```

    "ViewProperties": {
      "Height": "2",
      "Width": "4",
      "Title": "TopErrors",
      "View": "Table"
    },
    "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
  },
  {
    "ViewProperties": {
      "Height": "2",
      "Width": "4",
      "Title": "MostActiveRegions",
      "View": "PieChart",
      "LabelColumn": "awsRegion",
      "ValueColumn": "eventCount",
      "FilterColumn": "awsRegion"
    },
    "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT
100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
  },
  {
    "ViewProperties": {
      "Height": "2",
      "Width": "4",
      "Title": "AccountActivity",
      "View": "LineChart",
      "YAxisColumn": "eventCount",
      "XAxisColumn": "eventDate",
      "FilterColumn": "readOnly"
    },
    "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate,
IF(readOnly, 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly
ORDER BY DATE_TRUNC('?', eventTime), readOnly",
    "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$",
"$Period$"]
  },
  {

```

```
"ViewProperties": {
  "Height": "2",
  "Width": "4",
  "Title": "TopServices",
  "View": "BarChart",
  "LabelColumn": "service",
  "ValueColumn": "eventCount",
  "FilterColumn": "service",
  "Orientation": "Horizontal"
},
"QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
"QueryParameters": ["$StartTime$", "$EndTime$"]
}
]'
```

2. Cree un archivo independiente con la política de recursos necesaria para cada almacén de datos de eventos que se incluya en la QueryStatement del widget. Nombre el archivo *policy.json*, con el siguiente ejemplo de instrucción de la política:

Reemplace *123456789012* por el ID de su cuenta, *arn:aws:cloudtrail:us-east-1:123456789012:dashboard/exampleDashboard* por el ARN del panel.

Para obtener más información sobre las políticas basadas en recursos para los paneles, consulte [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#).

3. Ejecute el comando `put-resource-policy` para asociar la política. También puede actualizar la política basada en recursos de un almacén de datos de eventos en la consola de CloudTrail.

En el siguiente ejemplo se asocia la política basada en recursos a un almacén de datos de eventos.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy file://policy.json
```

4. Ejecute el comando `put-resource-policy` para asociar una política basada en recursos al panel. Para ver una política de ejemplo, consulte [Ejemplo de política basada en recursos para un panel](#).

En el siguiente ejemplo se asocia una política basada en recursos a un panel. Reemplace *account-id* por su ID de cuenta y *dashboard-arn* por el ARN del panel.

```
aws cloudtrail put-resource-policy \  
--resource-arn dashboard-arn \  
--resource-policy '{"Version": "2012-10-17", "Statement":  
  [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":  
    "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",  
    "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",  
      "AWS:SourceAccount": "account-id"}}}]}'
```

5. Ejecute el comando `update-dashboard` para establecer y habilitar un programa de actualización configurando el parámetro `--refresh-schedule`.

El `--refresh-schedule` consta de los siguientes parámetros opcionales:

- **Frequency:** el Unit y Value para el programa.

Para los paneles personalizados, la unidad puede ser HOURS o DAYS.

En el caso de los paneles personalizados, los siguientes valores son válidos cuando la unidad es HOURS, 1, 6, 12, 24.

En el caso de los paneles personalizados, el único valor válido cuando la unidad es DAYS es 1.

- **Status:** especifica si el programa de actualización está habilitado. Establezca el valor en ENABLED para habilitar el programa de actualización o DISABLED para deshabilitarlo.
- **TimeOfDay** : la hora del día en UTC en la que se ejecuta el programa; para ver solo por hora, consulte los minutos; el valor predeterminado es 00:00.

En el siguiente ejemplo, se establece un programa de actualización para cada seis horas y se habilita el programa.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \  
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":  
  "ENABLED"}'
```



## Habilitación del panel de aspectos destacados con el AWS CLI

El siguiente procedimiento indica cómo crear un panel de aspectos destacados, asociar las políticas basadas en recursos necesarias a los almacenes de datos de eventos y al panel, y actualizar el panel para establecer y habilitar un programa de actualización.

1. Ejecute el comando `create-dashboard` para crear el panel de aspectos destacados. A fin de crear este panel, `--name` debe ser `AWSCloudTrail-Highlights`.

```
aws cloudtrail create-dashboard --name AWSCloudTrail-Highlights
```

2. Para cada almacén de datos de eventos de su cuenta, ejecute el comando `put-resource-policy` a fin de asociar una política basada en recursos al almacén de datos de eventos. También puede actualizar la política basada en recursos de un almacén de datos de eventos en la consola de CloudTrail. Para ver una política de ejemplo, consulte [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#).

En el siguiente ejemplo se asocia la política basada en recursos a un almacén de datos de eventos. Reemplace *account-id* por su ID de cuenta, *eds-arn* por el ARN del almacén de datos del evento y *dashboard-arn* por el ARN del panel.

```
aws cloudtrail put-resource-policy \  
--resource-arn eds-arn \  
--resource-policy '{"Version": "2012-10-17", "Statement": [  
  [{"Sid": "EDSPolicy", "Effect": "Allow", "Principal": { "Service":  
    "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartQuery", "Condition":  
    { "StringEquals": { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount":  
      "account-id"}}} ]}'
```

3. Ejecute el comando `put-resource-policy` para asociar una política basada en recursos al panel. Para ver una política de ejemplo, consulte [Ejemplo de política basada en recursos para un panel](#).

En el siguiente ejemplo se asocia una política basada en recursos a un panel. Reemplace *account-id* por su ID de cuenta y *dashboard-arn* por el ARN del panel.

```
aws cloudtrail put-resource-policy \  
--resource-arn dashboard-arn \  
--resource-policy '{"Version": "2012-10-17", "Statement": [  
  [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":  
    "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
```

```
"Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
"AWS:SourceAccount": "account-id"}}}]}'
```

4. Ejecute el comando `update-dashboard` para establecer y habilitar un programa de actualización configurando el parámetro `--refresh-schedule`. Para el panel de aspectos destacados, la única UNIT válida es HOURS y lo único Value válido es 6.

```
aws cloudtrail update-dashboard --dashboard-id AWSCloudTrail-Highlights \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
"ENABLED"}'
```

## Consulte las propiedades de los widgets

En esta sección, se describen las propiedades de vista que pueden configurarse para los cuatro tipos de vista: tabla, gráfico de líneas, gráfico circular y gráfico de barras.

Tipos de vistas:

- [Tabla](#)
- [Gráfico de líneas](#)
- [Gráfico circular](#)
- [Gráfico de barras](#)

## Tabla

En el siguiente ejemplo, se muestra un widget configurado como una tabla.

```
{
  "ViewProperties": {
    "Height": "2",
    "Width": "4",
    "Title": "TopErrors",
    "View": "Table"
  },
  "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
ORDER BY eventCount DESC LIMIT 100",
  "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

En la siguiente tabla, se describen las propiedades de vista que pueden configurarse para una tabla.

| Parámetro | Obligatorio | Valor                                                                   |
|-----------|-------------|-------------------------------------------------------------------------|
| Height    | Sí          | La altura de la tabla en pulgadas.                                      |
| Width     | Sí          | El ancho de la tabla en pulgadas.                                       |
| Title     | Sí          | El título de la tabla.                                                  |
| View      | Sí          | El tipo de vista del widget. En el caso de una tabla, el valor esTable. |

## Gráfico de líneas

En el siguiente ejemplo, se muestra un widget configurado como un gráfico de líneas.

```
{
  "ViewProperties": {
    "Height": "2",
    "Width": "4",
    "Title": "AccountActivity",
    "View": "LineChart",
    "YAxisColumn": "eventCount",
    "XAxisColumn": "eventDate",
    "FilterColumn": "readOnly"
  },
  "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate, IF(readOnly, 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly ORDER BY DATE_TRUNC('?', eventTime), readOnly",
  "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$", "$Period$"]
}
```

En la siguiente tabla, se describen las propiedades de vista que pueden configurarse para un gráfico de líneas.

| Parámetro    | Obligatorio | Valor                                                                                                              |
|--------------|-------------|--------------------------------------------------------------------------------------------------------------------|
| Height       | Sí          | La altura del gráfico de líneas en pulgadas.                                                                       |
| Width        | Sí          | El ancho del gráfico de líneas en pulgadas.                                                                        |
| Title        | Sí          | El título del gráfico de líneas.                                                                                   |
| View         | Sí          | El tipo de vista del widget.<br>En el caso de un gráfico de líneas, el valor es LineChart .                        |
| YAxisColumn  | Sí          | El campo de los resultados de la consulta que quiere utilizar para la columna del eje Y. Por ejemplo, eventCount . |
| XAxisColumn  | Sí          | El campo de los resultados de la consulta que quiere utilizar para la columna del eje X. Por ejemplo, eventDate .  |
| FilterColumn | No          | El campo de los resultados de la consulta que quiere filtrar. Por ejemplo, readOnly.                               |

## Gráfico circular

En el siguiente ejemplo, se muestra un widget configurado como un gráfico circular.

```
{
  "ViewProperties": {
    "Height": "2",
    "Width": "4",
    "Title": "MostActiveRegions",
    "View": "PieChart",
```

```

    "LabelColumn": "awsRegion",
    "ValueColumn": "eventCount",
    "FilterColumn": "awsRegion"
  },
  "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
  "QueryParameters": ["$StartTime$", "$EndTime$"]
}

```

En la siguiente tabla, se describen las propiedades de vista que pueden configurarse para un gráfico circular.

| Parámetro    | Obligatorio | Valor                                                                                  |
|--------------|-------------|----------------------------------------------------------------------------------------|
| Height       | Sí          | La altura del gráfico circular en pulgadas.                                            |
| Width        | Sí          | El ancho del gráfico circular en pulgadas.                                             |
| Title        | Sí          | El título del gráfico circular.                                                        |
| View         | Sí          | El tipo de vista del widget. En el caso de un gráfico circular, el valor es PieChart.  |
| LabelColumn  | Sí          | La etiqueta de los segmentos del gráfico circular. Por ejemplo, awsRegion .            |
| ValueColumn  | Sí          | El valor de los segmentos del gráfico circular. Por ejemplo, ValueColumn .             |
| FilterColumn | No          | El campo de los resultados de la consulta que quiere filtrar. Por ejemplo, awsRegion . |

## Gráfico de barras

En el siguiente ejemplo, se muestra un widget configurado como un gráfico de barras.

```
{
  "ViewProperties": {
    "Height": "2",
    "Width": "4",
    "Title": "TopServices",
    "View": "BarChart",
    "LabelColumn": "service",
    "ValueColumn": "eventCount",
    "FilterColumn": "service",
    "Orientation": "Horizontal"
  },
  "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
  "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

En la siguiente tabla, se describen las propiedades de vista que pueden configurarse para un gráfico de barras.

| Parámetro   | Obligatorio | Valor                                                                                                   |
|-------------|-------------|---------------------------------------------------------------------------------------------------------|
| Height      | Sí          | La altura del gráfico de barras en pulgadas.                                                            |
| Width       | Sí          | Ancho del gráfico de barras en pulgadas.                                                                |
| Title       | Sí          | El título del gráfico de barras.                                                                        |
| View        | Sí          | El tipo de vista del widget.<br>En el caso de un gráfico de barras, el valor es <code>BarChart</code> . |
| LabelColumn | Sí          | La etiqueta de las barras del gráfico de barras. Por ejemplo, <code>service</code> .                    |

| Parámetro    | Obligatorio | Valor                                                                                             |
|--------------|-------------|---------------------------------------------------------------------------------------------------|
| ValueColumn  | Sí          | El valor de las barras del gráfico de barras. Por ejemplo, <code>eventCount</code> .              |
| FilterColumn | No          | El campo de los resultados de la consulta que quiere filtrar. Por ejemplo, <code>service</code> . |
| Orientation  | No          | La orientación del gráfico de barras, ya sea <code>Horizontal</code> o <code>Vertical</code> .    |

## Administre los paneles con el AWS CLI

En esta sección, se describen distintos comandos que puede ejecutar para administrar sus paneles, como obtener un panel, enumerar sus paneles, actualizar un panel.

Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la Región de AWS 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.

Ejemplos:

- [Obtenga un panel con AWS CLI](#)
- [Enumere los paneles con el AWS CLI](#)
- [Asocie una política basada en recursos a un almacén de datos de eventos o a un panel con el AWS CLI](#)
- [Actualice de manera manual un panel con el AWS CLI](#)
- [Actualización de un panel con el AWS CLI](#)

### Obtenga un panel con AWS CLI

Ejecute el comando `get-dashboard` para volver a un panel. Especifique el `--dashboard-id` mediante el ARN del panel o el nombre del panel.

```
aws cloudtrail get-dashboard --dashboard-id arn:aws:cloudtrail:us-east-1:123456789012:dashboard/exampleDash
```

Enumere los paneles con el AWS CLI

Ejecute el comando `list-dashboards` para enumerar los paneles de su cuenta.

- Incluya el parámetro `--type` para ver solo los paneles CUSTOM o MANAGED.
- Incluya el parámetro `--max-results` para limitar la cantidad de resultados. Los valores válidos son 1-100.
- Incluya los `--name-prefix` para volver a los paneles que coincidan con el prefijo especificado.

En el ejemplo siguiente, se muestran todos los paneles.

```
aws cloudtrail list-dashboards
```

En este ejemplo, se muestran solo los paneles de CUSTOM.

```
aws cloudtrail list-dashboards --type CUSTOM
```

En el siguiente ejemplo, se muestran solo los paneles de MANAGED.

```
aws cloudtrail list-dashboards --type MANAGED
```

En el último ejemplo se enumeran los paneles que coinciden con el prefijo especificado.

```
aws cloudtrail list-dashboards --name-prefix ExamplePrefix
```

Asocie una política basada en recursos a un almacén de datos de eventos o a un panel con el AWS CLI

Ejecute el comando `put-resource-policy` para aplicar una política basada en recursos a un almacén de datos de eventos o panel.

Asocie una política basada en recursos a un almacén de datos de eventos

Para ejecutar las consultas en un panel durante una actualización manual o programada, debe asociar una política basada en recursos a cada almacén de datos de eventos que esté asociado a un widget en el panel. Esto permite a CloudTrail Lake ejecutar las consultas en su nombre. Para obtener



más información sobre la política basada en recursos, consulte [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#).

En el siguiente ejemplo se asocia la política basada en recursos a un almacén de datos de eventos. Reemplace *account-id* por el ID de su cuenta, *eds-arn* por el ARN del almacén de datos de eventos para el que CloudTrail ejecutará las consultas y *dashboard-arn* por el ARN del panel.

```
aws cloudtrail put-resource-policy \  
--resource-arn eds-arn \  
--resource-policy '{"Version": "2012-10-17", "Statement": [{"Sid": "EDSPolicy",  
"Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":  
"cloudtrail:StartQuery", "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-  
arn", "AWS:SourceAccount": "account-id"}}}] }'
```

### Asociar una política basada en recursos a un panel

A fin de establecer un programa de actualización para un panel, tiene que asociar una política basada en recursos al panel para permitir que CloudTrail Lake actualice el panel en su nombre. Para obtener más información sobre la política basada en recursos, consulte [Ejemplo de política basada en recursos para un panel](#).

En el siguiente ejemplo se asocia una política basada en recursos a un panel. Reemplace *account-id* por su ID de cuenta y *dashboard-arn* por el ARN del panel.

```
aws cloudtrail put-resource-policy \  
--resource-arn dashboard-arn \  
--resource-policy '{"Version": "2012-10-17", "Statement":  
[{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":  
"cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",  
"Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",  
"AWS:SourceAccount": "account-id"}}}] }'
```

### Actualice de manera manual un panel con el AWS CLI

Ejecute el comando `start-dashboard-refresh` para actualizar de manera manual el panel. Antes de ejecutar este comando, debe [asociar una política basada en recursos](#) a cada almacén de datos de eventos asociado a un widget de panel.

En el siguiente ejemplo, se muestra cómo actualizar de manera manual un panel personalizado.

```
aws cloudtrail start-dashboard-refresh \  
--dashboard-id dashboard-id \  

```

```
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z"}'
```

En el siguiente ejemplo, se muestra cómo actualizar de manera manual un panel administrado. Como CloudTrail configura los paneles administrados, la solicitud de actualización debe incluir el ID del almacén de datos de eventos en el que se ejecutarán las consultas.

```
aws cloudtrail start-dashboard-refresh \  
--dashboard-id dashboard-id \  
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z", "$EventDataStoreId $": "eds-id"}'
```

## Actualización de un panel con el AWS CLI

Ejecute el comando `update-dashboard` para actualizar un panel. Puede actualizar el panel para establecer un programa de actualización, habilitar o deshabilitar un programa de actualización, modificar los widgets y habilitar o deshabilitar la protección contra la terminación.

Actualice el programa de actualización con el AWS CLI

En el ejemplo siguiente, se actualiza el programa de actualización de un panel personalizado conocido como `AccountActivityDashboard`.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \  
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status": "ENABLED"}'
```

Deshabilite la protección contra la terminación y el programa de actualización en un panel personalizado con AWS CLI

En el siguiente ejemplo, se deshabilita la protección contra la terminación de un panel personalizado conocido como `AccountActivityDashboard` para permitir eliminarlo. También deshabilita el programa de actualización.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \  
--refresh-schedule '{ "Status": "DISABLED"}' \  
--no-termination-protection-enabled
```

## Agregar un widget a un panel personalizado

En el siguiente ejemplo, se agrega un widget nuevo conocido como `TopServices` al panel personalizado denominado `AccountActivityDashboard`. La matriz de widgets incluye los dos widgets que ya se crearon para el panel y el widget nuevo.

**Note**

En este ejemplo, ? está rodeado de comillas simples porque se utiliza con `eventTime`. Según el sistema operativo que utilice, es posible que necesite poner comillas de escape entre las comillas simples. Para obtener más información, consulte [Uso de entrecomillado y literales con cadenas en la AWS CLI](#).

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--widgets '[
  {
    "ViewProperties": {
      "Height": "2",
      "Width": "4",
      "Title": "TopErrors",
      "View": "Table"
    },
    "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
  },
  {
    "ViewProperties": {
      "Height": "2",
      "Width": "4",
      "Title": "MostActiveRegions",
      "View": "PieChart",
      "LabelColumn": "awsRegion",
      "ValueColumn": "eventCount",
      "FilterColumn": "awsRegion"
    },
    "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
  },
  {
    "ViewProperties": {
      "Height": "2",
      "Width": "4",
      "Title": "TopServices",
      "View": "BarChart",
```

```
    "LabelColumn": "service",
    "ValueColumn": "eventCount",
    "FilterColumn": "service",
    "Orientation": "Vertical"
  },
  "QueryStatement": "SELECT replace(eventSource, '.amazonaws.com') AS service,
COUNT(*) as eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
  "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

## Eliminación de un panel con el AWS CLI

En esta sección, se describe cómo usar el comando AWS CLI `delete-dashboard` para eliminar el panel de CloudTrail Lake.

Para eliminar un panel, especifique el `--dashboard-id` mediante el ARN del panel o el nombre del panel.

```
aws cloudtrail delete-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

Si la operación se realiza correctamente, no se produce ninguna respuesta.

### Note

No puede eliminar un panel si está configurado `--termination-protection-enabled`.

## Consultas de CloudTrail Lake

Las consultas de CloudTrail Lake se crean en SQL. Puede crear una consulta en la pestaña Editor de CloudTrail Lake mediante la escritura de la consulta en SQL desde cero, la apertura de una consulta guardada o de muestra y su edición, o mediante el generador de consultas para crear una consulta a partir de una petición redactada en inglés. 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 [Restricciones SQL de CloudTrail Lake](#).

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 las 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'
```

Para obtener más información sobre cómo optimizar las consultas, diríjase a [Optimización de consultas de CloudTrail Lake](#).

## Temas

- [Herramientas del editor de consultas](#)
- [Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural](#)
- [Visualización de consultas de ejemplo con la consola de CloudTrail](#)
- [Creación o edición de una consulta con la consola de CloudTrail](#)
- [Ejecutar una consulta y guardar los resultados de la consulta con la consola](#)
- [Visualización de los resultados de la consulta con la consola](#)
- [Resumen de los resultados de las consultas en lenguaje natural](#)
- [Descarga de los resultados de consultas guardados](#)
- [Validar resultados de consultas guardados de CloudTrail Lake](#)
- [Optimización de consultas de CloudTrail Lake](#)
- [Ejecución y administración de consultas de CloudTrail Lake con la AWS CLI](#)

## 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.

## Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural

Puede usar el generador de consultas de CloudTrail Lake para generar una consulta a partir de una petición en inglés que proporcione. El generador de consultas usa inteligencia artificial generativa (IA generativa) para generar una consulta SQL lista para usar a partir de su petición, que luego puede ejecutar en el editor de consultas de Lake o afinar. No es necesario tener amplios conocimientos de los campos de eventos de SQL o CloudTrail para utilizar el generador de consultas.

La petición puede ser una pregunta o una instrucción sobre los datos de eventos del almacén de datos de eventos de CloudTrail Lake. Por ejemplo, puede ingresar las peticiones como "What are my top errors in the past month?" y "Give me a list of users that used SNS."

La petición puede tener un mínimo de 3 caracteres y un máximo de 500.

La generación de consultas no conlleva cargos; sin embargo, al ejecutar consultas, incurre en cargos según la cantidad de datos optimizados y comprimidos que se escanean. Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales eventTime de inicio y finalización a las consultas.

### Note

Para enviar comentarios acerca de una consulta generada, pulse el botón con el pulgar hacia arriba o hacia abajo que aparece debajo de la consulta generada. Cuando envía comentarios, CloudTrail guarda su petición y la consulta generada.

No incluya ninguna información de identificación personal, confidencial o sensible en sus peticiones.

Esta característica usa modelos de lenguaje grandes (LLM) con IA generativa; se recomienda comprobar la respuesta del LLM.

Puede acceder al generador de consultas a través de la consola de CloudTrail y AWS CLI.

## CloudTrail console

### Uso del generador de consultas en la consola de CloudTrail

1. Inicie sesión en la Consola de administración de AWS 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 Consulta, seleccione la pestaña Editor.
4. Elija el almacén de datos de eventos para el que desea crear una consulta.
5. En el área del Generador de consultas, introduzca una petición en un inglés sencillo. Para ver ejemplos, consulte [Ejemplos de peticiones](#).
6. Elija Generar consulta. El generador de consultas intentará generar una consulta a partir de su petición. Si se ejecuta correctamente, el generador de consultas proporciona la consulta SQL en el editor. Si la petición no funciona, reformúlela e inténtelo de nuevo.
7. (Opcional) Puede enviar los comentarios sobre la consulta generada. Para enviar comentarios, pulse el botón con el pulgar hacia arriba o hacia abajo que aparece debajo de la petición. Cuando envía comentarios, CloudTrail guarda su petición y la consulta generada.
8. (Opcional) Seleccione Ejecutar para ejecutar la consulta.

#### Note

Cuando ejecuta consultas, incurre en cargos según la cantidad de datos optimizados y comprimidos que se escanean. Para ayudar a controlar los costos, le recomendamos que restrinja las consultas agregando marcas temporales `eventTime` de inicio y finalización a las consultas.

9. (Opcional) Si ejecuta la consulta y hay resultados, puede elegir Resumir los resultados para generar un resumen en lenguaje natural en inglés de los resultados de la consulta. Esta opción utiliza inteligencia artificial generativa (IA generativa) para producir el resumen. Para

obtener más información acerca de esta opción, consulta [Resumen de los resultados de las consultas en lenguaje natural](#).

Para ofrecer comentarios sobre el resumen, elija el botón de aprobación hacia arriba o hacia abajo que aparece debajo del resumen generado.

 Note

La característica de resumen de consultas se encuentra en la versión preliminar para CloudTrail Lake y está sujeta a cambios. Esta característica está disponible en las siguientes regiones: Asia-Pacífico (Tokio), Este de EE. UU. (Norte de Virginia) y Oeste de EE. UU. (Oregón).

## AWS CLI

Para generar una consulta con AWS CLI

Ejecute el comando `generate-query` para generar una consulta a partir de una petición en inglés. En `--event-data-stores`, brinde el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos que quiera consultar. Solo puede especificar un almacén de datos de eventos. Para `--prompt`, brinde la petición en inglés.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

Si se realiza de manera correcta, el comando genera una instrucción SQL y ofrece una `QueryAlias` que utilizará junto con el comando `start-query` para ejecutar la consulta en el almacén de datos de eventos.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

Para ejecutar una consulta con AWS CLI



Ejecute el comando [start-query](#) con el QueryAlias generado por el comando generate-query del ejemplo anterior. También tiene la opción de ejecutar el comando start-query mediante la QueryStatement.

```
aws cloudtrail start-query --query-alias AWSCloudTrail-UUID
```

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.

```
{  
  "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](#).

## Permisos necesarios

Las políticas administradas [AWSCloudTrail\\_FullAccess](#) y [AdministratorAccess](#) brindan los permisos necesarios para utilizar esta característica.

También puede incluir la acción `cloudtrail:GenerateQuery` en una política integrada o administrada por el cliente, nueva o existente.

## Compatibilidad de regiones

Esta característica puede utilizarse en las siguientes Regiones de AWS:

- Región Asia-Pacífico (Mumbai) (ap-south-1)

- Región Asia-Pacífico (Sídney) (ap-southeast-2)
- Región Asia-Pacífico (Tokio) (ap-northeast-1)
- Región Canadá (Central) (ca-central-1)
- Región Europa (Londres) (eu-west-2)
- Región Este de EE. UU. (Norte de Virginia) (us-east-1)
- Región Oeste de EE. UU. (Oregón) (us-west-2)

## Limitaciones

A continuación se enumeran las limitaciones del generador de consultas:

- El generador de consultas solo acepta peticiones en inglés.
- El generador de consultas solo puede generar consultas para los almacenes de datos de eventos que recopilan eventos de CloudTrail (eventos de administración, de datos y de actividad de la red).
- El generador de consultas no puede generar consultas de peticiones que no pertenezcan a los datos de eventos de CloudTrail Lake.

## Ejemplos de peticiones

En esta sección se proporcionan ejemplos de peticiones y las consultas SQL resultantes generadas a partir de ellas.

Si decide ejecutar las consultas de ejemplo de esta sección, sustituya *eds-id* por el ID del almacén de datos de eventos que quiera consultar y sustituya las marcas temporales por las que correspondan a su caso de uso. Las marcas temporales tienen el siguiente formato: YYYY-MM-DD HH:MM:SS.

Petición: What are my top errors in the past month?

Consulta SQL:

```
SELECT
    errorMessage,
    COUNT(*) as eventCount
FROM
    eds-id
WHERE
    errorMessage IS NOT NULL
```

```
AND eventTime >= timestamp '2024-05-01 00:00:00'
AND eventTime <= timestamp '2024-05-31 23:59:59'
GROUP BY 1
ORDER BY 2 DESC
LIMIT 2;
```

Petición: Give me a list of users that used Amazon SNS.

Consulta SQL:

```
SELECT
    DISTINCT userIdentity.arn AS user
FROM
    eds-id
WHERE
    eventSource = 'sns.amazonaws.com'
```

Petición: What are my API counts each day for read and write events in the past month?

Consulta SQL:

```
SELECT date(eventTime) AS event_date,
    SUM(
        CASE
            WHEN readonly = true THEN 1
            ELSE 0
        END
    ) AS read_events,
    SUM(
        CASE
            WHEN readonly = false THEN 1
            ELSE 0
        END
    ) AS write_events
FROM
    eds-id
WHERE
    eventTime >= timestamp '2024-05-04 00:00:00'
AND eventTime <= timestamp '2024-06-04 23:59:59'
GROUP BY 1
ORDER BY 1 ASC;
```

Petición: Show any events with access denied errors for the past three weeks.

## Consulta SQL:

```
SELECT *
FROM
    eds-id
WHERE
    WHERE (errorCode = 'AccessDenied' OR errorMessage = 'Access Denied')
    AND eventTime >= timestamp '2024-05-16 01:00:00'
    AND eventTime <= timestamp '2024-06-06 01:00:00'
```

Petición: Query the number of calls each operator performed on the date 2024-05-01. The operator is a principal tag.

## Consulta SQL:

```
SELECT element_at(
    eventContext.tagContext.principalTags,
    'operator'
) AS operator,
COUNT(*) AS eventCount
FROM
    eds-id
WHERE eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
GROUP BY 1
ORDER BY 2 DESC;
```

Petición: Give me all event IDs that touched resources within the CloudFormation stack with name myStack on the date 2024-05-01.

## Consulta SQL:

```
SELECT eventID
FROM
    eds-id
WHERE any_match(
    eventContext.tagcontext.resourcetags,
    rt->element_at(rt.tags, 'aws:cloudformation:stack-name') = 'myStack'
)
AND eventtime >= '2024-05-01 00:00:00'
AND eventtime < '2024-05-01 23:59:59'
```

Petición: Count the number of events grouped by resource tag 'solution' values, listing them in descending order of count.

Consulta SQL:

```
SELECT element_at(rt.tags, 'solution'),
       count(*) as event_count
FROM
     eds-id,
     unnest(eventContext.tagContext.resourceTags) as rt
WHERE eventtime < '2025-05-14 19:00:00'
GROUP BY 1
ORDER BY 2 DESC;
```

Petición: Find all Amazon S3 data events where resource tag Environment has value prod.

Consulta SQL:

```
SELECT *
FROM
     eds-id
WHERE eventCategory = 'Data'
     AND eventSource = 's3.amazonaws.com'
     AND eventtime >= '2025-05-14 00:00:00'
     AND eventtime < '2025-05-14 20:00:00'
     AND any_match(
         eventContext.tagContext.resourceTags,
         rt->element_at(rt.tags, 'Environment') = 'prod'
     )
```

## Visualización de consultas de ejemplo con 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.

Las consultas de CloudTrail generan cargos según 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. Para obtener más información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

 Note

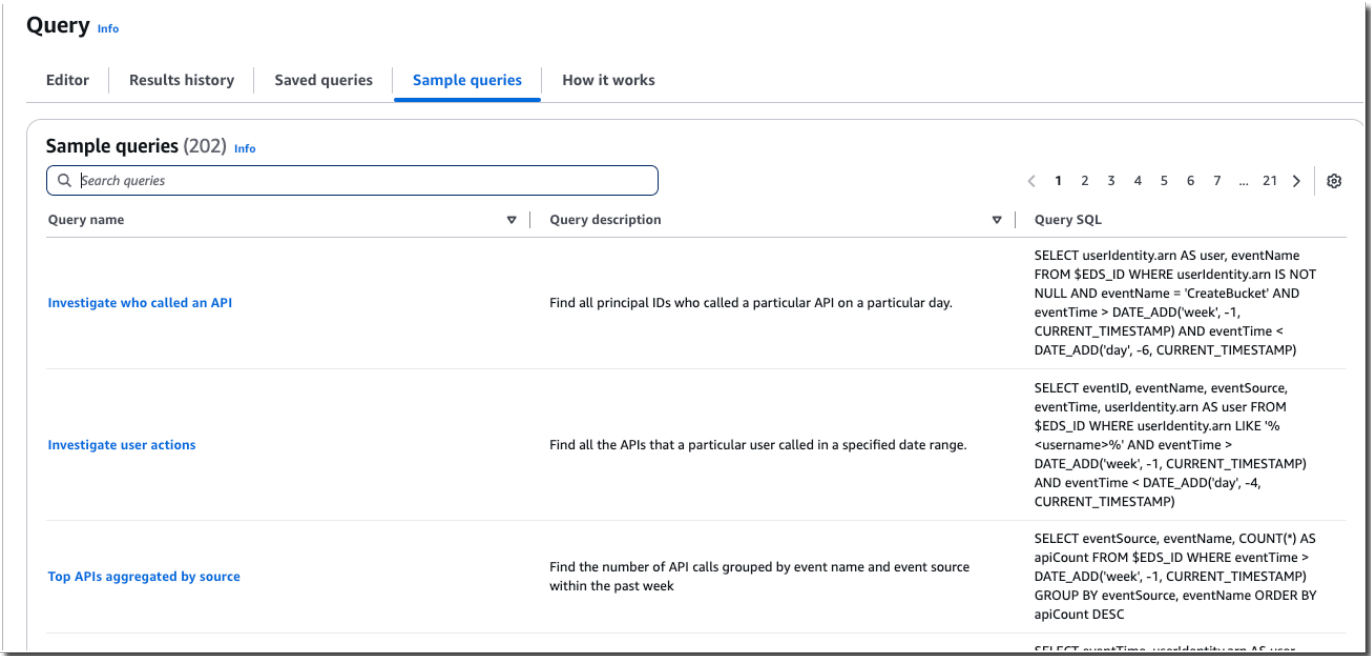
Además, puede ver consultas creadas por la comunidad de GitHub. Para obtener más información, consulte [Consultas de ejemplo de CloudTrail Lake](#) en el sitio web de GitHub. AWS CloudTrail no ha evaluado las consultas en GitHub.

Para ver y ejecutar una consulta de muestra

1. Inicie sesión en la Consola de administración de AWS 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. Elija una consulta de muestra de la lista o escriba una frase por la que buscar. 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.

 Note

De manera predeterminada, esta página utiliza la función de búsqueda básica. Puede mejorar la funcionalidad de búsqueda si agrega permisos para la acción `cloudtrail:SearchSampleQueries`, si su política de permisos aún no los proporciona. La política administrada de [AWSCloudTrail\\_FullAccess](#) ofrece los permisos para realizar la acción `cloudtrail:SearchSampleQueries`.



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

The screenshot shows the AWS CloudTrail Query console. On the left, the 'Event data store' section is highlighted with a yellow box, showing 'my-management-events-eds' selected. Below it, the 'Event properties' section lists various event attributes. The main area displays a SQL query: `SELECT userIdentity.arn AS user, eventName, eventTime, awsRegion, requestParameters AS resourceChangedManually FROM [redacted] WHERE sessionCredentialFromConsole='true' AND errorCode IS NULL AND eventTime > '2023-06-23 00:00:00'`. The 'Run' button is highlighted in orange. Below the query, the 'Query results' and 'Command output' tabs are visible, with 'Command output' selected. The 'Output' section shows a table with columns: Time stamp, Status, Delivery status, Response, Query SQL, Query ID, and Event data st... The 'Status' column for the first row is highlighted with a yellow box, showing 'Successful'.

## 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.

The screenshot shows the 'Command output' tab of the AWS CloudTrail Query console. The 'Output' section displays a table with columns: Time stamp, Status, Delivery status, Response, Query SQL, Query ID, and Event data st... The 'Status' column for the first row is highlighted with a yellow box, showing 'Successful'.

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.



Query results

Command output

Results

Info

Copy

Search queries

< 1 ... >

| <input type="checkbox"/> | user                                                  | eventName            | eventTime               | awsRegion |
|--------------------------|-------------------------------------------------------|----------------------|-------------------------|-----------|
| <input type="checkbox"/> | arn:aws:sts::[redacted]:assumed-role/Admin/[redacted] | UpdateEventDataStore | 2023-07-10 14:35:00.000 | us-east-1 |
| <input type="checkbox"/> | arn:aws:sts::[redacted]:assumed-role/Admin/[redacted] | LookupEvents         | 2023-07-07 23:10:14.000 | us-east-1 |
| <input type="checkbox"/> | arn:aws:sts::[redacted]:assumed-role/Admin/[redacted] | LookupEvents         | 2023-07-07 23:10:13.000 | us-east-1 |

Para obtener más información sobre la edición de una consulta, consulte [Creación o edición de una consulta con la consola de CloudTrail](#). Para obtener más información sobre cómo ejecutar una consulta y guardar los resultados, consulte [Ejecutar una consulta y guardar los resultados de la consulta con la consola](#).

## Creación o edición de una consulta con la consola de CloudTrail

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 Consola de administración de AWS 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).

## Save query



### Query name

3-64 characters. Only letters, numbers, periods, underscores, hyphens, and spaces are allowed.

### Query description

3-256 characters. Only letters, numbers, periods, underscores, hyphens, and spaces are allowed.

Cancel

Save query

**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.

- Abra la pestaña Saved queries (Consultas guardadas) para ver la nueva consulta en la tabla.

| Query <small>Info</small>                                                                                                                                                                                                                                               |                                    |                                                             |                                                                                                                                                                                                                     |                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| <div> <a href="#">Editor</a> <a href="#">Results history</a> <a href="#">Saved queries</a> <a href="#">Sample queries</a> <a href="#">How it works</a> </div>                                                                                                           |                                    |                                                             |                                                                                                                                                                                                                     |                                     |
| <div> <div>Saved queries (1) <small>Info</small></div> <div> <input type="text" value="Search queries"/> </div> <div> <span>&lt;</span> <span>1</span> <span>&gt;</span> <span>⌵</span> </div> <div> <span>↺</span> <span>Delete</span> <span>Edit</span> </div> </div> |                                    |                                                             |                                                                                                                                                                                                                     |                                     |
| <input type="checkbox"/>                                                                                                                                                                                                                                                | Query name                         | Query description                                           | Query SQL                                                                                                                                                                                                           | Time stamp                          |
| <input type="checkbox"/>                                                                                                                                                                                                                                                | Investigate actions taken by Alice | This query returns all actions taken by a user named Alice. | <pre>SELECT eventId, eventName, eventSource, eventTime, userIdentity.arn AS user FROM WHERE userIdentity.arn LIKE '%Alice%' AND eventTime &gt; '2023-06-23 00:00:00' AND eventTime &lt; '2023-06-26 00:00:00'</pre> | June 30, 2023, 17:17:50 (UTC-05:00) |

## Ejecutar una consulta y guardar los resultados de la consulta con la consola

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 Consola de administración de AWS 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. Si elige el bucket de S3 predeterminado, su política de IAM debe incluir permiso para la acción `s3:PutEncryptionConfiguration`, porque el cifrado en el servidor está habilitado de forma predeterminada para el bucket. 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 [Descarga de los 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 [Validar resultados de consultas guardados de CloudTrail Lake](#).

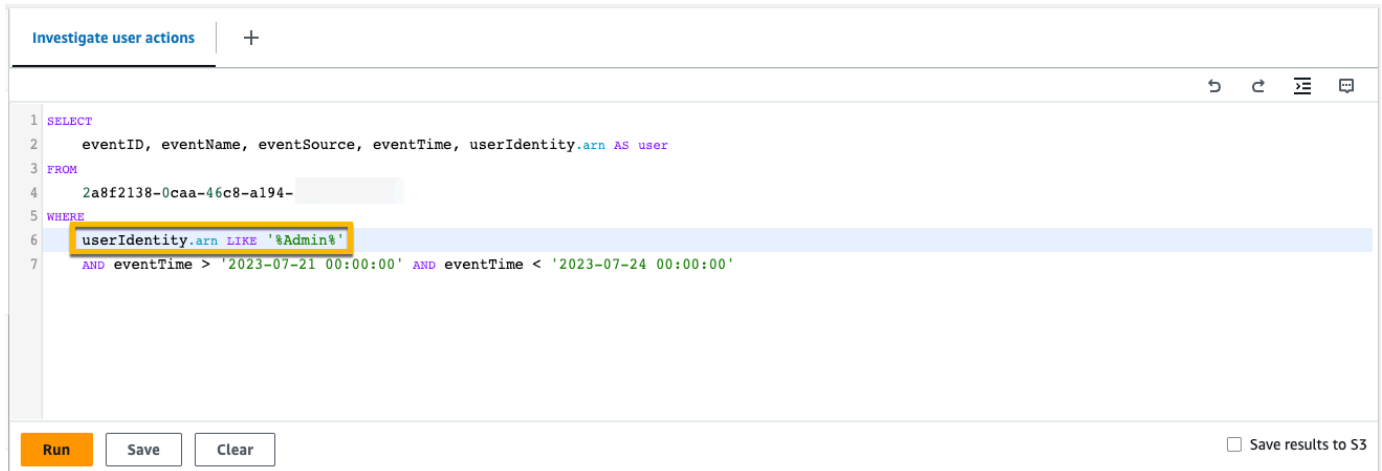
## Ejemplo: guardar los resultados de las consultas en un bucket de Amazon S3

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

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

1. Inicie sesión en la Consola de administración de AWS 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 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 seleccionar el almacén de datos de eventos de la lista, CloudTrail rellena automáticamente el ID del almacén de datos de eventos en la línea From.

- 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.



```
1 SELECT
2   eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
3 FROM
4   2a8f2138-0caa-46c8-a194-
5 WHERE
6   userIdentity.arn LIKE '%Admin%'
7   AND eventTime > '2023-07-21 00:00:00' AND eventTime < '2023-07-24 00:00:00'
```

Run Save Clear ☐ Save results to S3

- Seleccione 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. Si elige el bucket de S3 predeterminado, su política de IAM debe incluir permiso para la acción `s3:PutEncryptionConfiguration`, porque el cifrado en el servidor está habilitado de forma predeterminada para el bucket. 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 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](#).



7. Seleccione 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 complete la entrega de los resultados de las consultas guardados en su bucket de S3, la columna Estado de entrega proporciona un enlace al bucket de S3 que contiene los archivos de resultados de las consultas guardados, así como un [archivo de firma](#) que puede utilizar 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

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.

Query results

Command output

Output

< 1 > ⚙

| Time stamp              | Status       | Delivery status            | Response              | Query SQL                | Query ID               | Event data store      |
|-------------------------|--------------|----------------------------|-----------------------|--------------------------|------------------------|-----------------------|
| July 28, 2023, 18:20... | ✔ Successful | <a href="#">View in S3</a> | 468 records matche... | SELECT eventID, eventNar | 52ab2728-06de-4dac-8c5 | my-management-events- |

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.

52ab2728-06de-4dac-8c53-

/

Copy S3 URI

Objects

Properties

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

|                                     | Name             | Type | Last modified                       | Size    | Storage class |
|-------------------------------------|------------------|------|-------------------------------------|---------|---------------|
| <input checked="" type="checkbox"/> | result_1.csv.gz  | gz   | July 28, 2023, 13:20:12 (UTC-05:00) | 13.8 KB | Standard      |
| <input type="checkbox"/>            | result_sign.json | json | July 28, 2023, 13:20:18 (UTC-05:00) | 929.0 B | Standard      |

Para obtener información sobre la validación de resultados de consultas guardados, consulte [Validar resultados de consultas guardados de CloudTrail Lake](#).

## Visualización de los resultados de la consulta con la consola

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 [Descarga de los 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.

## Visualizar los resultados de la consulta

1. Seleccione la pestaña Resultados en el editor de consultas si aún no está seleccionada. 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. (Opcional) Elija Resumen de resultados para generar un resumen de lenguaje natural de los resultados de la consulta. El resumen se ofrece en inglés. Esta opción utiliza inteligencia artificial generativa (IA generativa) para producir el resumen. Para obtener más información acerca de esta opción, consulte [Resumen de los resultados de las consultas en lenguaje natural](#).

Para ofrecer comentarios sobre el resumen, elija el botón de aprobación hacia arriba o hacia abajo que aparece debajo del resumen generado.

 Note

La característica de resumen de consultas se encuentra en la versión preliminar para CloudTrail Lake y está sujeta a cambios. Esta característica está disponible en las siguientes regiones: Asia-Pacífico (Tokio), Este de EE. UU. (Norte de Virginia) y Oeste de EE. UU. (Oregón).

3. 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.

## Resumen de los resultados de las consultas en lenguaje natural

 Note

La característica de resumen de consultas se encuentra en la versión preliminar para CloudTrail Lake y está sujeta a cambios.

Una vez finalizada la consulta, puede obtener un resumen de los resultados de la consulta en lenguaje natural en la pestaña de Resultados de la consulta del editor de consultas. Esta opción utiliza inteligencia artificial generativa (IA generativa) para producir el resumen.

### Resumir los resultados de la consulta

1. En la pestaña Resultados de la consulta del editor de consultas, seleccione Resumir los resultados para generar un resumen en lenguaje natural de los resultados de la consulta. El resumen se ofrece en inglés.
2. (Opcional) Para ofrecer comentarios sobre el resumen, elija el botón de aprobación hacia arriba o hacia abajo que aparece debajo del resumen generado.

Si el almacén de datos del evento relacionado se cifra con una clave de KMS, no podrá utilizarla para cifrar los resultados y el resumen de la consulta. En su lugar, CloudTrail cifra los resultados y el resumen de la consulta.

El acceso al resumen generado se autoriza con los permisos `GetQueryResults`, `GenerateQueryResultsSummary` y KMS (si el almacén de fechas del evento relacionado está cifrado con una clave de KMS). Cuando se genera un resumen, CloudTrail registra un evento denominado `GenerateQueryResultsSummary` para su visibilidad.

## Permisos necesarios

Las políticas administradas [AWSCloudTrail\\_FullAccess](#) y [AdministratorAccess](#) brindan los permisos necesarios para utilizar esta característica.

También puede incluir las acciones `cloudtrail:GenerateQueryResultsSummary` y `cloudtrail:GetQueryResults` en una política integrada o administrada por el cliente, nueva o existente.

Si el almacén de datos de eventos relacionado con los resultados de la consulta que se resume está cifrado con una clave de KMS, también necesitará permisos para la clave de KMS.

## Compatibilidad de regiones

Esta característica está disponible en las siguientes Regiones de AWS:

- Región Asia-Pacífico (Tokio) (ap-northeast-1)
- Región Este de EE. UU. (Norte de Virginia) (us-east-1)
- Región Oeste de EE. UU. (Oregón) (us-west-2)

## Limitaciones

A continuación, se encuentran las limitaciones de esta característica:

- Los resúmenes se ofrecen solo en inglés.
- Los resúmenes se limitan a los almacenes de datos de eventos que recopilan los eventos de CloudTrail (eventos administrados, de datos y de actividad de la red).
- Cada resumen es para los resultados de una sola consulta.
- El tamaño de los resultados de la consulta debe ser inferior a 250 KB.
- La cuota mensual de los resultados de consultas que se pueden resumir es de 3 MB.

## Descarga de los 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 [Validar resultados de consultas guardados de CloudTrail Lake](#).

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
  amzn-s3-demo-bucket
    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.

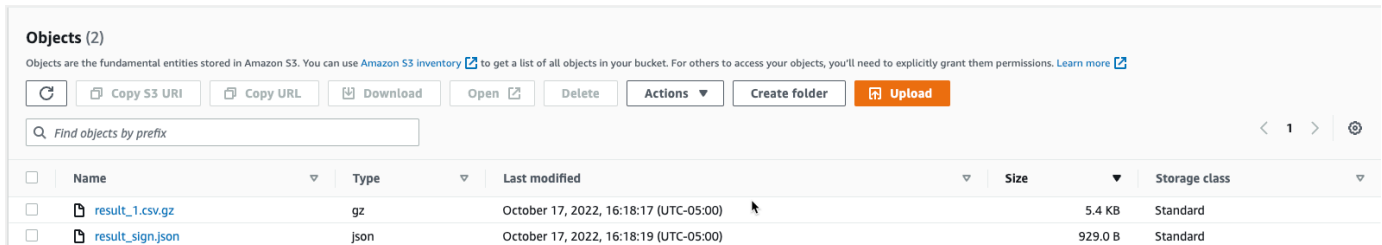
- Un archivo de firma en formato JSON que puede usar para validar los archivos de resultados de consultas. El archivo de firma se denomina result\_sign.json. Para obtener más información acerca del archivo de firma, consulte [Estructura de los archivos de firma de CloudTrail](#).
- Uno o más archivos 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.

## Validar resultados de consultas guardados de CloudTrail Lake

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 <string>`

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 <string>`

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 <string>`

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 amzn-s3-demo-bucket --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 <i>file_name</i> has inconsistent hash value with hash value recorded in sign file, hash value in sign file is <i>expected_hash</i> , but get <i>computed_hash</i> | 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 <code>fileHashValue</code> del archivo de firma. |

| Tipo de archivo | Mensaje de validación                                 | Descripción                                                                                  |
|-----------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Sign file       | ValidationError:<br>Invalid signature in<br>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://amzn-s3-demo-bucket/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 la 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.<br><br>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.<br><br>Tipo: DateTime                                       |

### Elementos de respuesta

PublicKeyList, una matriz de objetos PublicKey que contiene:

| Name  | 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.<br>Tipo: DateTime                                                                                  |
| ValidityEndTime   | La hora de finalización de la validez de la clave pública.<br>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.<br>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 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.");
}
}

```

## Optimización de consultas de CloudTrail Lake

En esta página, se ofrece orientación sobre cómo optimizar las consultas de CloudTrail Lake para mejorar el rendimiento y la fiabilidad. Abarca técnicas de optimización específicas, así como soluciones alternativas para los errores de consulta más comunes.

## Temas

- [Recomendaciones para optimizar las consultas](#)
- [Soluciones alternativas para los errores de la consulta](#)

## Recomendaciones para optimizar las consultas

Siga las recomendaciones que se encuentran en esta sección para optimizar sus consultas.

### Recomendaciones:

- [Optimización de las agregaciones](#)
- [Uso de técnicas de aproximación](#)
- [Limitar los resultados de la consulta](#)
- [Optimización de consultas LIKE](#)
- [Use UNION ALL en lugar de UNION](#)
- [Inclusión de las columnas necesarias únicamente](#)
- [Reducción del alcance de la función de ventana](#)

### Optimización de las agregaciones

La exclusión de las columnas redundantes en las cláusulas GROUP BY puede mejorar el rendimiento, debido a que menos columnas requieren menos memoria. Por ejemplo, en la siguiente consulta, podemos usar la función arbitrary en una columna redundante como eventType para mejorar el rendimiento. La función arbitrary en eventType se utiliza para seleccionar el valor del campo de manera aleatoria del grupo, ya que el valor es el mismo y no es necesario incluirlo en la cláusula GROUP BY.

```
SELECT eventName, eventSource, arbitrary(eventType), count(*)  
FROM $EDS_ID  
GROUP BY eventName, eventSource
```

Es posible mejorar el rendimiento de la función GROUP BY ordenando la lista de campos dentro de GROUP BY en orden decreciente según su recuento de valores únicos (cardinalidad). Por ejemplo, si se obtiene la cantidad de eventos de un tipo en cada Región de AWS, puede mejorarse el rendimiento mediante eventName, el orden de awsRegion en la función GROUP BY en lugar de awsRegion, eventName ya que existen más valores únicos de eventName que de awsRegion.

```
SELECT eventName, awsRegion, count(*)
FROM $EDS_ID
GROUP BY eventName, awsRegion
```

## Uso de técnicas de aproximación

Cuando no se necesiten valores exactos para contar valores distintos, utilice [funciones de agregación aproximada](#) para encontrar los valores más frecuentes. Por ejemplo, [approx\\_distinct](#) utiliza mucha menos memoria y se ejecuta más rápido que la operación `COUNT(DISTINCT fieldName)`.

## Limitar los resultados de la consulta

Si solo se necesita una respuesta de muestra para una consulta, restrinja los resultados a una cantidad reducida de filas mediante la condición `LIMIT`. De lo contrario, la consulta arrojará resultados de gran tamaño y tardará más tiempo en ejecutarse.

Si se utiliza `LIMIT` junto con `ORDER BY`, pueden obtenerse resultados más rápidos para los registros N superiores o inferiores, ya que reduce la cantidad de memoria necesaria y el tiempo necesario para ordenarlos.

```
SELECT * FROM $EDS_ID
ORDER BY eventTime
LIMIT 100;
```

## Optimización de consultas LIKE

Puede usar `LIKE` para encontrar cadenas coincidentes, pero con cadenas largas, esto requiere un uso intensivo de cómputos. La función [regexp\\_like](#) es, en la mayoría de los casos, una alternativa más rápida.

A menudo, puede optimizar una búsqueda anclando la subcadena que está buscando. Por ejemplo, si busca un prefijo, es mejor usar `“substr%”` en lugar de `“%substr”` con el operador `LIKE` y `“^substr”` con la función `regexp_like`.

## Use **UNION ALL** en lugar de **UNION**

`UNION ALL` y `UNION` son dos formas de combinar los resultados de dos consultas en un solo resultado, pero `UNION` elimina los duplicados. `UNION` necesita procesar todos los registros y encontrar los duplicados, lo que requiere mucha memoria y procesamiento, pero `UNION ALL` es una

operación relativamente rápida. A menos que necesite deduplicar registros, use `UNION ALL` para obtener el mejor rendimiento.

### Inclusión de las columnas necesarias únicamente

Si no necesita una columna, no la incluya en la consulta. Cuantos menos datos tenga que procesar una consulta, más rápido se ejecutará. Si tiene consultas que aplican `SELECT *` en la consulta más externa, debe cambiar `*` a una lista de columnas que necesita.

La cláusula `ORDER BY` devuelve los resultados de una consulta ordenados. Al ordenar una gran cantidad de datos, si no se dispone de la memoria necesaria, los resultados ordenados de manera intermedia se graban en el disco, lo que puede ralentizar la ejecución de la consulta. Si no necesita estrictamente ordenar el resultado, evite agregar una cláusula `ORDER BY`. Además, evite agregar `ORDER BY` a las consultas internas si no son estrictamente necesarias.

### Reducción del alcance de la función de ventana

Las [funciones de ventana](#) guardan en la memoria todos los registros en los que operan para calcular su resultado. Cuando la ventana es muy grande, la función de ventana puede quedarse sin memoria. Para asegurarse de que las consultas se ejecuten dentro de los límites de memoria disponibles, reduzca el tamaño de las ventanas sobre las que trabajan las funciones de ventana al agregar la cláusula `PARTITION BY`.

A veces, las consultas con funciones de ventana se pueden reescribir sin funciones de ventana. Por ejemplo, en lugar de usar `row_number` o `rank`, puede usar funciones agregadas como [max\\_by](#) o [min\\_by](#).

La siguiente consulta busca el alias asignado más recientemente a cada clave de KMS mediante `max_by`.

```
SELECT element_at(requestParameters, 'targetKeyId') as keyId,  
max_by(element_at(requestParameters, 'aliasName'), eventTime) as mostRecentAlias  
FROM $EDS_ID  
WHERE eventsource = 'kms.amazonaws.com'  
AND eventName in ('CreateAlias', 'UpdateAlias')  
AND eventTime > DATE_ADD('week', -1, CURRENT_TIMESTAMP)  
GROUP BY element_at(requestParameters, 'targetKeyId')
```

En este caso, la función `max_by` devuelve el alias del registro con la hora del último evento del grupo. Esta consulta se ejecuta más rápido y utiliza menos memoria que una consulta equivalente con una función de ventana.



## Soluciones alternativas para los errores de la consulta

En esta sección se ofrecen las soluciones para los errores de consulta más comunes.

Errores de consulta:

- [La consulta falla porque la respuesta es demasiado grande](#)
- [La consulta falla debido al agotamiento de los recursos](#)

### La consulta falla porque la respuesta es demasiado grande

Una consulta puede fallar si la respuesta es demasiado grande y da como resultado el mensaje **Query response is too large**. Si esto sucede, puede reducir el alcance de la agregación.

Las funciones de agregación, como `array_agg`, pueden hacer que al menos una fila de la respuesta a la consulta sea muy grande y ocasionar un error en la consulta. Por ejemplo, usar `array_agg(eventName)` en lugar de `array_agg(DISTINCT eventName)` aumentará de manera considerable el tamaño de la respuesta debido a la duplicación de los nombres de los eventos de CloudTrail seleccionados.

### La consulta falla debido al agotamiento de los recursos

Si no hay suficiente memoria disponible durante la ejecución de las operaciones que consumen mucha memoria, como uniones, agregaciones y funciones de ventana, los resultados intermedios se filtran en el disco, pero esto ralentiza la ejecución de la consulta y puede que no sea suficiente para evitar que la consulta falle con **Query exhausted resources at this scale factor**. Esto se puede solucionar si vuelve a intentar la consulta.

Si los errores anteriores persisten incluso después de optimizar la consulta, puede reducir el alcance de la consulta con `eventTime` de los eventos y ejecutar la consulta varias veces en intervalos más pequeños del rango de tiempo de la consulta original.

## Ejecución y administración de consultas de CloudTrail Lake con la AWS CLI

Puede usar la AWS CLI para ejecutar y administrar sus consultas de CloudTrail Lake. Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la Región de AWS 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.

## Comandos disponibles para consultas de CloudTrail Lake

Entre los comandos para ejecutar y administrar consultas en CloudTrail Lake se incluyen:

- [start-query](#) para ejecutar una consulta.
- [describe-query](#) para devolver los metadatos de una consulta.
- [generate-query](#) para generar una consulta a partir de una petición en inglés. Para obtener más información, consulte [Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural](#).
- [get-query-results](#) para devolver los resultados del ID de consulta especificado.
- [list-queries](#) para obtener una lista de consultas del almacén de datos de eventos especificado.
- [cancel-query](#) para cancelar una consulta en curso.

Para obtener una lista de los comandos disponibles para los almacenes de datos de eventos de CloudTrail Lake, consulte [Comandos disponibles para los almacenes de datos de eventos](#).

Para obtener una lista de los comandos disponibles para los paneles de CloudTrail Lake, consulte [Comandos disponibles para los paneles](#).

Para obtener una lista de los comandos disponibles para las integraciones de CloudTrail Lake, consulte [Comandos disponibles para las integraciones de CloudTrail Lake](#).

## Genere una consulta a partir de una petición en lenguaje natural con el AWS CLI

Ejecute el comando `generate-query` para generar una consulta a partir de una petición en inglés. En `--event-data-stores`, brinde el ARN (o el sufijo de ID del ARN) del almacén de datos de eventos que quiera consultar. Solo puede especificar un almacén de datos de eventos. Para `--prompt`, brinde la petición en inglés.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

Si se realiza de manera correcta, el comando genera una instrucción SQL y ofrece una `QueryAlias` que utilizará junto con el comando `start-query` para ejecutar la consulta en el almacén de datos de eventos.

```
{
  "QueryString": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

## 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-s3-uri` 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 [Restricciones SQL de CloudTrail Lake](#).

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
LIMIT 10'
--delivery-s3-uri "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.

### Output

```
{
  "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-s3-uri`, 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
```

## Output

```
{
  "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
```

## Output

```
{
  "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-ecccf7EXAMPLE
```

## Output

```
QueryId -> (string)
QueryStatus -> (string)
```

## Restricciones SQL de CloudTrail Lake

Las consultas de CloudTrail 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.

La sintaxis de CloudTrail Lake para una instrucción SELECT es la siguiente. Se especifica el ID del almacén de datos de eventos (la parte del ID del ARN del almacén de datos de eventos) para el valor FROM.

```
SELECT [ DISTINCT ] columns [ Aggregate ]
[ FROM table event_data_store_ID ]
[ WHERE columns [ Conditions ] ]
[ GROUP BY columns [ DISTINCT | Aggregate ] ]
[ HAVING columns [ Aggregate | Conditions ] ]
[ ORDER BY columns [ Aggregate | ASC | DESC | NULLS | FIRST | LAST ] ]
[ LIMIT [ INT ] ]
```

CloudTrail Lake admite todos los operadores, las funciones e instrucciones SELECT de Trino SQL válidos. Para obtener más información acerca de los operadores y las funciones SQL compatibles, consulte [Funciones y operadores](#) en el sitio web de documentación de Trino.

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 con la consola de CloudTrail](#).

Para obtener más información sobre cómo optimizar las consultas, diríjase a [Optimización de consultas de CloudTrail Lake](#).

## Temas

- [Funciones, condiciones y operadores join compatibles](#)
- [Soporte avanzado de consultas en varias tablas](#)

## Funciones, condiciones y operadores join compatibles

### Funciones compatibles

CloudTrail Lake admite todas las funciones de Trino. Para obtener más información acerca de otras funciones compatibles, consulte [Funciones y operadores](#) en el sitio web de documentación de Trino.

### 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 EXAMPLEb529-4e8f913d-6m2z-1kp5sEXAMPLE 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 administración, de datos y de actividad de la red de CloudTrail. Para obtener más información acerca de los campos de los registros de eventos de CloudTrail, consulte [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

```
[
  {
    "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>,onbehalfof:struct<userid:string,identitystorearn:string>,
inscopeof:struct<sourcearn:string,sourceaccount:string,issuertype:string,
credentialisissuedto: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": "vpcepointid",
    "Type": "string"
  },
  {
    "Name": "vpcepointaccountid",
    "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`. Para obtener las descripciones de estos campos, consulte [CloudTrail registra el contenido de los eventos de Insights para los almacenes de datos de eventos](#).

 Note

Los campos `insightvalue`, `insightaverage`, `baselinevalue` y `baselineaverage` incluidos en el campo `attributions` de `insightContext` comenzarán a quedar obsoletos el 23 de junio de 2025.

```
[
  {
    "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": "insighteventsourcesource",
      "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,
        insight:struct<value:string,average:double>,
        baseline:struct<value:string,average: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,resourcearn: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,originaeventid: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,errormessage:string,sourceipaddress:stri
recipientaccountid:string,additionaleventdata":map<string,string>>"
  }
]

```

## Métricas de CloudWatch admitidas

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 | <p>La cantidad de datos ingeridos en el almacén de datos de eventos durante la última hora. Esta métrica se actualiza cada hora.</p> <p>Esta métrica está disponible para todos los tipos de almacenes de datos de eventos.</p>                      | Bytes    |
| TotalDataRetained  | <p>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.</p> <p>Esta métrica está disponible para todos los tipos de almacenes de datos de eventos.</p> | Bytes    |
| TotalStorageBytes  | <p>El total de bytes comprimidos en el almacén de datos de eventos en el día actual.</p> <p>Esta métrica está disponible para todos los tipos de almacenes de datos de eventos.</p>                                                                  | Bytes    |

| Métrica               | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Unidades |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| TotalPaidStorageBytes | <p>Para los almacenes de datos de eventos que utilizan la <a href="#">opción de precio</a> 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.</p> <p>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 <a href="#">Precios de AWS CloudTrail</a>.</p> <p>Esta métrica solo está disponible para los almacenes de datos de eventos que utilizan la opción de precios de retención ampliables por un año.</p> | Bytes    |

| Métrica              | Descripción                                                                                                                                                                                                                                                 | Unidades |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| HourlyEventsAnalyzed | <p>El número total de eventos analizados por CloudTrail Insights en el almacén de datos de eventos. Esta métrica se actualiza cada hora.</p> <p>Esta métrica es para los almacenes de datos de eventos de CloudTrail que habilitan CloudTrail Insights.</p> | 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

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 CloudWatch](#) y [Amazon EventBridge](#).

Puede crear un registro de seguimiento para enviar una copia de los eventos de administración en curso a su bucket de 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](#).

Puede crear registros de seguimiento multirregión y de una sola región para su Cuenta de AWS.

## registros de seguimiento multirregión

Cuando crea un registro de seguimiento de varias regiones, CloudTrail registra los eventos de todas las Regiones de AWS que están [habilitadas](#) en la Cuenta de AWS y envía los archivos de registro de eventos de CloudTrail al bucket de S3 que se especifique. Como práctica recomendada, le sugerimos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas. Todos los registros de seguimiento que se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones. Puede convertir un registro de seguimiento de una sola región en uno de varias regiones mediante la AWS CLI. Para obtener más información, consulte [Cómo entender los registros de seguimiento de varias regiones y las regiones optativas](#), [Creación de un registro de seguimiento con la consola](#) y [Conversión de un registro de seguimiento de una sola región en un registro de seguimiento de varias regiones](#).

## registros de seguimiento de una sola región

Cuando crea un registro de seguimiento de una sola región, CloudTrail solo registra los eventos de esa región. A continuación, entrega los archivos de registros de eventos de CloudTrail al bucket de Amazon S3 que especifique. Solo puede crear un registro de seguimiento de una sola región mediante la AWS CLI. Si crea registros de seguimiento individuales adicionales, puede disponer que dichos registros de seguimiento envíen los archivos de registro de eventos de CloudTrail al mismo bucket de S3 o a buckets separados. Esta es la opción predeterminada al crear un registro de seguimiento mediante la AWS CLI o la API de CloudTrail. Para obtener más información, consulte [Creación, actualización y administración de registros de seguimiento con la AWS CLI](#).



 Note

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

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. Para obtener más información, consulte [Creación de un registro de seguimiento para una organización](#).

## Temas

- [Creación de un registro de seguimiento para su Cuenta de AWS](#)
- [Creación de un registro de seguimiento para una organización](#)
- [Cómo entender los registros de seguimiento de varias regiones y las regiones optativas](#)
- [Copia de eventos de registro de seguimiento en CloudTrail Lake](#)
- [Obtención y visualización de archivos de registros de CloudTrail](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Uso de AWS CloudTrail con los puntos de enlace de la VPC de la interfaz](#)
- [Requisitos de nomenclatura de los recursos de CloudTrail, los buckets de S3 y las claves de KMS](#)
- [Cierre de Cuenta de AWS y registros de seguimiento](#)

## 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 de [varias regiones](#), aparecerá en la consola en todas las Regiones de AWS que estén [habilitadas](#) en la cuenta. Si crea un registro de seguimiento que solo registra los eventos en una región, solo podrá verlo y administrarlo en esa región. Como práctica recomendada, le recomendamos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas. Todos los registros de seguimiento que se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones. 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](#).

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

- [Creación y actualización de un registro de seguimiento con la consola](#)

- [Creación, actualización y administración de registros de seguimiento con la AWS CLI](#)
- [Creación de varios registros de seguimiento](#)

## 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.

Puede cambiar la siguiente configuración de su registro de seguimiento mediante la consola de CloudTrail:

- Puede cambiar la ubicación del bucket de S3 y especificar un prefijo.
- La cuenta de administración de una organización de AWS Organizations puede convertir un registro de seguimiento a nivel de cuenta en un registro de seguimiento de la organización o convertir un registro de seguimiento de la organización en un registro de seguimiento a nivel de cuenta.
- Puede habilitar o deshabilitar el cifrado de claves de KMS.
- Puede habilitar o deshabilitar la [validación de archivos de registro](#). La validación de archivos de registro le permite determinar si un archivo de registro se ha modificado, eliminado o no se ha modificado después de que CloudTrail lo haya entregado. De forma predeterminada, la validación de archivos de registro está habilitada.
- Puede configurar un registro de seguimiento para enviar notificaciones a un tema de Amazon SNS.
- Puede configurar un registro de seguimiento para enviar eventos a un grupo de registro de Registros de CloudWatch. Tanto el grupo de registro como el rol de IAM deben existir en su propia cuenta.
- Puede actualizar la configuración de los eventos de administración, eventos de datos, eventos de actividad de la red y eventos de Insights.
- Puede agregar o eliminar etiquetas. Puede agregar hasta 50 pares de claves y etiquetas para que le resulte más fácil identificar sus registros de seguimiento.

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, usar 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, usar la consola de CloudTrail le permite ver los tipos de datos disponibles. Para obtener más información, consulte [Registro de eventos de datos](#).
- En caso de que esté configurando un registro de seguimiento para eventos de actividad de la red, usar la consola de CloudTrail le permite ver los orígenes de eventos disponibles. Para obtener más información, consulte [Registro de eventos de actividad de la red](#).

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 con la consola de CloudTrail](#)
- [Actualización de un registro de seguimiento con la consola de CloudTrail](#)
- [Eliminación de un registro de seguimiento con la consola de CloudTrail](#)
- [Desactivación del registro de un registro de seguimiento](#)

## Creación de un registro de seguimiento con la consola de CloudTrail

Se puede aplicar un registro de seguimiento a todas las Regiones de AWS que estén [habilitadas](#) en su Cuenta de AWS, o puede aplicar a una sola región. Un registro de seguimiento que se aplica a todas las Regiones de AWS que están habilitadas en su Cuenta de AWS se denomina registro de seguimiento de varias regiones. Como práctica recomendada, le sugerimos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas. Todos los registros de seguimiento que se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones. Solo puede crear un registro de seguimiento de una sola región mediante el AWS CLI o la operación API de [CreateTrail](#).

 Note

Después de crear un registro de seguimiento, puede configurar otros Servicios de AWS para analizar y actuar según los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte [Integraciones de servicios de AWS con registros de CloudTrail](#).

## Temas

- [Creación de un registro de seguimiento con la consola](#)
- [Pasos a seguir a continuación](#)

## Creación de un registro de seguimiento con la consola

Utilice el siguiente procedimiento para crear un registro de seguimiento multirregión. Para registrar eventos en una sola región (no recomendado), [utilice la AWS CLI](#).

Para crear un registro de seguimiento de CloudTrail con la Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En la página de inicio del servicio CloudTrail, la página Trails (Registros de seguimiento), o la sección Trails (Registros de seguimiento) en la página Dashboard (Panel), 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 de los recursos de CloudTrail, los buckets de S3 y las claves de KMS](#).
4. Si se trata de un registro de seguimiento de organización de AWS Organizations, puede activar el registro de seguimiento de todas las cuentas de la 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. Cuando se crea un bucket, CloudTrail crea y aplica las políticas de buckets necesarias. Si opta por crear un nuevo bucket de S3, su política de IAM

debe incluir permiso para la acción `s3:PutEncryptionConfiguration` porque el cifrado en el servidor está habilitado de forma predeterminada para el bucket.

 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 del bucket debe conceder permiso a CloudTrail 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 registros, cree una carpeta nueva (también conocida como prefijo) en un bucket existente a fin de almacenar los registros de CloudTrail. Ingrese el prefijo en Prefix (Prefijo).

6. En Cifrado SSE-KMS de archivos de registro, elija Habilitado si desea cifrar sus archivos de registro y de resumen con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los archivos de registro y de resumen 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 AWS KMS key New (Nuevo) o Existing (Existente). En AWS KMS Alias (Alias de KMS), especifique un alias, en el formato `alias/MyAliasName`. Para obtener más información, consulte [Actualización de un recurso para que utilice su clave de KMS con la consola](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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 con la consola](#). La política de claves debe permitir que CloudTrail utilice la clave para cifrar

los archivos de registro y de resumen, y que los usuarios especificados lean archivos de registro y de resumen 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](#).

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 sus archivos de registros no cambien después de que CloudTrail los envíe. Para obtener más información, consulte [Validar la integridad de los archivos de registros de CloudTrail](#).
  - b. En SNS notification delivery (Envío de notificación SNS), elija Enabled (Habilitado) si desea recibir una notificación cada vez que se envíe un archivo de registros a su bucket. CloudTrail almacena varios eventos en un archivo de registros. 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 de varias regiones, las notificaciones de SNS para las entregas de archivo de registro de todas las regiones activadas se envían al tema de SNS único que haya creado.

Si elige New (Nuevo), CloudTrail especifica un nombre para el tema nuevo 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 de temas 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 [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.



8. También puede configurar CloudTrail para que envíe archivos de registros a CloudWatch Logs al elegir Enabled (Habilitado) en CloudWatch Logs. Para obtener más información, consulte [Envío de eventos a Amazon CloudWatch Logs](#).
  - a. Si habilita la integración con CloudWatch Logs, elija New (Nuevo) para crear un grupo de registros nuevo, o Existing (Existente) para utilizar uno existente. Si elige New (Nuevo), CloudTrail especifica un nombre para el grupo de registros nuevo o puede escribir un nombre.
  - b. Si elige Existing (Existente), elija un grupo de registros en la lista desplegable.
  - c. Elija New (Nuevo) para crear un rol de IAM nuevo con permisos para enviar registros a CloudWatch 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 para que CloudTrail utilice CloudWatch Logs para el monitoreo..](#)

 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.
- 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.

9. En Etiquetas, puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su registro de seguimiento y controlar el acceso a él. Las etiquetas pueden ayudarlo a identificar tanto los registros de seguimiento de CloudTrail como 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 [Grupos de recursos de AWS y Etiquetas](#).
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. Elija Exclude AWS KMS events (Excluir eventos de KMS) para filtrar eventos de AWS Key Management Service (AWS KMS) fuera del registro de seguimiento. 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. 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 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 más información, consulte [Precios de AWS CloudTrail](#).
  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 recursos](#) 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 Tipo de recurso, elija el tipo de recurso en el que desea registrar los eventos de datos. Para obtener más información sobre los tipos de recursos disponibles, consulte [Eventos de datos](#).

13. Elija una plantilla de selector de registros. Puede elegir una plantilla predefinida o elegir Personalizar para definir sus propias condiciones de recopilación de eventos.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
- Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
- Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
- Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
- Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).

#### Note

Elegir una plantilla predefinida para los buckets de S3 permite el registro de eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos que lleva a cabo cualquier identidad de IAM en su cuenta de AWS, aunque esta se haga en un bucket que pertenezca a otra cuenta de 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 crea un registro de seguimiento de varias regiones, elegir una plantilla predefinida para las funciones de Lambda permite el registro de eventos de datos de todas las funciones que se encuentran actualmente en la cuenta de AWS, así como de cualquier función de Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear un registro de seguimiento para una sola región (mediante la AWS CLI), esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función Lambda que cree en esa región después de crear el registro de seguimiento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.

El registro de eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos que lleve a cabo cualquier identidad de IAM de su cuenta de AWS, aunque esta se haga en una función que pertenezca a otra cuenta de AWS.

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. Si seleccionó Personalizado, en los selectores de eventos avanzados se crea una expresión basada en los valores de los campos de los selectores de eventos avanzados.

 Note

Los selectores no admiten el uso de caracteres comodín como \*. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

a. Elija uno de los siguientes campos.

- **readOnly**: `readOnly` se puede establecer en `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 utilizarlo para incluir o excluir cualquier evento de datos registrado en CloudTrail, como `PutBucket`, `GetItem` o `GetSnapshotBlock`.
- **eventSource**: el origen del evento que se va a incluir o excluir. Este campo puede utilizar cualquier operador.
- **eventType**: el tipo de evento que se va a incluir o excluir. Por ejemplo, puede establecer este campo en `no igual a AwsServiceEvent` para excluir [Servicio de AWSEventos de](#). Para obtener una lista de los tipos de eventos, consulte [eventType](#) en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).
- **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de la Consola de administración de AWS. Este campo se puede establecer como `igual` o `no igual` con un valor de `true`.
- **userIdentity.arn**: incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- **resources.ARN**: puede utilizar cualquier operador con `resources.ARN`, pero si utiliza `es igual a` o `no es igual a`, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo especificado en la plantilla como el valor de `resources.type`.

 Note

No puede usar el campo `resources.ARN` para filtrar los tipos de recursos que no tienen ARN.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte [Acciones, recursos y claves de condición para los Servicios de AWS](#) en la Referencia de autorizaciones de servicio.

- 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 eventos de datos de dos buckets de S3 de los eventos de datos registrados en su almacén de datos de eventos, puede establecer el campo en `resources.ARN`, configurar

el operador en no comienza por y, a continuación, pegar un ARN de bucket 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.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- 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 Agregar tipo de evento de datos. Repita los 12 pasos hasta este paso a fin de configurar selectores de eventos avanzados para el tipo de recursos.
17. Para registrar los eventos de actividad de la red, seleccione Eventos de actividad de la red. Los eventos de actividad de la red permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Se aplican cargos adicionales por el registro de eventos de actividad de la red. Para más información, consulte [Precios de AWS CloudTrail](#).

Para registrar eventos de actividad de la red, siga estos pasos:

- a. En Origen de eventos de actividad de la red, seleccione el origen de los eventos de actividad de la red.
- b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede optar por registrar todos los eventos de actividad de la red, registrar todos los eventos de acceso denegado a la actividad de la red o seleccionar Personalizar para crear un selector de registro personalizado que filtre por varios campos, como eventName y vpcEndpointId.

- c. (Opcional) Escriba un nombre para identificar el selector. El nombre del selector aparece como Nombre en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
  - d. En Selectores de eventos avanzados, cree expresiones mediante la selección de valores para Campo, Operador y Valor. Puede omitir este paso si utiliza una plantilla de registro predefinida.
    - i. Para excluir o incluir eventos de actividad de la red, puede elegir entre los siguientes campos de la consola.
      - **eventName** – puede utilizar cualquier operador con eventName. Puede utilizarlo para incluir o excluir cualquier evento, como CreateKey.
      - **errorCode** – puede usarlo para filtrar por un código de error. Actualmente, el único errorCode que se admite es VpceAccessDenied.
      - **vpcEndpointId** – identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con vpcEndpointId.
    - ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.
    - iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
  - e. Para agregar otro origen de eventos de actividad de la red que quiera registrar, seleccione Agregar selector de eventos de actividad de la red.
  - f. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
18. Elija Insights events (Eventos de Insights) si desea que su registro de seguimiento registre 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 actividades inusuales y registra eventos 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 [Trabajar con CloudTrail Insights](#). Se aplican cargos adicionales por registrar

eventos de Insights. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

Los eventos de Insights se envían a una carpeta diferente denominada `/CloudTrail-Insight` del mismo bucket de S3 que se especifica en el área de Storage location (Ubicación de almacenamiento) de la página de detalles del registro de seguimiento. CloudTrail crea el prefijo nuevo en su nombre. Por ejemplo, si el bucket de S3 de destino actual se denomina `amzn-s3-demo-bucket/AWSLogs/CloudTrail/`, el nombre del bucket de S3 con un nuevo prefijo se denomina `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`.

19. Cuando haya terminado de elegir los tipos de eventos para registrar, elija Next (Siguiente).
20. 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).
21. 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 API de AWS hechas en su cuenta. Puede ver los archivos de registro del bucket de S3 especificado.

Si habilita los eventos Insights para el registro de seguimiento, CloudTrail puede demorar hasta 36 horas en empezar a entregar los eventos de Insights, siempre que se detecte actividad inusual durante ese tiempo.

#### 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 servicio 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.

## Configurar los ajustes de eventos de datos mediante selectores de eventos básicos

Puede usar selectores de eventos avanzados para configurar todos los tipos de eventos de datos, así como los eventos de actividad de la red. Los selectores de eventos avanzados permiten crear selectores detallados para registrar solo los eventos que le interesen.

Si usa selectores de eventos básicos para registrar los eventos de datos, solo podrá registrar eventos de datos de buckets de Amazon S3, funciones de AWS Lambda y tablas de Amazon DynamoDB. Con los selectores de eventos básicos no puede filtrar por el campo eventName. Tampoco puede registrar los [eventos de actividad de la red](#).

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#) 

 **Basic event selectors are enabled**  
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

Switch to advanced event selectors

Data event: S3 [Info](#)

Remove

**Data event source**  
Select source of data events to log.

S3

S3

Lambda

DynamoDB

**Individual bucket selection**  
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

 bucket/prefix

Browse

☒ Read ☒ Write

×

Add bucket

Add data event type



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 más información, consulte [Precios de AWS CloudTrail](#).
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

Conservar la opción predeterminada All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) permite registrar los eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos que lleva a cabo cualquier identidad de IAM en su cuenta de AWS, aunque esta se haga en un bucket que pertenezca a otra cuenta de AWS.

Si crea un registro de seguimiento para una única región (mediante la AWS CLI), elegir All current and future S3 buckets (Todos los buckets de S3 actuales o futuros) habilita el registro de eventos de datos de todos los buckets que se encuentren en la misma región que el registro de seguimiento, así como de cualquier otro bucket que pudiera crear posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de la cuenta de AWS.

- 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 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 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 de varias 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 de Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear un registro de seguimiento para una sola región (mediante la AWS CLI), esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función Lambda que cree en esa región después de crear el registro de seguimiento. No

habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.

El registro de eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos que lleve a cabo cualquier identidad de IAM de su cuenta de AWS, aunque esta se haga en una función que pertenezca a otra cuenta de AWS.

- 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 en la consola de CloudTrail cuando cree un registro de seguimiento. 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 [Administración de registros de seguimiento con la 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, [???](#).

## Pasos a seguir a continuación

Después de crear el registro de seguimiento, puede volver a él para realizar cambios:

- Si aún no lo ha hecho, puede configurar CloudTrail para que envíe archivos de registros 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 para CloudTrail Logs en la consola de CloudTrail](#) 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 con la consola de CloudTrail

En esta sección se describe cómo cambiar la configuración del registro de seguimiento.

Para convertir un registro de seguimiento de una sola región a un registro de seguimiento de varias regiones, o actualizar un registro de seguimiento de varias regiones, debe utilizar el AWS CLI. Para obtener más información sobre cómo convertir un registro de seguimiento de una sola región en registro de seguimiento de varias regiones, consulte [Conversión de un registro de seguimiento de una sola región en un registro de seguimiento de varias 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 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 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 seguimiento de la organización en las cuentas de miembros aunque falle la validación de un recurso. Ejemplos de errores de validación:

- Una política de buckets de Amazon S3 incorrecta
- Una política de temas de Amazon SNS incorrecta
- Incapacidad de realizar envíos a un grupo de registro de Registros de CloudWatch
- Permisos insuficientes para cifrar mediante una clave de KMS

Las cuentas de miembros con permisos de CloudTrail pueden ver cualquier error de validación de un registro de seguimiento de la organización consultando la página de detalles del registro en la consola de CloudTrail o ejecutando el comando [get-trail-status](#) de la AWS CLI.

Para actualizar un registro de seguimiento con la Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS 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 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 de seguimiento a mi organización: cambie si este registro de seguimiento es un registro de seguimiento de organización de AWS Organizations.

 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 de seguimiento a un registro de seguimiento de organización de AWS Organizations, puede elegir habilitar el registro de seguimiento de todas las cuentas de la 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. Cuando se crea un bucket, CloudTrail crea y aplica las políticas de buckets necesarias. Si opta por crear un nuevo bucket de S3, su política de IAM debe incluir permiso para la acción `s3:PutEncryptionConfiguration` porque el cifrado en el servidor está habilitado de forma predeterminada para el bucket.

 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 del bucket debe conceder permiso a CloudTrail 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 registros, cree una carpeta nueva (también conocida como prefijo) en un bucket existente a fin de almacenar los registros de CloudTrail. Ingrese el prefijo en Prefix (Prefijo).

- c. En Cifrado SSE-KMS de archivos de registro, elija Habilitado si desea cifrar sus archivos de registro y de resumen con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los archivos de registro y de resumen 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 AWS KMS key New (Nuevo) o Existing (Existente). En AWS KMS Alias (Alias de KMS), especifique un alias, en el formato `alias/MyAliasName`. Para obtener más información, consulte [Actualización de un recurso para que utilice su clave de KMS con la consola](#). CloudTrail también admite claves de AWS KMS de varias regiones. 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 con la consola](#). La política de claves debe permitir que CloudTrail utilice la clave para cifrar los archivos de registro y de resumen, y que los usuarios especificados lean archivos de registro y de resumen 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](#).

- 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 sus archivos de registros no cambien después de que CloudTrail los envíe. Para obtener más información, consulte [Validar la integridad de los archivos de registros de CloudTrail](#).
- e. En SNS notification delivery (Envío de notificación SNS), elija Enabled (Habilitado) si desea recibir una notificación cada vez que se envíe un archivo de registros a su bucket. CloudTrail almacena varios eventos en un archivo de registros. 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 de varias regiones, las notificaciones de SNS para las entregas de archivo de registro de todas las regiones activadas se envían al tema de SNS único que haya creado.



Si elige New (Nuevo), CloudTrail especifica un nombre para el tema nuevo 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 de temas 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 [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

4. En CloudWatch Logs, elija Edit (Editar) para cambiar la configuración a fin de enviar archivos de registros de CloudTrail a CloudWatch Logs. Elija Enabled (Habilitado) en CloudWatch Logs para habilitar el envío de archivos de registros. Para obtener más información, consulte [Envío de eventos a Amazon CloudWatch Logs](#).
  - a. Si habilita la integración con CloudWatch Logs, elija New (Nuevo) para crear un grupo de registros nuevo, o Existing (Existente) para utilizar uno existente. Si elige New (Nuevo), CloudTrail especifica un nombre para el grupo de registros nuevo o puede escribir un nombre.
  - b. Si elige Existing (Existente), elija un grupo de registros en la lista desplegable.
  - c. Elija New (Nuevo) para crear un rol de IAM nuevo con permisos para enviar registros a CloudWatch 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 para que CloudTrail utilice CloudWatch Logs para el monitoreo](#).

 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.



- 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.

5. En Tags (Etiquetas), elija Edit (Editar) para cambiar, agregar o eliminar etiquetas en el registro de seguimiento. Puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su registro de seguimiento y controlar el acceso a él. Las etiquetas pueden ayudarlo a identificar tanto los registros de seguimiento de CloudTrail como 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 [Grupos de recursos de AWS y Etiquetas](#).
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. Elija Exclude AWS KMS events (Excluir eventos de KMS) para filtrar eventos de AWS Key Management Service (AWS KMS) fuera del registro de seguimiento. 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. 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 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, 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 tiene previsto registrar eventos de actividad de la red, debe utilizar selectores de eventos avanzados. 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 conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

En Tipo de recurso, elija el tipo de recurso en el que desea registrar los eventos de datos. Para obtener más información sobre los tipos de recursos disponibles, consulte [Eventos de datos](#).

8. Elija una plantilla de selector de registros. Puede elegir una plantilla predefinida o elegir Personalizar para definir sus propias condiciones de recopilación de eventos.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
- Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos Get\* o Describe\*.

- Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos Put\*, Delete\* o Write\*.
- Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
- Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un eventType de AwsServiceEvent y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).

#### Note

Elegir una plantilla predefinida para los buckets de S3 permite el registro de eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en un bucket que pertenezca a otra cuenta de 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 crea un registro de seguimiento de varias regiones, elegir una plantilla predefinida para las funciones de Lambda permite el registro de eventos de datos de todas las funciones que se encuentran actualmente en la cuenta de AWS, así como de cualquier función de Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear un registro de seguimiento para una sola región (mediante la AWS CLI), esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función Lambda que cree en esa región después de crear el registro de seguimiento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.

El registrar eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en una función que pertenezca a otra cuenta de AWS.

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. Si seleccionó Personalizado, en los selectores de eventos avanzados se crea una expresión basada en los valores de los campos de los selectores de eventos avanzados.

 Note

Los selectores no admiten el uso de caracteres comodín como \*. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

- a. Elija uno de los siguientes campos.
  - **readOnly**: `readOnly` se puede establecer en `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 utilizarlo para incluir o excluir cualquier evento de datos registrado en CloudTrail, como `PutBucket`, `GetItem` o `GetSnapshotBlock`.
  - **eventSource**: el origen del evento que se va a incluir o excluir. Este campo puede utilizar cualquier operador.
  - **eventType**: el tipo de evento que se va a incluir o excluir. Por ejemplo, puede establecer este campo en `no igual a AwsServiceEvent` para excluir [Servicio de AWSEventos de](#) . Para obtener una lista de los tipos de eventos, consulte [eventType](#) en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).
  - **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de la Consola de administración de AWS. Este campo se puede establecer como `igual` o `no igual` con un valor de `true`.

- `userIdentity.arn`: incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento `userIdentity` de CloudTrail](#).
- **`resources.ARN`**: puede utilizar cualquier operador con `resources.ARN`, pero si utiliza `es igual a` o `no es igual a`, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo especificado en la plantilla como el valor de `resources.type`.

 Note

No puede usar el campo `resources.ARN` para filtrar los tipos de recursos que no tienen ARN.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte [Acciones, recursos y claves de condición para los Servicios de AWS](#) en la Referencia de autorizaciones de servicio.

- 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 eventos de datos de dos buckets de S3 de los eventos de datos registrados en su almacén de datos de eventos, puede establecer el campo en `resources.ARN`, configurar el operador en `no comienza por` y, a continuación, pegar un ARN de bucket 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.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- 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 Agregar tipo de evento de datos. Repita los 3 pasos hasta este paso a fin de configurar selectores de eventos avanzados para el tipo de recursos.
12. En Eventos de actividad de la red, seleccione Editar para modificar la configuración de registro de eventos de actividad de la red. De forma predeterminada, los registros de seguimiento no registran eventos de actividad de la red. Se aplican cargos adicionales por el registro de eventos de actividad de la red. Para más información, consulte [Precios de AWS CloudTrail](#).

Para registrar eventos de actividad de la red, siga estos pasos:

- a. En Origen de eventos de actividad de la red, seleccione el origen de los eventos de actividad de la red.
- b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede optar por registrar todos los eventos de actividad de la red, registrar todos los eventos de acceso denegado a la actividad de la red o seleccionar Personalizar para crear un selector de registro personalizado que filtre por varios campos, como eventName y vpcEndpointId.
- c. (Opcional) Escriba un nombre para identificar el selector. El nombre del selector aparece como Nombre en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
- d. En Selectores de eventos avanzados, cree expresiones mediante la selección de valores para Campo, Operador y Valor. Puede omitir este paso si utiliza una plantilla de registro predefinida.
  - i. Para excluir o incluir eventos de actividad de la red, puede elegir entre los siguientes campos de la consola.
    - **eventName** – puede utilizar cualquier operador con eventName. Puede utilizarlo para incluir o excluir cualquier evento, como CreateKey.
    - **errorCode** – puede usarlo para filtrar por un código de error. Actualmente, el único errorCode que se admite es VpceAccessDenied.

- **vpcEndpointId** – identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con vpcEndpointId.
  - ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.
  - iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
  - e. Para agregar otro origen de eventos de actividad de la red que quiera registrar, seleccione Agregar selector de eventos de actividad de la red.
  - f. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
13. En Eventos de Insights, elija Editar si quiere que su registro de seguimiento 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 actividades inusuales y registra eventos 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 [Trabajar con CloudTrail Insights](#). Se aplican cargos adicionales por registrar eventos de Insights. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

Los eventos de Insights se envían a una carpeta diferente denominada /CloudTrail-Insight del mismo bucket de S3 que se especifica en el área de Storage location (Ubicación de almacenamiento) de la página de detalles del registro de seguimiento. CloudTrail crea el prefijo nuevo en su nombre. Por ejemplo, si el bucket de S3 de destino actual se denomina amzn-s3-demo-bucket/AWSLogs/CloudTrail/, el nombre del bucket de S3 con un nuevo prefijo se denomina amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/.

14. 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 usar selectores de eventos avanzados para configurar todos los tipos de eventos de datos, así como los eventos de actividad de la red. Los selectores de eventos avanzados permiten crear selectores detallados para registrar solo los eventos que le interesen.

Si usa selectores de eventos básicos para registrar los eventos de datos, solo podrá registrar eventos de datos de buckets de Amazon S3, funciones de AWS Lambda y tablas de Amazon DynamoDB. Con los selectores de eventos básicos no puede filtrar por el campo eventName. Tampoco puede registrar los [eventos de actividad de la red](#).

**Data events** [Info](#)  
Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#) 

**Basic event selectors are enabled**  
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail.

Switch to advanced event selectors

Data event: S3 [Info](#)

Remove

Data event source  
Select source of data events to log.

|          |   |
|----------|---|
| S3       | ▲ |
| S3       | ✓ |
| Lambda   |   |
| DynamoDB |   |

Individual bucket selection  
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

Browse

☒ Read ☒ Write ×

Add bucket

Add data event type



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 selectores de eventos de datos, puede especificar registrar eventos de datos para buckets de Amazon S3, funciones de AWS Lambda, tablas de Amazon DynamoDB o una combinación de estos recursos. Se admiten tipos de recursos 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 conocer 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

Conservar la opción predeterminada All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) permite registrar los eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en un bucket que pertenezca a otra cuenta de 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 la cuenta de AWS.

- 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 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 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 de varias 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 de Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear un registro de seguimiento para una sola región (mediante la AWS CLI), esta opción

habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función Lambda que cree en esa región después de crear el registro de seguimiento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.

El registrar eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en una función que pertenezca a otra cuenta de AWS.

- 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 en la consola de CloudTrail cuando cree un registro de seguimiento. 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 [Administración de registros de seguimiento con la AWS CLI](#).

4. Para agregar otro tipo de datos en el que registrar eventos de datos, elija 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 con la consola de CloudTrail](#).

## Eliminación de un registro de seguimiento con la consola de CloudTrail

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.

### Important

Si bien eliminar un registro de seguimiento de CloudTrail es una acción irreversible, CloudTrail no elimina los archivos de registro del bucket de Amazon S3 de ese registro de seguimiento, del propio bucket de Amazon S3 o del grupo de registro de CloudWatch al que el registro de seguimiento envía los eventos. Al eliminar un registro de seguimiento de varias regiones, se detendrá el registro de los eventos en todas las regiones de AWS habilitadas en su Cuenta de AWS. Si elimina un registro de seguimiento de una sola región, solo se dejarán de registrar los eventos de esa región. No detendrá el registro de eventos en otras regiones, incluso si los registros de seguimiento de esas otras regiones tienen nombres idénticos a los del registro de seguimiento eliminado.

Para obtener información sobre el cierre de las cuentas y la eliminación de los registros de seguimiento de CloudTrail, consulte [Cierre de Cuenta de AWS y registros de seguimiento](#).

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 Consola de administración de AWS 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 registro que ya se hayan entregado al bucket de Amazon S3 no se eliminarán y seguirán incurriendo en cargos de S3.

 Note

El contenido entregado a los buckets de Amazon S3 puede contener contenido del cliente. Para obtener más información sobre la eliminación de datos confidenciales, consulte [Vaciar un bucket](#) y [Eliminar un bucket](#) en la Guía del usuario de Amazon S3.

## Desactivación del registro de un registro de seguimiento

Cuando crea un registro de seguimiento, el registro está activado de forma automática. Puede desactivar un registro de seguimiento desde la página de detalles de dicho registro de seguimiento.

 Note

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 obtener información acerca de los precios de S3, consulte [Precios de Amazon S3](#).

Para desactivar el registro de un registro de seguimiento con la consola de CloudTrail.

1. Inicie sesión en la Consola de administración de AWS 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 administración de registros de seguimiento con la AWS CLI

Puede utilizar la AWS CLI para crear, actualizar y administrar registros de seguimiento. Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la región de AWS 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.

### Note

Para ejecutar los comandos de la AWS (AWS Command Line Interface) de este tema, es necesario disponer de las herramientas de línea de comandos de AWS CLI. Asegúrese de que tiene instalada una versión reciente de la AWS CLI. Para obtener más información, consulte la [Guía del usuario de AWS Command Line Interface](#). Para obtener ayuda con los comandos de CloudTrail en la línea de comandos de la AWS CLI, escriba `aws cloudtrail help`.

## Comandos de uso frecuente para la creación, la administración y el estado de los registros de seguimiento

Estos son algunos de los comandos más utilizados para crear y actualizar registros de seguimiento en CloudTrail:

- [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-trails](#) para devolver información sobre los registros de seguimiento de una región de AWS.
- [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, debe crear registros de seguimiento que registren eventos de todas las regiones de AWS.
- Crear un registro de seguimiento que reciba archivos de registro de todas las cuentas de AWS de una organización con la opción `--is-organization-trail`.
- 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 clave de AWS KMS que ya se ha creado y a la que se ha asociado una política que permite a CloudTrail cifrar los registros. Para obtener más información, consulte [Habilitar y deshabilitar el cifrado de los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail con 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 de registros y el rol de CloudWatch Logs para que CloudTrail pueda enviar eventos a un grupo de registros de CloudWatch Logs. 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 del comando **create-trail** para crear un registro de seguimiento

Puede ejecutar el comando `create-trail` para crear registros de seguimiento configurados específicamente a fin de satisfacer sus necesidades empresariales. Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la región de AWS 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 de varias regiones

Un registro de seguimiento se puede aplicar a todas las Regiones de AWS que estén [habilitadas](#) en su Cuenta de AWS o se puede aplicar a una sola región. Un registro de seguimiento que se aplica a todas las Regiones de AWS que están habilitadas en su Cuenta de AWS se denomina registro de seguimiento de varias regiones. Como práctica recomendada, le sugerimos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas.

Para crear un registro de seguimiento de varias 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 asegurarse de que registra los eventos de servicios globales y captura toda la actividad de los



eventos de administración de su cuenta de AWS, debe crear registros de seguimiento que registren los eventos de todas las regiones de AWS.

 Note

Cuando crea un registro de seguimiento, si especifica un bucket de Amazon S3 que no se ha creado con CloudTrail, debe asociarle la política correspondiente. Consulte [Política de bucket de Amazon S3 para CloudTrail](#).

En el siguiente ejemplo, se crea un registro de seguimiento de varias regiones denominado *my-trail* y una etiqueta con una clave denominada *Group* con el valor *Marketing* que envía los registros de todas las regiones habilitadas en su cuenta a un bucket existente denominado *amzn-s3-demo-bucket*.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

Para confirmar que el registro de seguimiento es uno de varias regiones, compruebe que en el elemento `IsMultiRegionTrail` de la salida se muestre `true`.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "amzn-s3-demo-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

En la consola de CloudTrail, el registro se activa de forma automática cuando se crean registros de seguimiento.

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 ya debe existir y tener aplicados los permisos de CloudTrail adecuados. Para obtener más información, consulte [Política de bucket de Amazon S3 para CloudTrail](#).

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket
```

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": "amzn-s3-demo-bucket"
}
```

Creación de un registro de seguimiento de varias que tiene habilitada 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 de varias regiones que envía los archivos de registro al bucket especificado. El comando utiliza la opción `--enable-log-file-validation`.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

## Uso del comando **update-trail** para actualizar un registro de seguimiento

### Important

A partir del 22 de noviembre de 2021, AWS CloudTrail cambió la forma en que los registros de seguimiento capturan eventos de servicios globales. Tras el cambio, los eventos creados por Amazon CloudFront, AWS Identity and Access Management y AWS STS se registrarán en la región en la que se crearon, la región Este de EE. UU. (Norte de Virginia), `us-east-1`. Esto hace que el tratamiento de CloudTrail de estos servicios sea coherente con el de otros servicios globales de AWS. 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 consola de CloudTrail y el comando `aws cloudtrail lookup-events` mostrarán estos eventos en la Región de AWS en que se produjeron.

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 puede actualizar los registros de seguimiento de la región de AWS en la que se creó el registro de seguimiento (su región principal). Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la región de AWS 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.

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 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 la AWS CLI o uno de los SDK de AWS para modificar un registro de seguimiento, asegúrese de que la política del bucket del registro de seguimiento está actualizada. Para que su bucket reciba automáticamente eventos de una nueva Región de AWS, la política debe contener 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 de una sola región en un registro de seguimiento de varias 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 de una sola región en un registro de seguimiento de varias regiones

Para cambiar un registro de seguimiento de una sola región existente en uno de varias 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 es ahora uno de varias regiones, compruebe que el elemento `IsMultiRegionTrail` de la salida muestre `true`.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "amzn-s3-demo-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": "amzn-s3-demo-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": "amzn-s3-demo-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. Reemplace *myExistingSingleRegionTrailWithGSE* con el nombre de registro de seguimiento 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 registro de seguimiento para una sola región en `us-east-1` a fin de recibir eventos de CloudFront, IAM y AWS STS:

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --  
name myTrail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

Para validar archivos de registro con la AWS CLI, consulte [Validación de la integridad de los archivos de registros de CloudTrail con la AWS CLI](#).

## Administración de registros de seguimiento con la AWS CLI

La AWS CLI incluye otros comandos que le ayudan a administrar sus registros de seguimiento. Estos comandos permiten agregar etiquetas a los registros de seguimiento, obtener su estado, iniciar y detener el registro en ellos y eliminarlos. Debe ejecutar estos comandos desde la misma región de AWS en la que se creó el registro de seguimiento (su región principal). Cuando utilice la AWS CLI, recuerde que los comandos se ejecutan en la región de AWS 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.



## 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 selectores de eventos de CloudTrail Insights](#)
- [Configuración de selectores de eventos avanzados](#)
- [Configuración de selectores de eventos básicos](#)
- [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 *Propietario* con el valor *Mary* a un 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 *Ubicación* y *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 comando `describe-trails` para recuperar información sobre los registros de seguimiento de una región de AWS. 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": "amzn-s3-demo-bucket1",
      "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": "amzn-s3-demo-bucket2",
      "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": "amzn-s3-demo-bucket3",
      "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": "amzn-s3-demo-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 región de AWS en la que se creó (la región principal) o especificar esa región al agregar el parámetro `--region`.

 Note

Si el registro de seguimiento es de organización y usted es una cuenta miembro de la organización en AWS Organizations, debe proporcionar el ARN completo de ese registro de seguimiento, 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 enviar un archivo de registros a un bucket.

## Configuración de 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 región de AWS en la que se creó

el registro de seguimiento (la región principal) o especificar esa región añadiendo el parámetro `--region` 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 ejemplo siguiente se utiliza `put-insight-selectors` para crear un selector de eventos de Insights para un registro de seguimiento denominado *TrailName3*. Esto habilita la recopilación de eventos de Insights para el registro de seguimiento *TrailName3*. 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 ejemplo siguiente se utiliza `put-insight-selectors` para eliminar el selector de eventos de Insights para un registro de seguimiento denominado *TrailName3*. Al borrar la cadena JSON de selectores

de Insights, se deshabilita la recopilación de eventos de Insights para el registro de seguimiento *TrailName3*.

```
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 avanzados

Puede utilizar selectores de eventos avanzados para registrar los [eventos de administración](#), los [eventos de datos](#) para todos los tipos de recursos y los [eventos de actividad de la red](#).

Por el contrario, puede usar selectores de eventos básicos para registrar los eventos de administración y los eventos de datos para los tipos de recursos `AWS::DynamoDB::Table`, `AWS::Lambda::Function` y `AWS::S3::Object`. Puede usar selectores de eventos básicos o avanzados, pero no ambos. Si aplica selectores de eventos avanzados a un registro de seguimiento que está usando selectores de eventos básicos, estos últimos se sobrescriben.

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 los selectores adicionales.

Debe ejecutar el comando `get-event-selectors` desde la Región de AWS en la que se creó el registro de seguimiento (la región de origen) o agregar el parámetro `--region` para especificar esa región.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

 Note

Si el registro de seguimiento es de organización y ha iniciado sesión en una cuenta miembro de la organización en AWS Organizations, debe proporcionar el ARN completo de ese registro de seguimiento, y no solo el nombre.

El siguiente ejemplo muestra la configuración de un registro de seguimiento que usa selectores de eventos avanzados para registrar los eventos de administración. De forma predeterminada, se configura un registro de seguimiento para registrar todos los eventos de administración y no los de datos ni de la actividad de la red.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/management-events-trail",
  "AdvancedEventSelectors": [
    {
      "Name": "Management events selector",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ]
}
```

Para crear un selector de eventos avanzados, ejecute el comando `put-event-selectors`. Cuando se produce un evento en su cuenta, CloudTrail evalúa la configuración de sus registros de seguimiento. 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](#) y [Registro de eventos de actividad de la red](#).

## Temas



- [Ejemplo de registro de seguimiento con selectores de eventos avanzados específicos](#)
- [Ejemplo de registro de seguimiento que utiliza selectores de eventos avanzados personalizados para registrar eventos de datos de Amazon S3 en eventos de datos AWS Outposts](#)
- [Ejemplo de registro de seguimiento que utiliza selectores de eventos avanzados para excluir eventos de AWS Key Management Service](#)
- [Ejemplo de registro de seguimiento que usa selectores de eventos avanzados para excluir eventos de administración de la API de datos de Amazon RDS](#)

## Ejemplo de registro de seguimiento con selectores de eventos avanzados específicos

En el siguiente ejemplo se crean selectores de eventos avanzados personalizados para un registro de seguimiento denominado *TrailName* a fin de incluir eventos de administración de lectura y escritura (se omite el selector `readOnly`), eventos de datos `PutObject` y `DeleteObject` de todas las combinaciones de bucket/prefijo de Amazon S3, excepto de un bucket llamado `amzn-s3-demo-bucket`, eventos de datos de una función de AWS Lambda denominada `MyLambdaFunction` y eventos de actividad de la red para eventos de acceso denegado de AWS KMS a través de un punto de conexión de VPC. 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:::amzn-s3-demo-bucket/" ] }
    ]
  },
  {
```

```

    "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"] }
    ]
  },
  {
    "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["NetworkActivity"]},
      { "Field": "eventSource", "Equals": ["kms.amazonaws.com"]},
      { "Field": "errorCode", "Equals": ["VpceAccessDenied"]}
    ]
  }
]'
```

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:::amzn-s3-demo-bucket/" ]
    },
  ],
},
{
  "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-2:123456789012:function/
MyLambdaFunction" ]
    }
  ]
},
{
  "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    },
    {
      "Field": "eventSource",
      "Equals": ["kms.amazonaws.com"]
    },
    {
      "Field": "errorCode",
      "Equals": ["VpceAccessDenied"]
    }
  ]
}

```

```

    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}

```

Ejemplo de registro de seguimiento que utiliza selectores de eventos avanzados personalizados para registrar eventos de datos de Amazon S3 en eventos de datos AWS Outposts

En el siguiente ejemplo se muestra cómo configurar el registro de seguimiento a fin de que incluya todos los eventos de datos para todos los objetos de Amazon S3 on AWS Outposts. En esta versión, el valor admitido de los eventos de S3 on AWS Outposts para el campo `resources.type` 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 registro de seguimiento que utiliza selectores de eventos avanzados para excluir eventos de AWS Key Management Service

En el siguiente ejemplo se crea un selector de eventos avanzados para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura (se omite el selector `readOnly`), pero excluye los eventos de AWS Key Management Service (AWS KMS). Como los eventos de AWS KMS se tratan como eventos de administración y puede haber una gran cantidad de ellos, su factura de CloudTrail se puede ver incrementada si tiene más de un registro de seguimiento que captura 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"] }
    ]
  }
]'
```

Ejemplo de registro de seguimiento que usa selectores de eventos avanzados para excluir eventos de administración de la API de datos de Amazon RDS

En el siguiente ejemplo se crea un selector de eventos avanzados para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura (se omite el selector `readOnly`), pero excluye los eventos de administración de la API de datos de Amazon RDS. A fin de excluir eventos de administración de la API de datos de Amazon RDS, especifique el origen de los eventos de la API de datos de Amazon RDS en el valor de cadena del campo `eventSource`: `rdsdata.amazonaws.com`.

Si elige no registrar eventos de administración, no se registrarán los eventos de administración de la API de datos de Amazon RDS y no podrá cambiar la configuración del registro de eventos de la API de datos de Amazon RDS.

Para comenzar de nuevo a registrar eventos de administración de la API de datos de Amazon RDS en un registro de seguimiento, elimine 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 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"] }
    ]
  }
]'
```

### Configuración de selectores de eventos básicos

Solo puede usar selectores de eventos básicos para registrar los eventos de administración y los eventos de datos de los tipos de recursos `AWS::DynamoDB::Table`, `AWS::Lambda::Function` y `AWS::S3::Object`. Puede registrar eventos de administración, todos los tipos de recursos de datos y los eventos de actividad de la red mediante selectores de eventos avanzados.

Puede usar selectores de eventos básicos o avanzados, pero no ambos. Si aplica selectores de eventos básicos a un registro de seguimiento que está usando selectores de eventos avanzados, estos últimos se sobrescriben.

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 Región de AWS en la que se creó (la región de origen) o especificar esa región mediante el parámetro `--region`.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

#### Note

Si el registro de seguimiento es de organización y usted es una cuenta miembro de la organización en AWS Organizations, debe proporcionar el ARN completo de ese registro de seguimiento, y no solo el nombre.

El siguiente ejemplo muestra la configuración de un registro de seguimiento que usa selectores de eventos básicos para registrar los eventos de administración.



```
{
  "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 [Trabajar con CloudTrail Insights](#).

Cuando se produce un evento en su cuenta, CloudTrail evalúa la configuración de sus registros de seguimiento. 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 registro de seguimiento que no registra eventos de AWS Key Management Service](#)
- [Ejemplo de registro de seguimiento que registra eventos de AWS Key Management Service relevantes de bajo volumen](#)
- [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

El siguiente ejemplo crea un selector de eventos a fin de que un registro de seguimiento denominado *TrailName* incluya eventos de administración de solo lectura y de solo escritura, eventos de datos para dos combinaciones de bucket/prefijo de Amazon S3 y eventos de datos para una sola función de AWS Lambda denominada *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:::amzn-s3-
demo-bucket/prefix", "arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket/prefix",
            "arn:aws:s3:::amzn-s3-demo-bucket2/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

El siguiente ejemplo crea un selector de eventos para un registro de seguimiento denominado *TrailName2* que incluye todos los eventos de administración, incluidos los eventos de administración de solo lectura y solo escritura, así como los eventos de datos de todos los buckets de Amazon S3, las funciones de AWS Lambda y las tablas de Amazon DynamoDB de la Cuenta de

AWS. Dado que este ejemplo utiliza selectores de eventos básicos, no puede configurar el registro de eventos de S3 en AWS Outposts, las llamadas JSON-RPC de Amazon Managed Blockchain en los nodos de Ethereum, ni otros tipos de recursos de selectores de eventos avanzados. Con los selectores de eventos básicos tampoco puede registrar los eventos de actividad de la red. Puede utilizar selectores de eventos avanzados para registrar eventos de actividad de la red y eventos de datos de todos los demás tipos de 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"
        }
      ]
    }
  ]
}
```

```

        "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 registro de seguimiento que no registra eventos de AWS Key Management Service

En el ejemplo siguiente se crea un selector de eventos para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura, pero excluye los eventos de AWS Key Management Service (AWS KMS). Como los eventos de AWS KMS se tratan como eventos de administración y puede haber una gran cantidad de ellos, su factura de CloudTrail se puede ver incrementada si tiene más de un registro de seguimiento que captura 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 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 iniciar de nuevo el registro de eventos de AWS KMS en un registro de seguimiento, 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 iniciar de nuevo el registro de eventos de AWS KMS en un registro de seguimiento, pase una matriz vacía como 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}]'
```

Ejemplo de registro de seguimiento que registra eventos de AWS Key Management Service relevantes de bajo volumen

En el ejemplo siguiente, se crea un selector de eventos para un seguimiento llamado *NombreSeguimiento* que incluye los eventos de administración de solo escritura y los eventos de AWS KMS. Como los eventos de AWS KMS se tratan como eventos de administración y puede haber una gran cantidad de ellos, su factura de CloudTrail se puede ver incrementada si tiene más de un registro de seguimiento que captura eventos de administración. El usuario de este ejemplo ha optado por incluir eventos Escritura de AWS KMS, entre los que se incluyen `Disable`, `Delete` y `ScheduleKey`, pero ya no se incluyen acciones de gran volumen como `Encrypt`, `Decrypt` y `GenerateDataKey` (que ahora se tratan como eventos 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 de 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 un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura, pero excluye eventos de la API de datos de Amazon RDS. Como los eventos de API de datos de Amazon RDS se tratan como eventos de administración y puede haber una gran cantidad de ellos, su factura de CloudTrail se puede ver incrementada si tiene más de un registro de seguimiento que captura 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 iniciar de nuevo el registro de eventos de administración de la API de datos de Amazon RDS en un registro de seguimiento, pase una matriz vacía como 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 iniciar de nuevo el registro de eventos de administración de la API de datos de Amazon RDS en un registro de seguimiento, pase una matriz vacía como 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}]'
```

## Detención e inicio del registro de un registro de seguimiento

Los siguientes comandos inician y detienen el registro de CloudTrail.

```
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 trata de enviar los archivos de registros a un bucket con el mismo nombre durante un periodo de tiempo limitado. Si detiene el registro o elimina un registro de seguimiento, CloudTrail Insights se deshabilita en ese registro de seguimiento.

## Eliminación de un registro de seguimiento

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.

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).

#### Important

Si bien eliminar un registro de seguimiento de CloudTrail es una acción irreversible, CloudTrail no elimina los archivos de registro del bucket de Amazon S3 de ese registro de seguimiento, del propio bucket de Amazon S3 o del grupo de registro de CloudWatch al que el registro de seguimiento envía los eventos. Al eliminar un registro de seguimiento de varias regiones, se detendrá el registro de los eventos en todas las regiones de AWS habilitadas en su Cuenta de AWS. Si elimina un registro de seguimiento de una sola región, solo se dejarán de registrar los eventos de esa región. No detendrá el registro de eventos en otras regiones, incluso si los registros de seguimiento de esas otras regiones tienen nombres idénticos a los del registro de seguimiento eliminado.

Para obtener información sobre el cierre de las cuentas y la eliminación de los registros de seguimiento de CloudTrail, consulte [Cierre de Cuenta de AWS y registros de seguimiento](#).

```
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 Consola de administración de AWS, la AWS CLI o la API de servicio para eliminar estos recursos por separado.

## Creación de 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 primera copia de los eventos de administración de cada Región de AWS de una cuenta es gratuita. Si crea más registros de seguimiento que envían los mismos eventos de administración a otros destinos, las entregas posteriores generarán costos de CloudTrail.

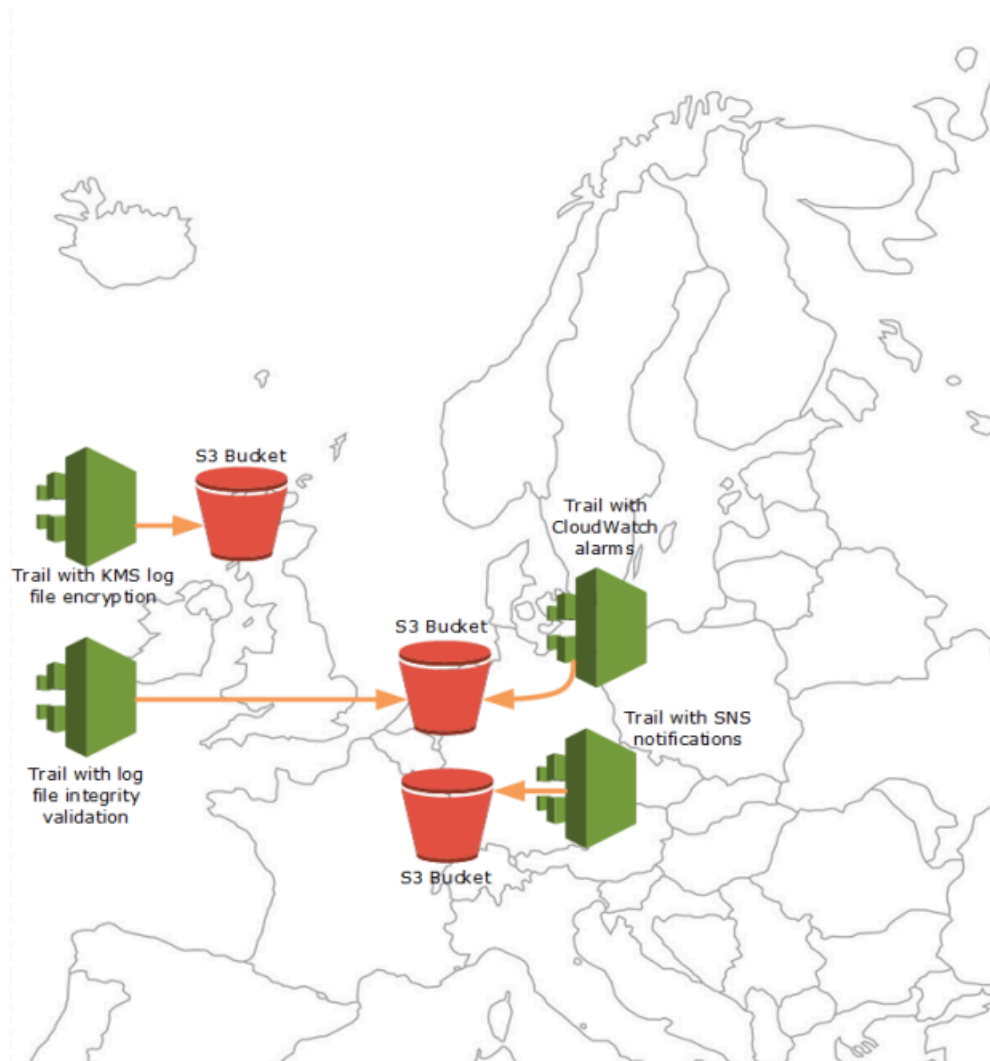


Para obtener más información sobre los costos de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de los registros de seguimiento de CloudTrail](#).

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 hasta cinco registros de seguimiento por Región de AWS. Un registro de seguimiento multirregión 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 de , consulte [Ejemplos: creación y aplicación de políticas para acciones en registros de seguimiento específicos](#).

Para obtener más información sobre varios registros de seguimiento, consulte las [Preguntas frecuentes sobre CloudTrail](#).

## Creación de un registro de seguimiento para una organización

Si ha creado una organización en AWS Organizations, puede crear un registro de seguimiento que registre todos los eventos de todas las Cuentas de AWS en dicha 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 [Cómo agregar un administrador delegado de 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 sobre 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 de seguimiento de la organización creados con la consola son registros de seguimiento multirregión que registran los eventos de las Regiones de AWS [habilitadas](#) en cada cuenta de miembro de la organización. Para registrar eventos en todas las particiones de AWS de su organización, cree un registro de seguimiento multirregión en cada partición. Puede crear un registro de seguimiento de la organización de una sola región o de varias regiones mediante la AWS CLI. Si

crea un registro de seguimiento de una sola región, solo registrará la actividad en la Región de AWS del registro de seguimiento (también denominada región de origen).

Aunque la mayoría de Regiones de AWS están habilitadas por defecto en su Cuenta de AWS, debe habilitar manualmente determinadas regiones (también denominadas regiones optativas). Para obtener información sobre qué regiones están habilitadas por defecto, consulte [Considerations before enabling and disabling Regions](#) en la Guía de referencia de AWS Account Management. Para ver la lista de las regiones que admite CloudTrail, consulte [Regiones compatibles con CloudTrail](#).

Al crear un registro de seguimiento de la organización, se creará una copia con el nombre que le asigne en las cuentas de miembros que pertenezcan a su organización.

- Si el registro de seguimiento de la organización corresponde a una sola región y su región de origen no es una región optativa, se crea una copia en la región de origen del registro de seguimiento de la organización en cada cuenta de miembro.
- Si el registro de seguimiento de la organización corresponde a una sola región y su región de origen es una región optativa, se crea una copia en la región de origen del registro de seguimiento de la organización en las cuentas de miembros que tengan activada esa región.
- Si el registro de seguimiento de la organización es multirregión y su región de origen no es una región optativa, se crea una copia en cada Región de AWS habilitada en cada cuenta de miembro. Cuando una cuenta de miembro habilita una región optativa, tras la activación de dicha región se crea una copia del registro de seguimiento multirregión en la nueva región optativa habilitada.
- Si el registro de seguimiento de la organización es multirregión y la región de origen es una región optativa, las cuentas de miembros no enviarán la actividad al registro de seguimiento de la organización a menos que habiliten la Región de AWS en la que se creó el registro de seguimiento multirregión. Por ejemplo, si crea un registro de seguimiento multirregión y elige la región de Europa (España) como región de origen dicho registro, solo las cuentas de miembros que hayan habilitado la región de Europa (España) en su cuenta enviarán su actividad al registro de seguimiento de la organización.

 Note

CloudTrail crea registros de seguimiento de la organización en las cuentas de miembros aunque falle la validación de un recurso. Ejemplos de errores de validación:

- Una política de buckets de Amazon S3 incorrecta
- Una política de temas de Amazon SNS incorrecta

- Incapacidad de realizar envíos a un grupo de registro de Registros de CloudWatch
- Permisos insuficientes para cifrar mediante una clave de KMS

Las cuentas de miembros con permisos de CloudTrail pueden ver cualquier error de validación de un registro de seguimiento de la organización consultando la página de detalles del registro en la consola de CloudTrail o ejecutando el comando [get-trail-status](#) de la AWS CLI.

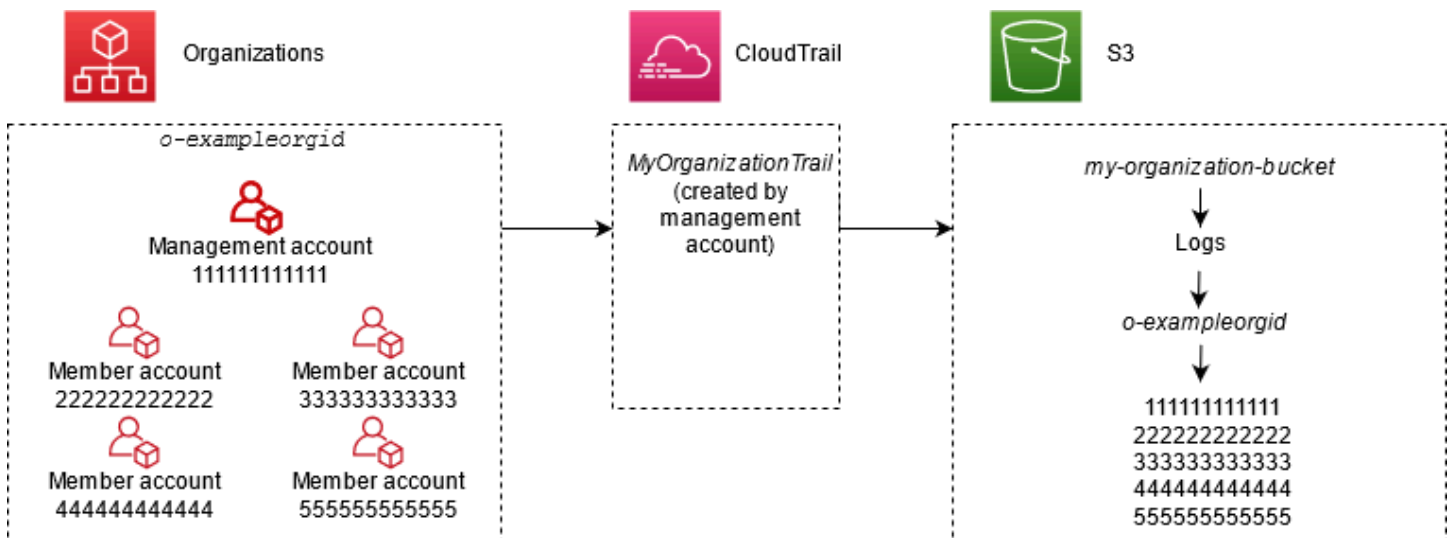
Los usuarios con permisos de CloudTrail en cuentas de miembros podrán ver los registros de seguimiento de la organización cuando inicien sesión en la consola de CloudTrail desde sus Cuentas de AWS o cuando ejecuten comandos de la AWS CLI como `describe-trails`. Sin embargo, los usuarios de cuentas de miembros no tienen permisos suficientes para eliminar los registros de seguimiento de la organización, activar o desactivar el registro, cambiar los tipos de eventos registrados o alterar los registros de seguimiento de la organización de cualquier otro modo.

Al crear un registro de seguimiento de la organización en la consola, o se crea un [rol vinculado a servicio](#) para realizar tareas de registro en las cuentas miembro de la organización. Este rol se denomina `AWSServiceRoleForCloudTrail` y es necesario para que CloudTrail registre los eventos de registro de una organización. Si se agrega una Cuenta de AWS a una organización, el registro de seguimiento de la organización y el rol vinculado al servicio se agregan a esa Cuenta de AWS y se inicia automáticamente el registro para esa cuenta en el registro de seguimiento de la organización. Si se elimina una Cuenta de AWS de una organización, el registro de seguimiento de la organización y el rol vinculado al servicio se eliminarán de la 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 organización de AWS Organizations crea un registro de seguimiento de organización, pero posteriormente se elimina como cuenta de administración de la organización, cualquier registro de seguimiento de organización creado con su cuenta pasa a ser un registro de seguimiento ajeno a la organización.

En el siguiente ejemplo, la cuenta de administración 111111111111 de la organización crea un registro de seguimiento denominado *MyOrganizationTrail* para la organización *o-exampleorgid*. 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 trazas, pero las cuentas miembro no pueden eliminar ni modificar la traza 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 de Amazon S3 para el registro de seguimiento y 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 miembro 444444444444 se elimina de la organización en el futuro, *MyOrganizationTrail* y el rol vinculado a servicios ya no aparecerán en la cuenta 444444444444 de AWS y no se registrarán más eventos para esa cuenta en el registro de seguimiento de la organización. 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 varias 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 de seguimiento en la consola y elige si desea registrar los eventos de datos para los buckets de Amazon S3 o las funciones de AWS Lambda, los únicos recursos que aparecen en la consola de CloudTrail son los de

la cuenta de administración, pero puede agregar los ARN de los recursos de las cuentas miembro. 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 [Registro de eventos de administración](#), [Registro de eventos de datos](#) y [Trabajar con CloudTrail Insights](#).

 Note

En la consola, cree un registro de seguimiento multirregión. Es una práctica recomendada registrar la actividad de todas las regiones habilitadas de su Cuenta de AWS, ya que ayuda a mantener más seguro su entorno de AWS. Para crear un registro de seguimiento de una sola región, [utilice la AWS CLI](#).

Cuando vea eventos en Event history (Historial de eventos) de una organización en AWS Organizations, solo puede ver los eventos de la Cuenta de AWS con la que ha 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.

Puede configurar otros servicios de AWS para efectuar un análisis más detallado y actuar en función de los datos de eventos recopilados en los registros de CloudTrail de un registro de seguimiento de la organización del mismo modo que con cualquier otro registro de seguimiento. Por ejemplo, puede analizar los datos en un registro de seguimiento de organización mediante Amazon Athena. Para obtener más información, consulte [Integraciones de servicios de AWS con registros de CloudTrail](#).

## Temas

- [Cambio de registros de seguimiento de cuentas de miembros a 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](#)
- [Creación de un registro de seguimiento para una organización con la AWS CLI](#)
- [Solución de problemas con un registro de seguimiento de la organización](#)



## Cambio de registros de seguimiento de cuentas de miembros a registros de seguimiento de la organización

Si ya tiene registros de seguimiento de CloudTrail configurados para cuentas miembro individuales, pero desea pasar a un registro de seguimiento de organización a fin de registrar eventos en todas las cuentas, no querrá perder eventos al eliminar registros de seguimiento de cuentas miembro individuales antes de crear un registro de seguimiento 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`. Este rol lo crea Organizations de forma automática al crear la organización y es necesario para que CloudTrail registre 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. Si opta por crear un nuevo bucket de S3 para un registro de seguimiento



de la organización mediante la consola de CloudTrail, su política también debe incluir la acción `s3:PutEncryptionConfiguration` porque el cifrado en el servidor está habilitado de forma predeterminada para el bucket. La siguiente política de ejemplo muestra los permisos mínimos necesarios.

 Note

No debe compartir la política `AWSCloudTrail_FullAccess` de forma amplia en toda su Cuenta de AWS. En cambio, debe restringirla a los administradores de Cuenta de AWS debido al alto nivel de confidencialidad de la información que recopila 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.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "iam:CreateServiceLinkedRole",
        "organizations:DisableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}
```

- Si desea utilizar la AWS CLI o las API de CloudTrail a fin de crear un registro de seguimiento de organización, debe habilitar el acceso de confianza para CloudTrail en Organizations y debe crear manualmente un bucket de Amazon S3 con una política que permita el registro de un registro de

seguimiento de organización. Para obtener más información, consulte [Creación de un registro de seguimiento para una organización con la AWS CLI](#).

- Para utilizar un rol de IAM existente a fin de agregar la supervisión de un registro de seguimiento de organización a Registros de Amazon CloudWatch, debe modificar manualmente el rol de IAM para permitir el envío de Registros de CloudWatch de las cuentas miembro al grupo de Registros de CloudWatch de la cuenta de administración, tal y como se muestra en el siguiente ejemplo.

 Note

Debe utilizar un rol de IAM y un grupo de registro de CloudWatch Logs que exista en su propia cuenta. No puede utilizar un rol de IAM ni un grupo de registro de CloudWatch Logs que pertenezca a otra cuenta.

## JSON

```
{
  "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_*"
    ]
}
]
}

```

Puede obtener más información sobre CloudTrail y Amazon CloudWatch Logs en [Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs](#). Además, tenga en cuenta los límites en CloudWatch Logs y las consideraciones de precio para el servicio antes de decidir habilitar la experiencia para un registro de seguimiento de organización. Para obtener más información, consulte [Límites de CloudWatch Logs](#) y [Precios de Amazon CloudWatch](#).

- 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 la cuenta miembro no se muestran en la consola de CloudTrail al crear un registro de seguimiento; puede buscar recursos en la cuenta de administración en la 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 conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

También debe considerar la posibilidad de revisar cuántos registros de seguimiento ya existen en la cuenta de administración y en las cuentas miembro antes de crear un registro de seguimiento de organización. CloudTrail limita el número de registros de seguimiento 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## 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 de temas de Amazon SNS para CloudTrail](#)

## Creación de un registro de seguimiento para la organización en la consola

Para crear un registro de seguimiento de organización desde la consola de CloudTrail, debe iniciar sesión en ella con un usuario o un rol de la cuenta de administración o la de administrador delegado que tenga [permisos suficientes](#). Si no inicia sesión con la cuenta de administración o la de administrador delegado, no verá la opción para aplicar un registro de seguimiento a una organización cuando cree o edite un registro de seguimiento desde la consola de CloudTrail.

Para crear un registro de seguimiento de organización con la Consola de administración de AWS

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 de los recursos de CloudTrail, los buckets de S3 y las claves de KMS](#).
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. Cuando se crea un bucket, CloudTrail crea y aplica las políticas de buckets necesarias.

 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. Puede elegir un bucket que pertenezca a cualquier cuenta; sin embargo, la política del bucket debe otorgar permiso a CloudTrail 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 registros, cree una carpeta nueva (también conocida como prefijo) en un bucket existente a fin de almacenar los registros de CloudTrail. Ingrese el prefijo en Prefix (Prefijo).

6. En Cifrado SSE-KMS de archivos de registro, elija Habilitado si desea cifrar sus archivos de registro y de resumen con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los archivos de registro y de resumen 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 AWS KMS key New (Nuevo) o Existing (Existente). En AWS KMS Alias (Alias de KMS), especifique un alias, en el formato `alias/MyAliasName`. Para obtener más información, consulte [Actualización de un recurso para que utilice su clave de KMS con la consola](#).

 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 con la consola](#). La política de claves debe permitir que CloudTrail utilice la clave para cifrar los archivos de registro y de resumen, y que los usuarios especificados lean archivos de registro y de resumen 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](#).

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 sus archivos de registros no cambien después de que CloudTrail los envíe. Para obtener más información, consulte [Validar la integridad de los archivos de registros de CloudTrail](#).
  - b. En SNS notification delivery (Envío de notificación SNS), elija Enabled (Habilitado) si desea recibir una notificación cada vez que se envíe un archivo de registros a su bucket. CloudTrail almacena varios eventos en un archivo de registros. 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 de varias regiones, las notificaciones de SNS para las entregas de archivo de registro de todas las regiones se envían al tema de SNS único que haya creado.

Si elige **New** (Nuevo), CloudTrail especifica un nombre para el tema nuevo 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 de temas 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 [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

8. También puede configurar CloudTrail para que envíe archivos de registros a CloudWatch Logs al elegir **Enabled** (Habilitado) en CloudWatch Logs. Para obtener más información, consulte [Envío de eventos a Amazon CloudWatch Logs](#).

 **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.

- a. Si habilita la integración con CloudWatch Logs, elija **New** (Nuevo) para crear un grupo de registros nuevo, o **Existing** (Existente) para utilizar uno existente. Si elige **New** (Nuevo), CloudTrail especifica un nombre para el grupo de registros nuevo o puede escribir un nombre.
- b. Si elige **Existing** (Existente), elija un grupo de registros en la lista desplegable.

- c. Elija New (Nuevo) para crear un rol de IAM nuevo con permisos para enviar registros a CloudWatch 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 para que CloudTrail utilice CloudWatch Logs para el monitoreo..](#)

 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 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. En Etiquetas, puede agregar hasta 50 pares de claves y etiquetas para que lo ayuden a identificar y ordenar su registro de seguimiento y controlar el acceso a él. Las etiquetas pueden ayudarlo a identificar tanto los registros de seguimiento de CloudTrail como 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 [Grupos de recursos de AWS y Etiquetas](#).
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. Elija Exclude AWS KMS events (Excluir eventos de KMS) para filtrar eventos de AWS Key Management Service (AWS KMS) fuera del registro de seguimiento. 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. 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 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 más información, consulte [Precios de AWS CloudTrail](#).

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 recursos](#) y ofrecen un control detallado de los eventos de datos que captura su registro de seguimiento. Si tiene previsto registrar eventos de actividad de la red, debe utilizar selectores de eventos avanzados. Si usa selectores de eventos básicos, siga 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 Tipo de recurso, elija el tipo de recurso en el que desea registrar los eventos de datos. Para obtener más información sobre los tipos de recursos disponibles, consulte [Eventos de datos](#).

13. Elija una plantilla de selector de registros. Puede elegir una plantilla predefinida o elegir Personalizar para definir sus propias condiciones de recopilación de eventos.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.

- Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
- Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
- Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
- Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).

#### Note

Elegir una plantilla predefinida para los buckets de S3 permite el registro de eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos que lleva a cabo cualquier identidad de IAM en su cuenta de AWS, aunque esta se haga en un bucket que pertenezca a otra cuenta de 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 crea un registro de seguimiento de varias regiones, elegir una plantilla predefinida para las funciones de Lambda permite el registro de eventos de datos de todas las funciones que se encuentran actualmente en la cuenta de AWS, así como de cualquier función de Lambda que cree en cualquier región después de crear el registro de seguimiento. Si va a crear un registro de seguimiento para una sola región (mediante la AWS CLI), esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función Lambda que cree en esa región después de crear el registro de seguimiento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.

El registro de eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos que lleve a cabo cualquier identidad de IAM de su cuenta de AWS, aunque esta se haga en una función que pertenezca a otra cuenta de AWS.

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. Si seleccionó Personalizado, en los selectores de eventos avanzados se crea una expresión basada en los valores de los campos de los selectores de eventos avanzados.

 Note

Los selectores no admiten el uso de caracteres comodín como \*. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

a. Elija uno de los siguientes campos.

- **readOnly**: `readOnly` se puede establecer en `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 utilizarlo para incluir o excluir cualquier evento de datos registrado en CloudTrail, como `PutBucket`, `GetItem` o `GetSnapshotBlock`.
- **eventSource**: el origen del evento que se va a incluir o excluir. Este campo puede utilizar cualquier operador.
- **eventType**: el tipo de evento que se va a incluir o excluir. Por ejemplo, puede establecer este campo en no igual a `AwsServiceEvent` para excluir [Servicio de AWSEventos de](#). Para obtener una lista de los tipos de eventos, consulte [eventType](#) en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

- `sessionCredentialFromConsole`: incluya o excluya los eventos que se originan en una sesión de la Consola de administración de AWS. Este campo se puede establecer como igual o no igual con un valor de `true`.
- `userIdentity.arn`: incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento `userIdentity` de CloudTrail](#).
- **`resources.ARN`**: puede utilizar cualquier operador con `resources.ARN`, pero si utiliza `es igual a` o `no es igual a`, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo especificado en la plantilla como el valor de `resources.type`.

 Note

No puede usar el campo `resources.ARN` para filtrar los tipos de recursos que no tienen ARN.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte [Acciones, recursos y claves de condición para los Servicios de AWS](#) en la Referencia de autorizaciones de servicio.

- 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 eventos de datos de dos buckets de S3 de los eventos de datos registrados en su almacén de datos de eventos, puede establecer el campo en `resources.ARN`, configurar el operador en `no comienza por` y, a continuación, pegar un ARN de bucket 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.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- 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 un tipo de datos en el que registrar eventos de datos, elija Agregar tipo de evento de datos. Repita los 12 pasos hasta este paso a fin de configurar selectores de eventos avanzados para el tipo de recursos.
17. Para registrar los eventos de actividad de la red, seleccione Eventos de actividad de la red. Los eventos de actividad de la red permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Se aplican cargos adicionales para registrar eventos de datos. Para más información, consulte [Precios de AWS CloudTrail](#).

Para registrar eventos de actividad de la red, siga estos pasos:

- a. En Origen de eventos de actividad de la red, seleccione el origen de los eventos de actividad de la red.
- b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede optar por registrar todos los eventos de actividad de la red, registrar todos los eventos de acceso denegado a la actividad de la red o seleccionar Personalizar para crear un selector de registro personalizado que filtre por varios campos, como `eventName` y `vpcEndpointId`.
- c. (Opcional) Escriba un nombre para identificar el selector. El nombre del selector aparece como Nombre en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
- d. En Selectores de eventos avanzados, cree expresiones mediante la selección de valores para Campo, Operador y Valor. Puede omitir este paso si utiliza una plantilla de registro predefinida.
  - i. Para excluir o incluir eventos de actividad de la red, puede elegir entre los siguientes campos de la consola.
    - **eventName** – puede utilizar cualquier operador con `eventName`. Puede utilizarlo para incluir o excluir cualquier evento, como `CreateKey`.

- **errorCode** – puede usarlo para filtrar por un código de error. Actualmente, el único errorCode que se admite es VpceAccessDenied.
  - **vpcEndpointId** – identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con vpcEndpointId.
- ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.
  - iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
- e. Para agregar otro origen de eventos de actividad de la red que quiera registrar, seleccione Agregar selector de eventos de actividad de la red.
  - f. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
18. Elija Insights events (Eventos de Insights) si desea que su registro de seguimiento registre 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 actividades inusuales y registra eventos 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 [Trabajar con CloudTrail Insights](#). Se aplican cargos adicionales por registrar eventos de Insights. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

Los eventos de Insights se envían a una carpeta diferente denominada /CloudTrail-Insight del mismo bucket de S3 que se especifica en el área de Storage location (Ubicación de almacenamiento) de la página de detalles del registro de seguimiento. CloudTrail crea el prefijo nuevo en su nombre. Por ejemplo, si el bucket de S3 de destino actual se denomina amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail/, el nombre del bucket de S3 con un nuevo prefijo se denomina amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail-Insight/.

19. Cuando haya terminado de elegir los tipos de eventos para registrar, elija Next (Siguiente).
20. 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).
21. 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 habilitadas en 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 registros que muestran las llamadas a la API de AWS hechas 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.

## Pasos a seguir a continuación

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 con la consola de CloudTrail](#).
- 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 que envíe los archivos de registros a CloudWatch Logs. Para obtener más información, consulte [Envío de eventos a Amazon CloudWatch Logs](#) y [el elemento de CloudWatch Logs](#) en [Prepararse a fin de crear un registro de seguimiento para la organización](#).

 Note

Solo la cuenta de administración puede configurar un grupo de registro de Registros de CloudWatch para un registro de seguimiento 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 para CloudTrail Logs en la consola de CloudTrail](#) 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 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.

## Creación de un registro de seguimiento para una organización con la AWS CLI

Puede crear un registro de seguimiento de organización mediante la AWS CLI. La AWS CLI se actualiza periódicamente con funcionalidad y comandos adicionales. Para ayudar a garantizar el éxito, asegúrese de que ha instalado o actualizado una versión reciente de la AWS CLI antes de comenzar.

#### 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 AWS CLI para administrar registros de seguimiento, consulte [Administración de registros de seguimiento con la AWS CLI](#) y [Configuración del monitoreo de CloudWatch Logs con la AWS CLI](#). Cuando se crea o actualiza un registro de seguimiento de organización con la AWS CLI, se debe utilizar un perfil de la AWS CLI de la cuenta de administración o 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 un 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 bucket debe tener una política que permita a CloudTrail guardar los archivos de registros de la organización en el bucket.

A continuación, se muestra un ejemplo de política para un bucket de Amazon S3 denominado *amzn-s3-demo-bucket*, que es propiedad de la cuenta de administración de la organización. Reemplace *amzn-s3-demo-bucket*, *region*, *managementAccountID*, *trailName* y *o-organizationID* por los valores de su organización.

Esta política de bucket contiene tres instrucciones.

- La primera instrucción permite a CloudTrail hacer una llamada a la acción `GetBucketAcl` 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 CloudTrail escribe en el bucket de S3 solo para una traza o trazas 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.

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
```

```

    "Principal": {
      "Service": [
        "cloudtrail.amazonaws.com"
      ]
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "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:::amzn-s3-demo-bucket/
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:::amzn-s3-demo-bucket/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](#).

## Habilitación de CloudTrail como servicio de confianza 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 características, debe configurar Organizations para que confíe en CloudTrail como un servicio de confianza.

Para crear la 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

Cuando se crea un registro de seguimiento de organización con la AWS CLI, se debe utilizar un perfil de la AWS CLI de la cuenta de administración o 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 *amzn-s3-demo-bucket*:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-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 seguimiento de organización que solo registra eventos en una sola Región de AWS, también conocido como registro de seguimiento de una sola región. La región de AWS en la que se registrarán los eventos es la región especificada en el perfil de configuración para la AWS CLI.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-organization-trail
```

Para obtener más información, consulte [Requisitos de nomenclatura de los recursos de CloudTrail, los buckets de S3 y las claves de KMS](#).

Salida 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": "amzn-s3-demo-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 utiliza la AWS CLI o uno de los SDK de AWS para actualizar un registro de seguimiento, asegúrese de que la política de bucket del registro de seguimiento se encuentre actualizada. Para obtener más información, consulte [Creación de un registro de seguimiento para una organización con la AWS CLI](#).

Cuando se actualiza un registro de seguimiento de organización con la AWS CLI, se debe utilizar un perfil de la AWS CLI de la cuenta de administración o 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 seguimiento de la organización en las cuentas de miembros aunque falle la validación de un recurso. Ejemplos de errores de validación:

- Una política de buckets de Amazon S3 incorrecta
- Una política de temas de Amazon SNS incorrecta
- Incapacidad de realizar envíos a un grupo de registro de Registros de CloudWatch
- Permisos insuficientes para cifrar mediante una clave de KMS

Las cuentas de miembros con permisos de CloudTrail pueden ver cualquier error de validación de un registro de seguimiento de la organización consultando la página de detalles del registro en la consola de CloudTrail o ejecutando el comando [get-trail-status](#) de la AWS CLI.

## Aplicación de un registro de seguimiento existente a una organización

Para cambiar un registro de seguimiento existente de modo que también se aplique a una organización en lugar de a una sola cuenta de AWS, agregue la opción `--is-organization-trail`, 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": "amzn-s3-demo-bucket"
}
```

En el ejemplo anterior, el registro de seguimiento se configuró como registro de seguimiento de varias 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 una sola región en un registro de seguimiento de varias regiones

Para convertir un registro de seguimiento de organización de una sola región existente en un registro de seguimiento de organización de varias regiones, agregue la opción `--is-multi-region-trail` tal 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 varias regiones, controle que 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": "amzn-s3-demo-bucket"
}
```

# Solución de problemas con un registro de seguimiento de la organización

En esta sección, se ofrece información sobre cómo solucionar los problemas con un registro de seguimiento de la organización.

## Temas

- [CloudTrail no envía eventos](#)
- [CloudTrail no envía notificaciones de Amazon SNS a una cuenta de miembro de una organización](#)

## CloudTrail no envía eventos

Si CloudTrail no envía los archivos de registro de CloudTrail al bucket de Amazon S3

Compruebe si hay algún problema con el bucket de S3.

- Desde la consola de CloudTrail, consulte la página de detalles del registro de seguimiento. Si hay algún problema con el bucket de S3, la página de detalles incluye una advertencia de que se ha producido un error en la entrega al bucket de S3.
- Desde AWS CLI, ejecute el comando [get-trail-status](#). Si se produce un error, el resultado del comando incluye el campo LatestDeliveryError, que muestra cualquier error de Amazon S3 que CloudTrail haya detectado al intentar enviar los archivos de registro al bucket designado. Este error solo se produce cuando hay algún 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 de bucket para que CloudTrail pueda escribir en él o cree un nuevo bucket y, a continuación, llame a `update-trail` para especificar el nuevo bucket. Para obtener información sobre la política de bucket de la organización, consulte [Creación o actualización de un bucket de Amazon S3 para utilizarlo para almacenar los archivos de registro de un registro de seguimiento de la organización](#).

### 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.



## Si CloudTrail no entrega los registros a Registros de CloudWatch

Compruebe si hay algún problema con la configuración de la política de roles de Registros de CloudWatch.

- Desde la consola de CloudTrail, consulte la página de detalles del registro de seguimiento. Si hay algún problema con Registros de CloudWatch, la página de detalles incluye una advertencia que indica que se ha producido un error en la entrega de Registros de CloudWatch.
- Desde AWS CLI, ejecute el comando [get-trail-status](#). Si se produce un error, el resultado del comando incluye el campo LatestCloudWatchLogsDeliveryError, que muestra cualquier error de Registros de CloudWatch que CloudTrail haya detectado al intentar enviar los registros a Registros de CloudWatch. Para resolver el problema, corrija la política de roles de Registros de CloudWatch. Para obtener información acerca de la política de roles de Registros de CloudWatch, consulte [Documento de política de roles para que CloudTrail utilice CloudWatch Logs para el monitoreo](#).

Si no ve la actividad de una cuenta de miembro en un registro de seguimiento de la organización

Si no ve la actividad de una cuenta de miembro en un registro de seguimiento de la organización, compruebe lo siguiente:

- Compruebe la región de origen del registro de seguimiento para comprobar si es una región optativa

Aunque la mayoría de Regiones de AWS están habilitadas por defecto en su Cuenta de AWS, debe habilitar manualmente determinadas regiones (también denominadas regiones optativas). Para obtener información sobre qué regiones están habilitadas por defecto, consulte [Considerations before enabling and disabling Regions](#) en la Guía de referencia de AWS Account Management. Para ver la lista de las regiones que admite CloudTrail, consulte [Regiones compatibles con CloudTrail](#).

Si el registro de seguimiento de la organización es multirregión y la región de origen es una región optativa, las cuentas de miembros no enviarán la actividad al registro de seguimiento de la organización a menos que habiliten la Región de AWS en la que se creó el registro de seguimiento multirregión. Por ejemplo, si crea un registro de seguimiento multirregión y elige la región de Europa (España) como región de origen dicho registro, solo las cuentas de miembros que hayan habilitado la región de Europa (España) en su cuenta enviarán su actividad al registro de seguimiento de la organización. Para resolver el problema, habilite la región optativa en cada

cuenta de miembro de la organización. Para obtener información sobre cómo habilitar una región optativa, consulte [Enable or disable a Region in your organization](#) en la Guía de referencia de AWS Account Management.

- Compruebe si la política basada en recursos de la organización entra en conflicto con la política de roles vinculados a servicios de CloudTrail

CloudTrail usa el rol vinculado a un servicio denominado [AWSServiceRoleForCloudTrail](#) para admitir los registros de seguimiento de la organización. Este rol vinculada a un servicio permite a CloudTrail realizar acciones en los recursos de la organización, como por ejemplo `organizations:DescribeOrganization`. Si la política basada en recursos de la organización deniega una acción que está permitida en la política de roles vinculados a un servicio, CloudTrail no podrá realizar la acción aunque esté permitida en la política de roles vinculados a un servicio. Para resolver el problema, corrija la política basada en recursos de la organización para que no deniegue las acciones que están permitidas en la política de roles vinculados a un servicio.

## CloudTrail no envía notificaciones de Amazon SNS a una cuenta de miembro de una organización

Si una cuenta de miembro con un registro de seguimiento de la organización de AWS Organizations no envía notificaciones de Amazon SNS, podría haber un problema con la configuración de la política de temas de SNS. CloudTrail crea registros de seguimiento de la organización en las cuentas de miembros incluso si hay algún error durante la validación de un recurso; por ejemplo, el tema de SNS del registro de seguimiento de la organización no incluye todos los ID de las cuentas de 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 un registro de seguimiento tiene un error de autorización:

- Desde la consola de CloudTrail, consulte la página de detalles del registro de seguimiento. Si se produce un error en la autorización, la página de detalles incluye una advertencia de SNS `authorization failed` e indica que hay que corregir la política de temas de SNS.
- Desde AWS CLI, ejecute el comando [get-trail-status](#). Si se produce un error de autorización, el resultado del comando incluye el campo `LastNotificationError` con un valor de `AuthorizationError`. Para resolver el problema, corrija la política de temas de Amazon SNS. Para obtener más información acerca de la política de temas de Amazon SNS, consulte [Política de temas de Amazon SNS para CloudTrail](#).

Para obtener información acerca de los temas de SNS y cómo suscribirse a ellos, consulte [Introducción a Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

## Cómo entender los registros de seguimiento de varias regiones y las regiones optativas

Un registro de seguimiento se puede aplicar a todas las Regiones de AWS que estén [habilitadas](#) en su Cuenta de AWS o se puede aplicar a una sola región. Un registro de seguimiento que se aplica a todas las Regiones de AWS que están habilitadas en su Cuenta de AWS se denomina registro de seguimiento de varias regiones. Como práctica recomendada, le sugerimos crear un registro de seguimiento de varias regiones, ya que captura la actividad en todas las regiones habilitadas. Todos los registros de seguimiento que se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones. Solo puede crear un registro de seguimiento de una sola región mediante el AWS CLI o la operación API de [CreateTrail](#).

Aunque la mayoría de Regiones de AWS están habilitadas por defecto en su Cuenta de AWS, debe habilitar manualmente determinadas regiones (también denominadas regiones optativas). Para obtener información sobre qué regiones están habilitadas por defecto, consulte [Considerations before enabling and disabling Regions](#) en la Guía de referencia de AWS Account Management. Para ver la lista de las regiones que admite CloudTrail, consulte [Regiones compatibles con CloudTrail](#).

### Temas

- [¿Cuáles son las ventajas de los registro de seguimiento de varias regiones?](#)
- [¿Qué ocurre cuando se crea un registro de seguimiento de varias regiones?](#)
- [¿Qué sucede cuando se habilita una región optativa?](#)
- [¿Qué sucede cuando se deshabilita una región optativa?](#)

## ¿Cuáles son las ventajas de los registro de seguimiento de varias regiones?

Los registros de seguimiento multirregión tienen las siguientes ventajas:

- Los valores de configuración del registro de seguimiento se aplican de forma sistemática a todas las Regiones de AWS [habilitadas](#).
- Recibirá eventos de CloudTrail desde todas las Regiones de AWS habilitadas en un único bucket de Amazon S3 y, de manera opcional, en un grupo de registro de Registros de CloudWatch.

- Las configuraciones del registro de seguimiento para todas las Regiones de AWS habilitadas se administran desde una sola ubicación.

## ¿Qué ocurre cuando se crea un registro de seguimiento de varias regiones?

Crear un registro de seguimiento de varias regiones tiene los siguientes efectos:

- CloudTrail envía los archivos de registros sobre la actividad de la cuenta desde todas las Regiones de AWS [habilitadas](#) al bucket de Amazon S3 que se especifique y, de manera opcional, a un grupo de registro de registros de CloudWatch.
- Si ha configurado un tema de Amazon SNS para el registro de seguimiento, las notificaciones de SNS sobre los envíos de archivos de registros de todas las Regiones de AWS habilitadas se envían a este tema de SNS de forma exclusiva.
- Puede ver el registro de seguimiento de varias regiones en todas las Regiones de AWS habilitadas, pero solo puede modificar el registro de seguimiento en la región de origen en la que se creó.

## ¿Qué sucede cuando se habilita una región optativa?

Después de habilitar una región optativa, en CloudTrail se crea una copia idéntica de cada registro de seguimiento de varias regiones de la región optativa que habilitó.

CloudTrail utiliza un modelo de computación distribuida denominado [coherencia final](#). Como la activación de una región demora entre unos minutos y varias horas, es posible que no vea de inmediato todos los eventos en los registros de la región recién habilitada. CloudTrail puede demorar varias horas en entregar todos los registros de la región recién habilitada. Durante este periodo, puede ver los últimos 90 días de los eventos de administración registrados en esa región consultando el [Historial de eventos](#) de CloudTrail o ejecutando el comando [aws cloudtrail lookup-events --region <region>](#). El historial de eventos está habilitado de manera predeterminada en su Cuenta de AWS, captura los últimos 90 días de los eventos de administración registrados en una región y no requiere un registro de seguimiento.

Para obtener información sobre cómo habilitar una región optativa para la Cuenta de AWS, consulte [Habilitar o deshabilitar una región para cuentas independientes](#) o [Habilitar o deshabilitar de una región en la organización](#).

## ¿Qué sucede cuando se deshabilita una región optativa?

Como su cuenta puede tener actividad en la región que deshabilitó, como acciones Servicios de AWS para eliminar recursos, en CloudTrail se seguirá registrando la actividad e intentando enviar eventos al bucket de S3 para cualquier registro de seguimiento que no se elimine antes de deshabilitar la región.

## Copia de 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. 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 registros de seguimiento en un almacén de datos de eventos existente configurado para los eventos de CloudTrail, o puede crear un nuevo almacén de datos de eventos de CloudTrail y seleccionar la opción Copiar eventos de los registros de seguimiento como parte de la creación del almacén 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 registros de seguimiento a un almacén de datos de eventos existente con la consola de CloudTrail](#). Para obtener más información acerca de la creación de un nuevo almacén de datos de eventos, consulte [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

Copiar eventos de registro de seguimiento en un almacén de datos de eventos de CloudTrail Lake le permite ejecutar consultas en los eventos copiados. Las consultas de CloudTrail Lake ofrecen una visión más detallada y personalizable de los eventos que las simples búsquedas de claves y valores en el Event history (Historial de eventos), o ejecutando LookupEvents. Para obtener más información acerca de CloudTrail Lake, consulte [Trabajar 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.

Los almacenes de datos de eventos de CloudTrail Lake conllevan gastos. 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 los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#) y [Administración de los costos de CloudTrail Lake](#).

Cuando copia los eventos de registros de seguimiento en un almacén de datos de eventos de CloudTrail Lake, genera cargos según la cantidad de datos de eventos que ingiera el almacén de datos de eventos.

Al copiar eventos de registros de seguimiento en CloudTrail Lake, CloudTrail descomprime los registros que están almacenados en formato gzip (comprimido) y, a continuación, 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 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 [Administración de los costos de CloudTrail Lake](#).

## 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?                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Analizar y consultar eventos de registros de seguimiento históricos en CloudTrail Lake sin ingerir nuevos eventos | Cree un <a href="#">nuevo almacén de datos de eventos</a> 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 el registro de seguimiento existente por un almacén de datos de eventos de CloudTrail Lake              | Cree un almacén de datos de eventos con los mismos selectores 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.                                                                                                                                                                                                                 |

| Escenario | ¿Cómo puedo lograr esto en la consola?                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <p>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.</p> <p>Después de crear el almacén de datos de eventos, puede desactivar el registro del registro de seguimiento para evitar cargos adicionales.</p> |

## Temas

- [Consideraciones para copiar eventos de registros de seguimiento](#)
- [Permisos necesarios para copiar eventos de registro de seguimiento](#)
- [Copiar eventos de registros de seguimiento a un almacén de datos de eventos existente con la consola de 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 registros de seguimiento, CloudTrail utiliza la operación de la API [GetObject](#) de S3 para recuperar los eventos de registros de seguimiento en el bucket 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.
- Cuando copia eventos de registros de seguimiento en un almacén de datos de eventos, CloudTrail copia todos los eventos de registros de seguimiento, independientemente de la configuración de los tipos de eventos, los selectores de eventos avanzados o la Región de AWS del almacén de datos de eventos de destino.
- 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](#).
- Periodo de retención: el periodo de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos de eventos. CloudTrail solo copia los eventos de registros de seguimiento que tengan un valor de eventTime dentro del periodo de retención del almacén de datos de eventos. 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 conservar los eventos en el almacén de datos de eventos (periodo de retención = *el evento más antiguo en días* más *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.
- 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 registro de seguimiento de los archivos de registros comprimidos Gzip que están en el bucket de S3 de origen. CloudTrail no copia los eventos de registro de seguimiento de los archivos de registros sin comprimir ni de los archivos de registros 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 los eventos de CloudTrail contenidos en el prefijo CloudTrail del bucket de S3 y los prefijos dentro del prefijo CloudTrail y no comprueba los prefijos de otros servicios de AWS. Si desea copiar los eventos de CloudTrail contenidos en otro prefijo, debe elegir el prefijo al copiar los eventos del registro 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 registro de seguimiento, asegúrese de tener todos los permisos necesarios para su rol 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 elige crear un nuevo rol de IAM, CloudTrail proporciona todos los permisos necesarios para el rol.

Si el bucket de S3 de origen usa una clave de KMS para el cifrado de datos, verifique que la política de la clave de KMS permite a CloudTrail descifrar datos en el bucket. Si el bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave de manera que permitan a CloudTrail descifrar los datos que se encuentran en el 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. Cuando elige un nuevo rol de IAM, CloudTrail crea un rol de IAM con los permisos necesarios y no se requiere ninguna acción adicional de su parte.

Si elige un rol existente, asegúrese de que las políticas de roles de IAM permitan a CloudTrail copiar los eventos de registro de seguimiento desde el bucket de S3 de origen. Esta sección proporciona ejemplos de las políticas de confianza y de permisos necesarias para el rol de IAM.

El siguiente ejemplo muestra la política de permisos, que permite a CloudTrail copiar los eventos de registro de seguimiento en el bucket de S3 de origen. Sustituya *amzn-s3-demo-bucket*, *myAccountID*, *region*, *prefix* y *eventDataStoreId* por los valores correspondientes para la configuración. *myAccountID* es el ID de la cuenta de AWS utilizado para CloudTrail Lake, que puede no ser el ID de la cuenta de AWS del bucket de S3.

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:::amzn-s3-demo-bucket"
      ],
      "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:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/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 muestra la política de confianza de IAM, que permite a CloudTrail asumir un rol de IAM para copiar los eventos de registro de seguimiento del bucket de S3. Complete *myAccountID* (ID de la cuenta), *region* (Región) y *eventDataStoreArn* (ARN del almacén de datos de eventos) con los valores apropiados para la configuración. *myAccountID* es el ID de la Cuenta de AWS que se usa para CloudTrail Lake, que puede no ser igual al ID de la cuenta de AWS 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 registro de seguimiento, debe actualizar la política de buckets de S3 para permitir que CloudTrail copie los eventos de registro de seguimiento en el bucket de S3.

Puede agregar la siguiente instrucción a la política de buckets de S3 para conceder estos permisos. Sustituya *roleArn* y *amzn-s3-demo-bucket* por los valores apropiados para la configuración.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3::amzn-s3-demo-bucket",
    "arn:aws:s3::amzn-s3-demo-bucket/*"
  ]
},
```

## Política de claves KMS para descifrar datos en el bucket de S3 de origen

Si el bucket de S3 de origen usa una clave de KMS para el cifrado de datos, verifique que la política de claves de KMS proporcione a CloudTrail los permisos necesarios `kms:Decrypt` y `kms:GenerateDataKey` para copiar eventos de registros de seguimiento de un bucket de S3 con el cifrado SSE-KMS activado. Si su bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave. Actualizar la política de la clave de KMS permite a CloudTrail descifrar los datos en el bucket de S3 de origen, ejecutar comprobaciones de validación para garantizar que los eventos cumplan los estándares de CloudTrail y copiar los eventos en el almacén de datos de eventos de CloudTrail Lake.

El siguiente ejemplo muestra la política de la clave de KMS, la cual permite a CloudTrail descifrar los datos en el bucket de S3 de origen. Sustituya *roleArn*, *amzn-s3-demo-bucket*, *myAccountID*, *region* y *eventDataStoreId* por los valores apropiados para su configuración. *myAccountID* es el ID de la cuenta de AWS utilizado para CloudTrail Lake, que puede no ser el ID de la cuenta de AWS del bucket de S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
        "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

## Copiar eventos de registros de seguimiento a un almacén de datos de eventos existente con la consola de 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 [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

### 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](#).

- **Periodo de retención:** el periodo de retención determina cuánto tiempo se guardan los datos del evento en el almacén de datos de eventos. CloudTrail solo copia los eventos de registros de seguimiento que tengan un valor de `eventTime` dentro del periodo de retención del almacén de datos de eventos. 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 conservar los eventos en el almacén de datos de eventos (periodo de retención = *el evento más antiguo en días* más *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.

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

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. Elija Trails (Registros de seguimiento) en el panel de navegación izquierdo de la consola de CloudTrail.
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 bucket de S3 de origen para el registro de seguimiento usa una clave de KMS para el cifrado de datos, asegúrese de que la política de la clave de KMS permita que CloudTrail descifre los datos que se encuentran en el bucket. Si el bucket de S3 de origen utiliza varias claves de KMS, debe actualizar la política de cada clave de manera que permitan a CloudTrail descifrar datos en el 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](#).
4. (Opcional) De forma predeterminada, CloudTrail solo copia los eventos de CloudTrail contenidos en el prefijo `CloudTrail` del bucket S3 y los prefijos dentro del prefijo `CloudTrail` y no comprueba los prefijos de otros servicios de AWS. Si desea copiar los eventos de CloudTrail contenidos en otro prefijo, elija Enter S3 URI (Introducir la URI de S3) y, a continuación, elija Browse S3 (Examinar S3) para buscar el prefijo.

La política de buckets de S3 debe conceder acceso a CloudTrail para copiar los eventos de registro 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 intervalo de tiempo de eventos, seleccione el intervalo de tiempo de copia de los eventos. CloudTrail comprueba el prefijo y el nombre del registro para comprobar que el nombre contenga una fecha situada entre la fecha de inicio y la fecha de finalización elegidas antes de intentar copiar los eventos del registro 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 registros de seguimiento que tengan un valor de `eventTime` dentro del periodo de retención del almacén de datos de eventos. Por ejemplo, si el periodo de retención de un almacén de datos de eventos es de 90 días, CloudTrail no copiará ningún evento de registro de seguimiento con un valor de `eventTime` anterior a 90 días.

- Si elige Intervalo relativo, puede elegir si desea copiar los eventos registrados en los últimos 6 meses, 1 año, 2 años, 7 años o un intervalo personalizado. CloudTrail copia los eventos registrados dentro del periodo seleccionado.
  - Si selecciona Absolute range (Intervalo absoluto), puede elegir fechas de inicio y de finalización específicas. CloudTrail copia los eventos que se produjeron entre las fechas de inicio y de finalización seleccionadas.
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.

- Seleccione Usar 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.
  - 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 de la copia 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). Cuando vuelva a realizar la copia, CloudTrail reanuda la copia 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 [Visualización de detalles de la copia de eventos con la consola de CloudTrail](#).

## 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 servicio 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 registros de CloudTrail](#)
- [Descarga de los archivos de registros de CloudTrail](#)

## Búsqueda de los archivos de registros de CloudTrail

CloudTrail publica archivos de registros 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 de bucket que ha especificado al crear el registro de seguimiento (que se encuentra en la página Trails (Registros de seguimiento) de la consola de CloudTrail).
- 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:

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/  
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

 Note

Para los registros de seguimiento de la organización, el nombre de objeto del archivo de registro en el bucket de S3 incluye el ID de la unidad organizativa en la ruta, tal y como se indica a continuación:

```
amzn-s3-demo-bucket/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  
  amzn-s3-demo-bucket  
    AWSLogs  
      123456789012  
        CloudTrail  
          us-west-1  
            2014  
              06
```

Un archivo de registro para la jerarquía de objetos anterior se parecerá a lo siguiente:

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTX0A3Vnhbc.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 event ID. Para obtener más información acerca del campo event ID, consulte [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

## 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.

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 [Información general de los 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 Consola de administración de AWS.

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 [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

AWS colabora con terceros especialistas en el registro y análisis para proporcionar soluciones que utilizan la información de CloudTrail. Para obtener más información, consulte [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 eventos de CloudTrail](#).

## 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

En la consola de CloudTrail, puede configurar un registro de seguimiento para que utilice un tema de Amazon SNS habilitando la opción de entrega de notificaciones de SNS al [crear](#) o [actualizar](#) un registro de seguimiento. Si elige un tema nuevo, CloudTrail crea el tema de Amazon SNS de manera automática y adjunta una política adecuada, de forma que CloudTrail tenga permiso para publicar en ese tema.

Con el AWS CLI, puede [crear](#) o [actualizar](#) un registro de seguimiento para usar un tema de Amazon SNS mediante la especificación de un valor para el parámetro `--sns-topic-name`. Puede especificar el nombre o el ARN para el tema de Amazon SNS.

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 las notificaciones para un registro de seguimiento de varias 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 [Suscripción a un tema de Amazon SNS](#) 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 [Suscripción de una cola de Amazon SQS a un tema de Amazon SNS \(consola\)](#) 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": "amzn-s3-demo-bucket", "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": "amzn-s3-demo-bucket",
  "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 información sobre la estructura JSON, consulte [Fanout to Amazon SQS queues](#) 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 de temas 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](#).

## 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 privada entre su VPC y AWS CloudTrail. Puede utilizar esta conexión para habilitar que CloudTrail se comuniquen 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 usted 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.

Con el fin de conectar la VPC a CloudTrail, debe definir un punto de enlace de la VPC de la 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 de enlace ofrece conectividad escalable de confianza con CloudTrail sin necesidad de utilizar una gateway de Internet, una instancia de conversión de las direcciones de red (NAT) o una conexión de 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 la tecnología de 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](#).

Las siguientes secciones son para usuarios de Amazon VPC. Para obtener más información, consulte [Introducción a Amazon VPC](#) en la Guía del usuario de Amazon VPC.

## Temas

- [Regiones](#)
- [Crear un punto de enlace de la VPC para CloudTrail](#)
- [Crear una política de punto de conexión de VPC para CloudTrail](#)
- [Subredes compartidas](#)

## Regiones

AWS CloudTrail admite los puntos de conexión de VPC y las políticas de punto de conexión de VPC en todas las Regiones de AWS en las que se admite CloudTrail.

### Crear un punto de enlace de la VPC para CloudTrail

Con el fin de comenzar a utilizar CloudTrail con la VPC, cree un punto de enlace de la VPC de interfaz para CloudTrail. Para obtener más información, consulte [Acceso a un Servicio de AWS a través de un punto de conexión de VPC de interfaz](#) en la Guía del usuario de Amazon VPC.

No necesita cambiar la configuración de CloudTrail. CloudTrail llama a otros Servicios de AWS con puntos de conexión públicos o puntos de conexión de VPC de interfaz privados, lo que esté en uso.

### Crear una política de punto de conexión de VPC para CloudTrail

Una política de punto de conexión de VPC es un recurso de IAM que puede adjuntar a un punto de conexión de VPC de interfaz. La política de punto de conexión predeterminada brinda acceso completo a las API de CloudTrail a través del punto de conexión de VPC de interfaz. Para controlar el acceso otorgado a CloudTrail desde su VPC, adjunte una política de punto de conexión personalizada al punto de conexión de VPC de interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.



Para obtener más información acerca de las políticas de punto de conexión de VPC, incluida cómo actualizar una política, consulte [Control del acceso a los servicios con puntos de conexión de VPC](#) en la Guía del usuario de VPC de Amazon.

A continuación, se muestran ejemplos de políticas de punto de conexión de VPC personalizadas para CloudTrail.

Ejemplos de políticas:

- [Ejemplo: permitir todas las acciones de CloudTrail](#)
- [Ejemplo: permitir acciones de CloudTrail específicas](#)
- [Ejemplo: denegar todas las acciones de CloudTrail](#)
- [Ejemplo: denegar acciones específicas de CloudTrail](#)
- [Ejemplo: permitir todas las acciones de CloudTrail desde una VPC específica](#)
- [Ejemplo: permitir todas las acciones de CloudTrail desde un punto de conexión de VPC específico](#)

## Ejemplo: permitir todas las acciones de CloudTrail

La siguiente política de punto de conexión de VPC de muestra concede acceso a todas las acciones de CloudTrail para todas las entidades principales en todos los recursos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "cloudtrail:*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

## Ejemplo: permitir acciones de CloudTrail específicas

La siguiente política de punto de conexión de VPC de muestra concede acceso para realizar las acciones de `cloudtrail:ListTrails` y `cloudtrail:ListEventDataStores` para todas las entidades principales en todos los recursos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["cloudtrail:ListTrails",
"cloudtrail:ListEventDataStores"],
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

## Ejemplo: denegar todas las acciones de CloudTrail

La siguiente política de punto de conexión de VPC de muestra deniega acceso a todas las acciones de CloudTrail para todas las entidades principales en todos los recursos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "cloudtrail:*",
      "Effect": "Deny",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

## Ejemplo: denegar acciones específicas de CloudTrail

La siguiente política de punto de conexión de VPC de muestra deniega las acciones de `cloudtrail:CreateTrail` y `cloudtrail:CreateEventDataStore` para todas las entidades principales en todos los recursos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": ["cloudtrail:CreateTrail",
"cloudtrail:CreateEventDataStore"],
      "Effect": "Deny",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

## Ejemplo: permitir todas las acciones de CloudTrail desde una VPC específica

La siguiente política de punto de conexión de VPC de muestra concede acceso para realizar todas las acciones de CloudTrail para todas las entidades principales en todos los recursos, pero solo si el solicitante utiliza la VPC específica para realizar la solicitud. Reemplace *vpc-id* por el ID de la VPC.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudtrail:*",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "StringEquals": {
```

```

    "aws:SourceVpc": "vpc-1234567890abcdef0"
  }
}
]
}

```

Ejemplo: permitir todas las acciones de CloudTrail desde un punto de conexión de VPC específico

La siguiente política de punto de conexión de VPC de muestra concede acceso para realizar todas las acciones de CloudTrail para todas las entidades principales en todos los recursos, pero solo si el solicitante utiliza el punto de conexión de VPC específico para realizar la solicitud. Reemplace *vpc-endpoint-id* por su ID de punto de conexión de VPC.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudtrail:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}

```

## Subredes compartidas

Un punto de conexión de VPC de CloudTrail, como cualquier otro punto de conexión de VPC, solo lo puede crear una cuenta de propietario en la subred compartida. No obstante, una cuenta de participante puede usar puntos de conexión de VPC de CloudTrail en subredes que se compartan

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.

## Requisitos de nomenclatura de los recursos de CloudTrail, los buckets de S3 y las claves de KMS

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](#)
- [AWS KMSRequisitos de nomenclatura para el alias de](#)

## 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 formato 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.

## AWS KMS Requisitos de nomenclatura para el alias de

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.

# Cierre de Cuenta de AWS y registros de seguimiento

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 una Cuenta de AWS. Los usuarios pueden crear un registro de seguimiento de CloudTrail para recibir una copia de estos eventos en un bucket de S3 de su propiedad.

CloudTrail es un servicio de seguridad fundamental, por lo tanto, los registros de seguimiento creados por los usuarios siguen existiendo y emitiendo eventos incluso después de cerrar una Cuenta de AWS, a menos que un usuario elimine explícitamente los registros de seguimiento en sus Cuenta de AWS antes de cerrarla. 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.

Antes de cerrar su Cuenta de AWS, tenga en cuenta lo siguiente:

- Los registros de seguimiento siguen existiendo incluso después de que haya pasado el periodo posterior al cierre. El periodo posterior al cierre se refiere a los 90 días que transcurren entre el momento en que usted cierra su cuenta y el momento en que AWS cierra su Cuenta de AWS definitivamente.
- 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 se crean en las cuentas de miembro de la organización.
- En el caso de los registros de seguimiento que envían eventos a un bucket de S3 en la misma cuenta, estos seguirán existiendo incluso después de cerrar la cuenta. Sin embargo, dado que el bucket de S3 se elimina cuando se cierra la cuenta, los registros de seguimiento no siguen publicando eventos.
- En el caso de los registros de seguimiento que envían eventos a un bucket de S3 en una cuenta diferente, estos seguirán existiendo incluso después de cerrar la cuenta. Los registros de seguimiento también siguen enviando eventos al bucket de S3 si es posible entregarlos. Por ejemplo, si cierra la cuenta de miembro de una organización, pero no cierra la cuenta de administración, los eventos se siguen distribuyendo al bucket de S3.
- En el caso de los registros de seguimiento cifrados con AWS KMS keys, seguirán existiendo después de cerrar la cuenta, además de las claves de KMS.

Los usuarios tienen la opción de eliminar los registros de seguimiento antes de cerrar sus Cuenta de AWS o ponerse en contacto con [AWS Support](#) para solicitar la eliminación del registro de seguimiento antes de cerrar sus Cuenta de AWS.

Para obtener información sobre cómo cerrar un Cuenta de AWS, consulte [Cerrar un Cuenta de AWS](#) en la Guía de referencia de AWS Account Management.

 **Note**

Si la validación de archivos de registro de CloudTrail está habilitada, los usuarios seguirán recibiendo archivos de resumen cada hora, lo que indica si se creó algún registro de CloudTrail o no.

Los almacenes de datos de eventos de CloudTrail Lake, los canales de CloudTrail Lake para integraciones, los canales vinculados a servicios de CloudTrail y los recursos creados para los registros de seguimiento (por ejemplo, los grupos de registros de Amazon CloudWatch y los buckets de Amazon S3 existentes en la cuenta cerrada) siguen el comportamiento estándar de AWS para el cierre de la cuenta y se eliminan permanentemente tras el periodo posterior al cierre (normalmente 90 días).



# Configuración de los ajustes de CloudTrail

Puede usar la página Configuración de la consola de CloudTrail para configurar y revisar la configuración de CloudTrail, como administrar los administradores delegados de una organización de AWS Organizations y ver los canales vinculados a servicios creados para su cuenta.

Para acceder a la página Configuración

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. Elija Settings (Configuración) en el panel de navegación izquierdo de la consola de CloudTrail.
3. Revise y actualice la configuración según sea necesario.

Está disponible la siguiente configuración:

- [Administradores delegados de la organización](#): si tiene una organización de AWS Organizations, puede ver los administradores delegados de CloudTrail, agregar más (hasta tres como máximo) y eliminarlos. Solo la cuenta de administración de la organización puede agregar o eliminar administradores delegados.

La cuenta de administración de la organización puede asignar cualquier cuenta de la organización para que actúe como administrador delegado de CloudTrail y gestione los registros de seguimiento y los almacenes de datos de eventos de la organización en su nombre.

- [Visualización de canales vinculados a servicios](#): puede ver cualquier canal vinculado a servicios creado para su cuenta.

Los Servicios de AWS pueden crear un canal vinculado a servicios para recibir eventos de CloudTrail 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 de AWS o a una sola Región de AWS.

## Administrador delegado de la organización

Cuando se utiliza CloudTrail con una organización de AWS Organizations, se puede asignar cualquier cuenta de la organización para que actúe como administrador delegado de CloudTrail y gestione los registros de seguimiento y los almacenes de datos de eventos de la organización en su

nombre. Un administrador delegado es una cuenta miembro de una organización que puede hacer las mismas tareas administrativas (salvo en los [casos indicados](#)) en CloudTrail que la cuenta de administración.

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 agregue un administrador delegado en la consola de CloudTrail o mediante la AWS CLI o la API de CloudTrail, CloudTrail comprobará si la cuenta de administración de la organización tiene un rol vinculado al servicio. Si la cuenta de administración no tiene un rol vinculado al servicio, CloudTrail creará dicho rol para la cuenta de administración. Para obtener más información acerca de los roles vinculados a servicios, consulte [Uso de roles vinculados a servicios para CloudTrail](#).

 Note

Al agregar un administrador delegado mediante la CLI de AWS Organizations o la operación de la API, los roles vinculados al servicio de CloudTrail no se crean de manera automática si no existen. Los roles vinculados al servicio solo se crean al realizar una llamada desde la cuenta de administración directamente al servicio de CloudTrail. Por ejemplo, cuando agrega un administrador delegado o crear un registro de seguimiento de la organización o un almacén de datos de eventos con la consola de CloudTrail, AWS CLI o la API de CloudTrail, se crea el rol vinculado al servicio de `AWSServiceRoleForCloudTrail`.

Al agregar un administrador delegado mediante la AWS CloudTrail, operación de CLI o API, CloudTrail crea los roles vinculados al servicio de `AWSServiceRoleForCloudTrail` y `AWSServiceRoleForCloudTrailEventContext`. Para obtener más información, consulte [Uso de roles vinculados a servicios para CloudTrail](#).

Tome nota de los siguientes factores que definen cómo funciona el administrador delegado en CloudTrail.

La cuenta de administración seguirá siendo la propietaria de todos los recursos de la organización que cree el administrador delegado en CloudTrail.

La cuenta de administración seguirá siendo la propietaria de todos los recursos de la organización que cree el administrador delegado en CloudTrail, como los registros de

seguimiento y los almacenes de datos de eventos. Esto proporciona continuidad a la organización en el caso de que el administrador delegado cambie.

La eliminación de una cuenta de administrador delegado no elimina ningún recurso de la organización en CloudTrail creado por aquella.

Los registros de seguimiento y los almacenes de datos de eventos de la organización creados por el administrador delegado no se eliminan cuando se elimina al administrador delegado, ya que la cuenta de administración siempre es la propietaria de los recursos de la organización en CloudTrail, independientemente de si los creó el administrador delegado o la cuenta de administración.

Una organización puede tener un máximo de tres administradores delegados de CloudTrail.

Se puede tener un máximo de tres administradores delegados de CloudTrail por organización. Para obtener más información acerca de cómo eliminar un administrador delegado, consulte [Cómo eliminar un administrador delegado de CloudTrail](#).

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 organización de AWS Organizations.

| 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 <sup>1</sup>                  | 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 <sup>1, 2</sup>               | No                  |
| Eliminar un registro de seguimiento de la organización.           | Sí                       | Sí                               | No                  |

| Capacidades                                                                                                                    | Cuenta de administración | Cuenta de administrador delegado | Cuentas de miembros |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------|---------------------|
| Crear un almacén de datos de eventos de la organización para eventos de CloudTrail o elementos de configuración de AWS Config. | 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 <sup>2</sup>                  | No                  |
| Iniciar o detener la ingesta de eventos en un almacén de datos de eventos de la organización.                                  | Sí                       | Sí                               | No                  |
| Habilitar la federación de consultas de Lake en un almacén de datos de eventos de la organización <sup>3</sup> .               | 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                  |

| Capacidades                                                                                                 | Cuenta de administración | Cuenta de administrador delegado | Cuentas de miembros |
|-------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------|---------------------|
| Consultar el panel administrado de un almacén de datos de eventos de la organización.                       | Sí                       | No                               | No                  |
| Habilitar el panel de aspectos destacados para los almacenes de datos de eventos de la organización.        | Sí                       | No                               | No                  |
| Crear un widget para un panel personalizado que consulte un almacén de datos de eventos de la organización. | Sí                       | No                               | No                  |

<sup>1</sup> El administrador delegado solo puede configurar un grupo de registros de CloudWatch Logs mediante la AWS CLI o las operaciones `CreateTrail` o `UpdateTrail` de la API de CloudTrail. Tanto el grupo de registro de CloudWatch como el rol de registro deben existir en la cuenta de llamada.

<sup>2</sup> Solo la cuenta de administración puede convertir un registro de seguimiento o almacén de datos de eventos de la organización en un registro de seguimiento o almacén de datos de eventos a nivel de cuenta, o convertir un registro de seguimiento o almacén de datos de eventos a nivel de cuenta en un registro de seguimiento o almacén de datos de 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 registro de seguimiento o almacén de datos de eventos de la organización se convierte en un registro de seguimiento o almacén de datos de eventos a nivel de cuenta, solo la cuenta de administración tiene acceso al registro de seguimiento o almacén de datos de eventos.

<sup>3</sup> 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](#)
- [Cómo agregar un administrador delegado de CloudTrail](#)
- [Cómo eliminar un administrador delegado de CloudTrail](#)

## Permisos necesarios para designar un administrador delegado

Cuando se asigna un administrador delegado de CloudTrail, se requieren permisos para agregar al administrador delegado a CloudTrail y eliminarlo de dicho servicio, así como para realizar determinadas acciones de la API de AWS Organizations, y los permisos de IAM que se enumeran en la siguiente instrucción 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": "*"
}
```

## Consideraciones a la hora de utilizar las claves de condición con las instrucciones de la política para los permisos del administrador delegado

Podría considerar la posibilidad de utilizar las claves de condición global de IAM al agregar las instrucciones de las políticas con el fin de agregar y eliminar el administrador delegado en CloudTrail para mayor seguridad. Al hacerlo, recuerde incluir ambos nombres de las entidades principales de servicio (SPN) en la condición. Por ejemplo:

```
{
```

```
"Condition": {
  "StringLike": {
    "iam:AWSServiceName": [
      "context.cloudtrail.amazonaws.com",
      "cloudtrail.amazonaws.com"
    ]
  }
},
"Action": "iam:CreateServiceLinkedRole",
"Resource": "*",
"Effect": "Allow"
}
```

Para obtener más información, consulte [Administración de identidades y accesos para AWS CloudTrail](#).

## Cómo agregar un administrador delegado de CloudTrail

Puede agregar un administrador delegado para que administre los recursos de CloudTrail de una organización, como, por ejemplo, los registros de seguimiento y los almacenes de datos de eventos.

Puede agregar un administrador delegado de CloudTrail para su organización de AWS mediante la consola de CloudTrail o la 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 acerca de cómo crear una nueva cuenta de AWS para su organización, consulte [Creación de una cuenta de AWS en su organización](#). Para obtener información acerca de cómo invitar a una cuenta de AWS existente a su organización, consulte [Invitar a una cuenta de AWS a unirse a su organización](#).

### CloudTrail console

En el siguiente procedimiento, se muestra cómo agregar un administrador delegado de CloudTrail a través de la consola de este servicio.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. Elija Settings (Configuración) en el panel de navegación izquierdo de la consola de CloudTrail.

3. En la sección Organization delegated administrators (Administradores delegados de la organización), seleccione Register administrator (Registrar administrador).
4. Escriba el ID de 12 dígitos de la cuenta de AWS que desea designar como administrador delegado de CloudTrail para los registros de seguimiento y los almacenes de datos de eventos de la organización.
5. Elija Register administrator (Registrar administrador).

## AWS CLI

En el siguiente ejemplo, se agrega un administrador delegado de CloudTrail.

```
aws cloudtrail register-organization-delegated-admin  
--member-account-id="memberAccountId"
```

Este comando no genera ningún resultado si se utiliza correctamente.

## Cómo eliminar un administrador delegado de CloudTrail

Puede eliminar un administrador delegado de CloudTrail mediante la consola de CloudTrail o la AWS CLI.

### CloudTrail console

En el siguiente procedimiento, se muestra cómo eliminar un administrador delegado de CloudTrail a través de la consola de este servicio.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. Elija Settings (Configuración) en el panel de navegación izquierdo de la consola de CloudTrail.
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 delegado de CloudTrail.

```
aws cloudtrail deregister-organization-delegated-admin  
--delegated-admin-account-id="delegatedAdminAccountId"
```

Este comando no genera ningún resultado si se utiliza correctamente.

## Visualización de canales vinculados a servicios

Los servicios de AWS pueden crear un canal vinculado a servicios para recibir eventos de CloudTrail 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 de AWS o a una sola 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

Con la consola de CloudTrail, puede ver la información sobre cualquier canal vinculado a servicios de CloudTrail creado por los servicios de 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. Elija Settings (Configuración) en el panel de navegación izquierdo de la consola de CloudTrail.
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"
}
```

# Descripción de los eventos de CloudTrail

Un evento en CloudTrail es el registro de una actividad en una cuenta de AWS. Esta actividad puede ser una acción de una identidad de IAM o un servicio que CloudTrail puede supervisar. Los eventos de CloudTrail proporcionan un historial de las actividades de la cuenta, tanto de la API como no de esta, que se realizan a través de la Consola de administración de AWS, los SDK de AWS, las herramientas de línea de comando y otros Servicios de AWS.

Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas a la API públicas, por lo que los eventos no aparecen en un orden específico.

Hay cuatro tipos de eventos de CloudTrail:

- [Eventos de administración](#)
- [Eventos de datos](#)
- [Eventos de actividad de la red](#)
- [Eventos de 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, de actividad de la red o de Insights.

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

Para obtener más información acerca de los campos de registros de eventos de CloudTrail para los eventos de administración, de datos y de actividad de la red, consulte [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

Para obtener más información acerca de los campos de registros de eventos de CloudTrail para los eventos de Insights a fin del registro de seguimiento, consulte [CloudTrail registra el contenido de los eventos de Insights para registros de seguimiento](#).

Para obtener más información acerca de los campos de registros de eventos de CloudTrail para los eventos de Insights a fin de los eventos de datos de eventos, consulte [CloudTrail registra el contenido de los eventos de Insights para los almacenes de datos de eventos](#).

# Eventos de administración

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su 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 AWS Identity and Access Management de `AttachRolePolicy`).
- 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 AWS CloudTrail de `CreateTrail`).

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](#).

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos de CloudTrail Lake registran los eventos de administración. Para obtener más información sobre el registro de eventos de administración, consulte [Registro de eventos de administración](#).

En el siguiente ejemplo, se muestra un registro único de un evento de administración. 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"
}
```

# 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 el nivel de objeto de Amazon S3](#) (por ejemplo, las operaciones `GetObject`, `DeleteObject` y `PutObject` de la API) en objetos de los buckets de S3.
- Actividad de ejecución de funciones de AWS Lambda (la API `Invoke`).
- La actividad de [PutAuditEvents](#) de CloudTrail en un [canal de CloudTrail Lake](#) que se utiliza para registrar eventos externos a AWS.
- Operaciones de la API [Publish](#) y [PublishBatch](#) de Amazon SNS sobre temas.

En la siguiente tabla, se muestran los tipos de recursos disponibles para los registros de seguimiento y los almacenes de datos de eventos. En la columna Tipo de recurso (consola), se muestra la selección adecuada en la consola. En la columna `resources.type value`, se muestra el valor de `resources.type` que debe especificar para incluir eventos de datos de ese tipo en el registro de seguimiento o el almacén de datos de eventos por medio de la AWS CLI o las API de CloudTrail.

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

## Eventos de datos compatibles con AWS CloudTrail

| Servicio de AWS | Descripción                                                                                                                                                                                                                           | Tipo de recurso (consola)                     | resources.type value   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|------------------------|
| Amazon RDS      | <a href="#">Actividad de la API de Amazon RDS</a> en un clúster de base de datos.                                                                                                                                                     | API de datos de RDS: clúster de base de datos | AWS::RDS::DBCluster    |
| Amazon S3       | <a href="#">Actividad de la API en el nivel de objeto de Amazon S3</a> (por ejemplo, las operaciones <code>GetObject</code> , <code>DeleteObject</code> y <code>PutObject</code> de la API) en objetos de los buckets de uso general. | S3                                            | AWS::S3::Object        |
| Amazon S3       | <a href="#">Actividad de la API de Amazon S3</a> en los puntos de acceso.                                                                                                                                                             | Punto de acceso de S                          | AWS::S3::AccessPoint   |
| Amazon S3       | <a href="#">Actividad de la API en el nivel de objeto de Amazon S3</a> (por ejemplo, las operaciones <code>GetObject</code> , <code>DeleteObject</code> y <code>PutObject</code> de la                                                | S3 Express                                    | AWS::S3Express::Object |

| Servicio de AWS     | Descripción                                                                                                                                        | Tipo de recurso (consola) | resources.type value             |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------------------|
|                     | API) en objetos de los buckets de directorio.                                                                                                      |                           |                                  |
| Amazon S3           | <a href="#">Actividad de la API en los puntos de acceso de Amazon S3 Object Lambda</a> , como las llamadas a CompleteMultipartUpload y GetObject . | S3 Object Lambda          | AWS::S3ObjectLambda::AccessPoint |
| Amazon S3           | Actividad de la API de Amazon FSx en volúmenes.                                                                                                    | Volumen de FSx            | AWS::FSx::Volume                 |
| Tablas de Amazon S3 | Actividad de la API de Amazon S3 en las <a href="#">tablas</a> .                                                                                   | Tabla de S3               | AWS::S3Tables::Table             |
| Tablas de Amazon S3 | Actividad de la API de Amazon S3 en los <a href="#">buckets de las tablas</a> .                                                                    | Bucket de tablas de S3    | AWS::S3Tables::TableBucket       |
| Amazon S3 Vectors   | Actividad de la API de Amazon S3 en los <a href="#">buckets de vectores</a> .                                                                      | Bucket de vector S3       | AWS::S3Vectors::VectorBucket     |
| Amazon S3 Vectors   | Actividad de la API de Amazon S3 en <a href="#">índices de vectores</a> .                                                                          | Índice de vector S3       | AWS::S3Vectors::Index            |

| Servicio de AWS       | Descripción                                                                                             | Tipo de recurso (consola)                 | resources.type value       |
|-----------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------|
| Amazon S3 en Outposts | <a href="#">Actividad de la API en cuanto a objetos de Amazon S3 en Outposts.</a>                       | S3 Outposts                               | AWS::S3Outposts::Object    |
| Amazon SNS            | Operaciones de la API <a href="#">Publish</a> de Amazon SNS en los puntos de conexión de la plataforma. | Punto de conexión de la plataforma de SNS | AWS::SNS::PlatformEndpoint |
| Amazon SNS            | Operaciones de la API <a href="#">Publish</a> y <a href="#">PublishBatch</a> de Amazon SNS sobre temas. | Tema de SNS                               | AWS::SNS::Topic            |
| Amazon SQS            | <a href="#">Actividad de la API de Amazon SQS</a> en los mensajes.                                      | SQS                                       | AWS::SQS::Queue            |
| AWS Supply Chain      | Actividad de la API de AWS Supply Chain en una instancia.                                               | Supply Chain                              | AWS::SCN::Instance         |
| Amazon SWF            | <a href="#">Actividad de la API de Amazon SWF</a> en los dominios.                                      | Dominio de SWF                            | AWS::SWF::Domain           |

| Servicio de AWS                 | Descripción                                                                                                                                                                                | Tipo de recurso (consola)           | resources.type value                       |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|--------------------------------------------|
| AWS AppConfig                   | <a href="#">Actividad de la API de AWS AppConfig</a> para operaciones de configuración, como las llamadas a <code>StartConfigurationSession</code> y <code>GetLatestConfiguration</code> . | AWS AppConfig                       | <code>AWS::AppConfig::Configuration</code> |
| AWS AppSync                     | <a href="#">Actividad de la API de AWS AppSync</a> en las API GraphQL de AppSync.                                                                                                          | AppSync Graph                       | <code>AWS::AppSync::GraphQLApi</code>      |
| Amazon Aurora DSQL              | Actividad de la API de Amazon Aurora DSQL en los recursos del clúster.                                                                                                                     | Amazon Aurora DSQL                  | <code>AWS::DSQL::Cluster</code>            |
| Intercambio de datos B2B de AWS | Actividad de la API de intercambio de datos entre empresas para operaciones de Transformer, como las llamadas a <code>GetTransformerJob</code> y <code>StartTransformerJob</code> .        | Intercambio de datos entre empresas | <code>AWS::B2BI::Transformer</code>        |

| Servicio de AWS | Descripción                                                                         | Tipo de recurso (consola)              | resources.type value        |
|-----------------|-------------------------------------------------------------------------------------|----------------------------------------|-----------------------------|
| AWS Backup      | Actividad de la API de datos de búsqueda de AWS Backup en trabajos de búsqueda.     | API de datos de búsqueda de AWS Backup | AWS::Backup::SearchJob      |
| Amazon Bedrock  | <a href="#">Actividad de la API de Amazon Bedrock</a> en un alias de agente.        | Alias de agente de Bedrock             | AWS::Bedrock::AgentAlias    |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en invocaciones asíncronas.                   | Invocación asíncrona de Bedrock        | AWS::Bedrock::AsyncInvoke   |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en un alias de flujo.                         | Alias de flujo de Bedrock              | AWS::Bedrock::FlowAlias     |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en barreras de protección.                    | Barrera de protección de Bedrock       | AWS::Bedrock::Guardrail     |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en un agente insertado                        | Agente insertado e invocado en Bedrock | AWS::Bedrock::InlineAgent   |
| Amazon Bedrock  | <a href="#">Actividad de la API de Amazon Bedrock</a> en una base de conocimientos. | Base de conocimientos de Bedrock       | AWS::Bedrock::KnowledgeBase |

| Servicio de AWS | Descripción                                                                                       | Tipo de recurso (consola)                                      | resources.type value                          |
|-----------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------|
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en modelos.                                                 | Modelo de Bedrock                                              | AWS::Bedrock::Model                           |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en peticiones.                                              | Petición de Bedrock                                            | AWS::Bedrock::PromptVersion                   |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en sesiones.                                                | Sesión de Bedrock                                              | AWS::Bedrock::Session                         |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en ejecuciones de flujo.                                    | Ejecución de flujo de Bedrock                                  | AWS::Bedrock::FlowExecution                   |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en una política de razonamiento automatizado.               | Política de razonamiento automatizado de Bedrock               | AWS::Bedrock::AutomatedReasoningPolicy        |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en una versión de la política de razonamiento automatizado. | Versión de la política de razonamiento automatizado de Bedrock | AWS::Bedrock::AutomatedReasoningPolicyVersion |
| Amazon Bedrock  | Actividad de la API del proyecto de automatización de datos de Amazon Bedrock.                    | Proyectos de automatización de datos de Bedrock                | AWS::Bedrock::DataAutomationProject           |



| Servicio de AWS | Descripción                                                                  | Tipo de recurso (consola)                             | resources.type value                    |
|-----------------|------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------|
| Amazon Bedrock  | Actividad de la API de invocación de automatización de datos de Bedrock.     | Invocación de automatización de datos de Bedrock      | AWS::Bedrock::DataAutomationInvocation  |
| Amazon Bedrock  | Actividad de la API del perfil de automatización de datos de Amazon Bedrock. | Perfil de automatización de datos de Bedrock          | AWS::Bedrock::DataAutomationProfile     |
| Amazon Bedrock  | Actividad de la API del esquema de Amazon Bedrock.                           | Esquema de Bedrock                                    | AWS::Bedrock::Blueprint                 |
| Amazon Bedrock  | Actividad de la API de intérprete de código de Amazon Bedrock.               | Intérprete de código AgentCore de Bedrock             | AWS::BedrockAgentCore::CodeInterpreter  |
| Amazon Bedrock  | Actividad de la API del navegador Amazon Bedrock.                            | Navegador AgentCore de Bedrock                        | AWS::BedrockAgentCore::Browser          |
| Amazon Bedrock  | Actividad de la API de identidad de carga de trabajo de Amazon Bedrock.      | Identidad de carga de trabajo de AgentCore de Bedrock | AWS::BedrockAgentCore::WorkloadIdentity |

| Servicio de AWS | Descripción                                                                            | Tipo de recurso (consola)                                           | resources.type value                             |
|-----------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------|
| Amazon Bedrock  | Actividad de la API del directorio de identidad de carga de trabajo de Amazon Bedrock. | Directorio de identidad de carga de trabajo de AgentCore de Bedrock | AWS::BedrockAgentCore::WorkloadIdentityDirectory |
| Amazon Bedrock  | Actividad de la API de bóveda de token de Amazon Bedrock .                             | Bóveda de token de AgentCore de Bedrock                             | AWS::BedrockAgentCore::TokenVault                |
| Amazon Bedrock  | Actividad de la API de CredentialProvider de APIKey de Amazon Bedrock.                 | Credentia IProvider de APIKey de AgentCore de Bedrock               | AWS::BedrockAgentCore::APIKeyCredentialProvider  |
| Amazon Bedrock  | Actividad de la API de tiempo de ejecución de Amazon Bedrock.                          | Tiempo de ejecución de AgentCore de Bedrock                         | AWS::BedrockAgentCore::Runtime                   |
| Amazon Bedrock  | Actividad de la API del tiempo de ejecución del punto de conexión de Amazon Bedrock.   | Tiempo de ejecución de AgentCore del punto de conexión de Bedrock   | AWS::BedrockAgentCore::RuntimeEndpoint           |
| Amazon Bedrock  | Actividad de la API de la puerta de enlace de Amazon Bedrock.                          | Puerta de enlace AgentCore de Bedrock                               | AWS::BedrockAgentCore::Gateway                   |

| Servicio de AWS | Descripción                                                                  | Tipo de recurso (consola)                               | resources.type value                            |
|-----------------|------------------------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------|
| Amazon Bedrock  | Actividad de la API de memoria de Amazon Bedrock.                            | Memoria de AgentCore de Bedrock                         | AWS::BedrockAgentCore::Memory                   |
| Amazon Bedrock  | Actividad de la API de CredentialProvider de Oauth2 de Amazon Bedrock.       | Credentia IProvider de Oauth2 de AgentCore de Bedrock   | AWS::BedrockAgentCore::OAuth2CredentialProvider |
| Amazon Bedrock  | Actividad de API personalizada del navegador Amazon Bedrock.                 | Navegador AgentCore personalizado de Bedrock            | AWS::BedrockAgentCore::BrowserCustom            |
| Amazon Bedrock  | Actividad de la API de intérprete de código personalizado de Amazon Bedrock. | Intérprete de código AgentCore personalizado de Bedrock | AWS::BedrockAgentCore::CodeInterpreterCustom    |
| Amazon Bedrock  | Actividad de la API de la herramienta de Amazon Bedrock.                     | Herramienta de Bedrock                                  | AWS::Bedrock::Tool                              |
| AWS Cloud Map   | <a href="#">Actividad AWS Cloud Map de la API en un espacio de nombres.</a>  | AWS Cloud Map Espacio de nombres de                     | AWS::ServiceDiscovery::Namespace                |

| Servicio de AWS                              | Descripción                                                                                                                                                       | Tipo de recurso (consola)                      | resources.type value             |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------|
| AWS Cloud Map                                | <a href="#">Actividad AWS Cloud Map de la API en un servicio.</a>                                                                                                 | AWS Cloud Map Servicio de                      | AWS::ServiceDiscovery::Service   |
| Amazon CloudFront                            | Actividad de la API de CloudFront en un <a href="#">KeyValueStore</a> .                                                                                           | CloudFront KeyValueStore                       | AWS::CloudFront::KeyValueStore   |
| AWS CloudTrail                               | La actividad de <a href="#">PutAuditEvents</a> de CloudTrail en un <a href="#">canal de CloudTrail Lake</a> que se utiliza para registrar eventos externos a AWS. | Canal de CloudTrail                            | AWS::CloudTrail::Channel         |
| Amazon CloudWatch                            | <a href="#">Actividad de la API de Amazon CloudWatch en las métricas.</a>                                                                                         | Métrica de CloudWatch                          | AWS::CloudWatch::Metric          |
| Monitor de flujo de red de Amazon CloudWatch | Actividad de la API del monitor de flujo de red de Amazon CloudWatch en los monitores.                                                                            | Monitor de flujo de red                        | AWS::NetworkFlowMonitor::Monitor |
| Monitor de flujo de red de Amazon CloudWatch | Actividad de la API del monitor de flujo de red de Amazon CloudWatch en el alcance.                                                                               | Agente del monitor de flujo de red del alcance | AWS::NetworkFlowMonitor::Scope   |

| Servicio de AWS                          | Descripción                                                                                           | Tipo de recurso (consola)        | resources.type value                  |
|------------------------------------------|-------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------|
| Amazon CloudWatch RUM                    | Actividad de la API de Amazon CloudWatch RUM en los monitores de aplicaciones.                        | Monitor de aplicaciones de RUM   | AWS::RUM::AppMonitor                  |
| Generador de perfiles de Amazon CodeGuru | Actividad de la API de perfiles de CodeGuru en grupos de creación de perfiles.                        | Grupo de perfiles de CodeGuru    | AWS::CodeGuruProfiler::ProfilingGroup |
| Amazon CodeWhisperer                     | Actividad de la API de Amazon CodeWhisperer en una personalización.                                   | Personalización de CodeWhisperer | AWS::CodeWhisperer::Customization     |
| Amazon CodeWhisperer                     | Actividad de la API de Amazon CodeWhisperer en un perfil.                                             | CodeWhisperer                    | AWS::CodeWhisperer::Profile           |
| Amazon Cognito                           | Actividad de la API de Amazon Cognito en los <a href="#">grupos de identidades</a> de Amazon Cognito. | Grupos de identidades de Cognito | AWS::Cognito::IdentityPool            |
| AWS Data Exchange                        | Actividad de la API de AWS Data Exchange en los activos.                                              | Activo de Data Exchange          | AWS::DataExchange::Asset              |
| Amazon Data Firehose                     | Actividad de la API del flujo de entrega de Amazon Data Firehose                                      | Amazon Data Firehose             | AWS::KinesisFirehose::DeliveryStream  |

| Servicio de AWS    | Descripción                                                                   | Tipo de recurso (consola)    | resources.type value  |
|--------------------|-------------------------------------------------------------------------------|------------------------------|-----------------------|
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en las flotas.       | Deadline Cloud Flota de      | AWS::Deadline::Fleet  |
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en los trabajos.     | Deadline Cloud Trabajo de    | AWS::Deadline::Job    |
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en las colas.        | Deadline Cloud Cola de       | AWS::Deadline::Queue  |
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en los trabajadores. | Deadline Cloud Trabajador de | AWS::Deadline::Worker |

| Servicio de AWS | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Tipo de recurso (consola) | resources.type value |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------|
| Amazon DynamoDB | <p><a href="#">Actividad de la API en el nivel de elemento de Amazon DynamoDB</a> en las tablas (por ejemplo, las operaciones PutItem, DeleteItem y UpdateItem de la API).</p> <div>  <p>Note</p> <p>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 ,</p> </div> | DynamoDB                  | AWS::DynamoDB::Table |

| Servicio de AWS | Descripción                                                                                                                                                                                                           | Tipo de recurso (consola) | resources.type value  |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------------|
|                 | <div>registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir <a href="#">eventos de flujos</a>, agregue un filtro en el campo eventName .</div> |                           |                       |
| Amazon DynamoDB | Actividad de la API de <a href="#">Amazon DynamoDB</a> en los flujos.                                                                                                                                                 | DynamoDB Streams          | AWS::DynamoDB::Stream |



| Servicio de AWS                   | Descripción                                                                                                                                                   | Tipo de recurso (consola)                    | resources.type value              |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------|
| Amazon Elastic Block Store        | API directas de <a href="#">Amazon Elastic Block Store (EBS)</a> , como PutSnapshotBlock, GetSnapshotBlock y ListChangedBlocks en instantáneas de Amazon EBS. | API directas de Amazon EBS                   | AWS::EC2::Snapshot                |
| Amazon Elastic Compute Cloud      | Actividad de la API del punto de conexión de Amazon EC2 Instance Connect                                                                                      | Punto de conexión a EC2 Instance Connect     | AWS::EC2::InstanceConnectEndpoint |
| Amazon Elastic Container Service  | Actividad de la API de Amazon Elastic Container en una instancia de contenedor.                                                                               | Instancia de contenedor de ECS               | AWS::ECS::ContainerInstance       |
| Amazon Elastic Kubernetes Service | Actividad de la API de Amazon Elastic Kubernetes Service en los paneles.                                                                                      | Paneles de Amazon Elastic Kubernetes Service | AWS::EKS::Dashboard               |

| Servicio de AWS                                         | Descripción                                                                                                                      | Tipo de recurso (consola)                                     | resources.type value                |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------|
| Amazon EMR                                              | <a href="#">Actividad de la API de Amazon EMR</a> en un espacio de trabajo de registros de escritura anticipada.                 | Espacio de trabajo de registro de escritura anticipada de EMR | AWS::EMRWAL::Workspace              |
| Mensajes SMS para usuarios finales de AWS               | Actividad de la API de <a href="#">Mensajes SMS para usuarios finales de AWS</a> en las identidades de origen.                   | Identidad de origen de SMS Voice                              | AWS::SMSVoice::OriginationIdentity  |
| Mensajes SMS para usuarios finales de AWS               | Actividad de la API de <a href="#">mensajes SMS para usuarios finales de AWS</a> en los mensajes.                                | Mensaje de voz de SMS                                         | AWS::SMSVoice::Message              |
| Mensajes de redes sociales para usuarios finales de AWS | Actividad de la API de <a href="#">Mensajes de redes sociales para usuarios finales de AWS</a> en los ID de números de teléfono. | ID de número de teléfono de mensajes de redes sociales        | AWS::SocialMessaging::PhoneNumberId |
| Mensajes de redes sociales para usuarios finales de AWS | Actividad de la API de Mensajes de redes sociales de AWS para usuarios finales de en los ID de Waba.                             | ID de Waba ID de mensajes de redes sociales                   | AWS::SocialMessaging::WabaId        |

| Servicio de AWS         | Descripción                                                                                                 | Tipo de recurso (consola)                  | resources.type value              |
|-------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------|
| Amazon FinSpace         | <a href="#">Amazon FinSpace</a><br>Actividad de la API de entornos.                                         | FinSpace                                   | AWS::FinSpace::Environment        |
| Amazon GameLift Streams | <a href="#">Actividad de la API de transmisión</a> de Amazon GameLift Streams en las aplicaciones.          | Aplicación de GameLift Streams             | AWS::GameLiftStreams::Application |
| Amazon GameLift Streams | <a href="#">Actividad de la API de transmisión</a> de Amazon GameLift Streams en los grupos de transmisión. | Grupo de transmisiones de GameLift Streams | AWS::GameLiftStreams::StreamGroup |
| AWS Glue                | Actividad de la API de AWS Glue en tablas creadas por Lake Formation.                                       | Lake Formation                             | AWS::Glue::Table                  |
| Amazon GuardDuty        | Actividad de la API de Amazon GuardDuty para un <a href="#">detector</a> .                                  | Detector de GuardDuty                      | AWS::GuardDuty::Detector          |
| AWS HealthImaging       | Actividad de la API de AWS HealthImaging en los almacenes de datos.                                         | Almacén de datos de MedicalImaging         | AWS::MedicalImaging::Datastore    |

| Servicio de AWS              | Descripción                                                                                                                                                                                                                                                                                    | Tipo de recurso (consola)              | resources.type value                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------|
| AWS HealthImaging            | Actividad de la API del conjunto de imágenes de AWS HealthImaging.                                                                                                                                                                                                                             | Conjunto de imágenes de MedicalImaging | AWS::MedicalImaging::Imageset       |
| AWS IoT                      | <a href="#">Actividad de la API de AWS IoT en los certificados.</a>                                                                                                                                                                                                                            | Certificado IoT                        | AWS::IoT::Certificate               |
| AWS IoT                      | <a href="#">Actividad de la API de AWS IoT en los objetos.</a>                                                                                                                                                                                                                                 | Objeto de IoT                          | AWS::IoT::Thing                     |
| AWS IoT Greengrass Version 2 | <a href="#">Actividad de la API de Greengrass</a> desde un dispositivo principal de Greengrass en una versión del componente. <div>  Note<br/>Greengrass no registra los eventos de acceso denegado. </div> | Versión del componente IoT Greengrass  | AWS::GreengrassV2::ComponentVersion |

| Servicio de AWS              | Descripción                                                                                                                                                                                                                                                                                 | Tipo de recurso (consola)        | resources.type value                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|--------------------------------------|
| AWS IoT Greengrass Version 2 | <p><a href="#">Actividad de la API de Greengrass</a> desde un dispositivo principal de Greengrass en una implementación.</p> <div>  Note<br/>Greengrass no registra los eventos de acceso denegado. </div> | Implementación de IoT Greengrass | AWS::GreengrassV2::Deployment        |
| AWS IoT SiteWise             | <a href="#">Actividad de la API de IoT SiteWise</a> en los activos.                                                                                                                                                                                                                         | Activo de IoT SiteWise           | AWS::IoTSiteWise::Asset              |
| AWS IoT SiteWise             | <a href="#">Actividad de la API de IoT SiteWise</a> en las series temporales.                                                                                                                                                                                                               | Serie temporal de IoT SiteWise   | AWS::IoTSiteWise::TimeSeries         |
| AWS IoT SiteWiseAssistant    | Actividad de la API de Sitewise Assistant en las conversaciones.                                                                                                                                                                                                                            | Conversación con Sitewise Assist | AWS::SitewiseAssistant::Conversation |
| AWS IoT TwinMaker            | Actividad de la API de IoT TwinMaker en una <a href="#">entidad</a> .                                                                                                                                                                                                                       | Entidad de IoT TwinMaker         | AWS::IoTTwinMaker::Entity            |

| Servicio de AWS                         | Descripción                                                                                                                  | Tipo de recurso (consola)           | resources.type value                |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| AWS IoT TwinMaker                       | Actividad de la API de IoT TwinMaker en un <a href="#">espacio de trabajo</a> .                                              | Espacio de trabajo de IoT TwinMaker | AWS::IoT::TwinMaker::Workspace      |
| Amazon Kendra Intelligent Ranking       | Actividad de la API de Amazon Kendra Intelligent Ranking en los <a href="#">planes de ejecución de nuevas puntuaciones</a> . | Kendra Ranking                      | AWS::Kendra::Ranking::ExecutionPlan |
| Amazon Keyspaces (for Apache Cassandra) | <a href="#">Actividad de la API de Amazon Keyspaces</a> en una tabla.                                                        | Tabla de Cassandra                  | AWS::Cassandra::Table               |
| Amazon Keyspaces (for Apache Cassandra) | Actividad de la API de Amazon Keyspaces (para Apache Cassandra) en transmisiones de Cassandra CDC.                           | Transmisiones de Cassandra CDC      | AWS::Cassandra::Stream              |
| Amazon Kinesis Data Streams             | Actividad de la API de Kinesis Data Streams en los <a href="#">flujos</a> .                                                  | Flujo de Kinesis                    | AWS::Kinesis::Stream                |
| Amazon Kinesis Data Streams             | Actividad de la API de Kinesis Data Streams en los <a href="#">consumidores de flujos</a> .                                  | Consumidor de flujos de Kinesis     | AWS::Kinesis::StreamConsumer        |

| Servicio de AWS              | Descripción                                                                                                  | Tipo de recurso (consola)                 | resources.type value                |
|------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------|
| Amazon Kinesis Video Streams | Actividad de la API de Kinesis Video Streams en transmisiones de video, como llamadas a GetMedia y PutMedia. | Kinesis Video Streams                     | AWS::KinesisVideo::Stream           |
| Amazon Kinesis Video Streams | Actividad de la API del canal de señalización de video de Kinesis Video Streams.                             | Canal de señalización de video de Kinesis | AWS::KinesisVideo::SignalingChannel |
| AWS Lambda                   | Actividad de ejecución de funciones de AWS Lambda (la API Invoke).                                           | Lambda                                    | AWS::Lambda::Function               |
| Mapas de Amazon Location     | Actividad de la API de mapas de Amazon Location                                                              | Mapas geográficos                         | AWS::GeoMaps::Provider              |
| Amazon Location Places       | Actividad de la API de Amazon Location Places.                                                               | Lugares geográficos                       | AWS::GeoPlaces::Provider            |
| Rutas de Amazon Location     | Actividad de la API de rutas de Amazon Location                                                              | Rutas geográficas                         | AWS::GeoRoutes::Provider            |
| Amazon Machine Learning      | Actividad de la API de machine learning en modelos de ML.                                                    | MLModel de machine learning               | AWS::MachineLearning::MLModel       |

| Servicio de AWS                              | Descripción                                                                                                                       | Tipo de recurso (consola) | resources.type value                  |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------|
| Amazon Managed Blockchain                    | Actividad de la API de Amazon Managed Blockchain en una red.                                                                      | Red de Managed Blockchain | AWS::ManagedBlockchain::Network       |
| Amazon Managed Blockchain                    | Llamadas JSON-RPC de <a href="#">Amazon Managed Blockchain</a> en nodos de Ethereum, como eth_getBalance o eth_getBlockByNumber . | Managed Blockchain        | AWS::ManagedBlockchain::Node          |
| Amazon Managed Blockchain Query              | Actividad de la API de Amazon Managed Blockchain Query.                                                                           | Managed Blockchain Query  | AWS::ManagedBlockchainQuery::QueryAPI |
| Amazon Managed Workflows para Apache Airflow | Actividad de la API de Amazon MWAA en entornos.                                                                                   | Managed Apache Airflow    | AWS::MWAA::Environment                |
| 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              |



| Servicio de AWS          | Descripción                                                                   | Tipo de recurso (consola)                     | resources.type value             |
|--------------------------|-------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------|
| Amazon One Enterprise    | Actividad de la API de Amazon One Enterprise en una clave de usuario.         | Clave de usuario de Amazon One                | AWS::One::UKey                   |
| Amazon One Enterprise    | Actividad de la API de Amazon One Enterprise en los usuarios.                 | Usuario de Amazon One                         | AWS::One::User                   |
| AWS Payment Cryptography | Actividad de la API de AWS Payment Cryptography en los alias.                 | Alias de Payment Cryptography                 | AWS::PaymentCryptography::Alias  |
| AWS Payment Cryptography | Actividad de la API de AWS Payment Cryptography en las claves.                | Clave de Payment Cryptography                 | AWS::PaymentCryptography::Key    |
| Amazon Pinpoint          | Actividad de la API de Amazon Pinpoint en aplicaciones de segmentación móvil. | Aplicación de segmentación móvil              | AWS::Pinpoint::App               |
| AWS Private CA           | Conector AWS Private CA para la actividad de la API de Active Directory.      | AWS Private CA Conector para Active Directory | AWS::PCAConnectorAD::Connector   |
| AWS Private CA           | Conector de AWS Private CA para la actividad de la API de SCEP.               | AWS Private CA Conector para SCEP             | AWS::PCAConnectorSCEP::Connector |

| Servicio de AWS    | Descripción                                                                      | Tipo de recurso (consola)            | resources.type value          |
|--------------------|----------------------------------------------------------------------------------|--------------------------------------|-------------------------------|
| Amazon Q Apps      | Actividad de la API de datos en <a href="#">Amazon Q Apps</a> .                  | Amazon Q Apps                        | AWS::QApps::QApp              |
| Amazon Q Apps      | Actividad de la API de datos en las sesiones de Amazon Q Apps.                   | Sesión de Amazon Q App               | AWS::QApps::QAppSession       |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en una aplicación.      | Aplicación de Amazon Q Business      | AWS::QBusiness::Application   |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en un origen de datos.  | Origen de datos de Amazon Q Business | AWS::QBusiness::DataSource    |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en un índice.           | Índice de Amazon Q Business          | AWS::QBusiness::Index         |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en una experiencia web. | Experiencia web de Amazon Q Business | AWS::QBusiness::WebExperience |
| Amazon Q Business  | Actividad de la API de integración de Amazon Q Business.                         | Integración de Amazon Q Business     | AWS::QBusiness::Integration   |
| Amazon Q Developer | Actividad de la API de Amazon Q Developer en una integración.                    | Integración para Q Developer         | AWS::QDeveloper::Integration  |

| Servicio de AWS     | Descripción                                                                                                 | Tipo de recurso (consola)                  | resources.type value             |
|---------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------|----------------------------------|
| Amazon Q Developer  | <a href="#">Actividad de la API de Amazon Q Developer en investigaciones operativas.</a>                    | Grupos de investigación de AIOps           | AWS::AIOps::InvestigationGroup   |
| Amazon Quick Suite  | Actividad de la API de Amazon Quick Suite en un conector de acciones.                                       | Acciones de QuickSuite de AWS              | AWS::Quicksight::ActionConnector |
| Amazon Quick Suite  | Actividad de la API de flujo de Amazon Quick Suite.                                                         | AWS::Quicksight::Flow                      | AWS::Quicksight::Flow            |
| Amazon Quick Suite  | Actividad de la API de FlowSession de Amazon Quick Suite.                                                   | AWS::Quicksight::FlowSession               | AWS::Quicksight::FlowSession     |
| Amazon SageMaker AI | Actividad de <a href="#">InvokeEndpointWithResponseStream</a> de Amazon SageMaker AI en puntos de conexión. | Punto de conexión de SageMaker AI          | AWS::SageMaker::Endpoint         |
| Amazon SageMaker AI | Actividad de la API de Amazon SageMaker AI en los almacenes de características.                             | Almacén de características de SageMaker AI | AWS::SageMaker::FeatureGroup     |

| Servicio de AWS             | Descripción                                                                                                              | Tipo de recurso (consola)                                        | resources.type value                     |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------|
| Amazon SageMaker AI         | Actividad de la API de Amazon SageMaker AI en los <a href="#">componentes del registro de seguimiento experimental</a> . | Componente de prueba del experimento de métricas de SageMaker AI | AWS::SageMaker::ExperimentTrialComponent |
| Amazon SageMaker AI         | Actividad de la API MLFlow de Amazon SageMaker AI.                                                                       | MLflow de Sagemaker                                              | AWS::SageMaker::MlflowTrackingServer     |
| AWS Signer                  | Actividad de la API de Signer sobre el trabajo de firma.                                                                 | Trabajo de firma de Signer                                       | AWS::Signer::SigningJob                  |
| AWS Signer                  | Actividad de la API de Signer sobre los trabajos de firma.                                                               | Perfil de firma del Signer                                       | AWS::Signer::SigningProfile              |
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en conjuntos de configuraciones.                         | Conjunto de configuración de SES                                 | AWS::SES::ConfigurationSet               |
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en identidades de correo electrónico.                    | Identidad de SES                                                 | AWS::SES::EmailIdentity                  |

| Servicio de AWS             | Descripción                                                                        | Tipo de recurso (consola)            | resources.type value             |
|-----------------------------|------------------------------------------------------------------------------------|--------------------------------------|----------------------------------|
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en plantillas.     | Plantilla de SES                     | AWS::SES::Template               |
| Amazon SimpleDB             | Actividad de la API de Amazon SimpleDB en los dominios.                            | Dominio de SimpleDB                  | AWS::SDB::Domain                 |
| AWS Step Functions          | <a href="#">Actividad de la API de Step Functions</a> en las actividades.          | Step Functions                       | AWS::StepFunctions::Activity     |
| AWS Step Functions          | <a href="#">Actividad de la API de Step Functions</a> en una máquina de estado.    | Máquina de estado de Step Functions  | AWS::StepFunctions::StateMachine |
| AWS Systems Manager         | <a href="#">Actividad de la API de Systems Manager</a> en los canales de control.  | Systems Manager                      | AWS::SSMMessages::ControlChannel |
| AWS Systems Manager         | Actividad de la API de Systems Manager sobre las evaluaciones de impacto.          | Evaluación de impacto de SSM         | AWS::SSM::ExecutionPreview       |
| AWS Systems Manager         | <a href="#">Actividad de la API de Systems Manager</a> en los nodos administrados. | Nodo administrado de Systems Manager | AWS::SSM::ManagedNode            |

| Servicio de AWS                     | Descripción                                                                                    | Tipo de recurso (consola)                | resources.type value                  |
|-------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------------|
| Amazon Timestream                   | Actividad de la API <a href="#">Query</a> de Amazon Timestream en las bases de datos.          | Base de datos de Timestream              | AWS::Timestream::Database             |
| Amazon Timestream                   | Actividad de la API de Amazon Timestream en los puntos de conexión regionales.                 | Punto de conexión regional de Timestream | AWS::Timestream::RegionalEndpoint     |
| Amazon Timestream                   | Actividad de la API <a href="#">Query</a> 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 |
| Cliente ligero de Amazon WorkSpaces | Actividad de la API de cliente ligero de WorkSpaces en un dispositivo.                         | Dispositivo de cliente ligero            | AWS::ThinClient::Device               |
| Cliente ligero de Amazon WorkSpaces | Actividad de la API de cliente ligero de WorkSpaces en un entorno.                             | Entorno de cliente ligero                | AWS::ThinClient::Environment          |
| AWS X-Ray                           | <a href="#">Actividad de la API de X-Ray</a> en los <a href="#">registros de seguimiento</a> . | Registros de seguimiento de X-Ray        | 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 eventos de datos de CloudTrail, debe agregar explícitamente los recursos o tipos de recursos admitidos cuya actividad desea recopilar. Para obtener más información, consulte [Creación de un registro de seguimiento con la consola de CloudTrail](#) y [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

Se aplican cargos adicionales para registrar eventos de datos. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

En el siguiente ejemplo, se muestra un registro único de un evento de datos para la acción Publish de Amazon SNS.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::123456789012:user/Bob",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "ExampleUser"
      },
      "attributes": {
        "creationDate": "2023-08-21T16:44:05Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-08-21T16:48:37Z",
  "eventSource": "sns.amazonaws.com",
  "eventName": "Publish",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
```

```

    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
        "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}

```

En el siguiente ejemplo, se muestra un registro único de un evento de datos para la acción `GetCredentialsForIdentity` de Amazon Cognito.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",

```



```

    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaa":
"HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}

```

## Eventos de actividad de la red

Los eventos de actividad de la red de CloudTrail permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Los eventos de actividad de la red muestran información sobre las operaciones de recursos realizadas dentro de una VPC.

Puede registrar los eventos de actividad de la red para los siguientes servicios:

- AWS AppConfig
- AWS App Mesh
- Amazon Athena
- Intercambio de datos de AWS B2B
- AWS Backup gateway
- Amazon Bedrock
- Administración de facturación y costos
- Calculadora de precios de AWS
- AWS Cost Explorer
- API de control de nube de AWS
- AWS CloudHSM
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Señales de aplicación de CloudWatch
- AWS CodeDeploy
- Amazon Comprehend Medical
- AWS Config
- Exportaciones de datos de AWS
- Amazon Data Firehose
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon EventBridge
- Programador de Amazon EventBridge
- Amazon Fraud Detector

- capa gratuita de AWS
- Amazon FSx
- AWS Glue
- AWS HealthLake
- AWS IoT FleetWise
- AWS IoT Secure Tunneling
- Facturación de AWS
- Amazon Keyspaces (for Apache Cassandra)
- AWS KMS
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Amazon Personalize
- Amazon Q Business
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon S3

 Note

Amazon S3 no admite [puntos de acceso de varias regiones](#).

- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Storage Gateway
- Administrador de incidentes de AWS Systems Manager
- Amazon Textract

- Amazon Transcribe
- Amazon Translate
- AWS Transform
- Amazon Verified Permissions
- Amazon WorkMail

El registro de los eventos de actividad de la red está deshabilitado de forma predeterminada cuando crea un registro de seguimiento o un almacén de datos de eventos. A fin de registrar eventos de actividad de la red de CloudTrail, debe establecer explícitamente el origen de los eventos cuya actividad desea recopilar. Para obtener más información, consulte [Registro de eventos de actividad de la red](#).

Se aplican cargos adicionales por el registro de eventos de actividad de la red. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

En el siguiente ejemplo, se muestra un evento ListKeys de AWS KMS correcto que ha atravesado un punto de conexión de VPC. El campo vpcEndpointId muestra el ID del punto de conexión de VPC. El campo vpcEndpointAccountId muestra el ID de la cuenta del propietario del punto de conexión de VPC. En este ejemplo, la solicitud la realizó el propietario del punto de conexión de VPC.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ASIAIOSFODNN7EXAMPLE:role-name",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/role-name",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2024-06-04T23:10:46Z",
        "mfaAuthenticated": "false"
      }
    }
  }
}
```

```

    }
  }
},
"eventTime": "2024-06-04T23:12:50Z",
"eventSource": "kms.amazonaws.com",
"eventName": "ListKeys",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"requestID": "16bcc089-ac49-43f1-9177-EXAMPLE23731",
"eventID": "228ca3c8-5f95-4a8a-9732-EXAMPLE60ed9",
"eventType": "AwsVpceEvent",
"recipientAccountId": "123456789012",
"sharedEventID": "a1f3720c-ef19-47e9-a5d5-EXAMPLE8099f",
"vpceEndpointId": "vpce-EXAMPLE08c1b6b9b7",
"vpceEndpointAccountId": "123456789012",
"eventCategory": "NetworkActivity"
}

```

El siguiente ejemplo muestra un evento `ListKeys` de AWS KMS incorrecto con una infracción de la política de puntos de conexión de VPC. Debido a que se ha producido una infracción de la política de VPC, se muestran los campos `errorCode` y `errorMessage`. El ID de la cuenta en los campos `recipientAccountId` y `vpceEndpointAccountId` es el mismo, lo cual indica que el evento se envió al propietario del punto de conexión de VPC. El `accountId` del elemento `userIdentity` no es el `vpceEndpointAccountId`, lo cual indica que el usuario que realiza la solicitud no es el propietario del punto de conexión de VPC.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSAccount",
    "principalId": "AKIAIOSFODNN7EXAMPLE",
    "accountId": "777788889999"
  },
  "eventTime": "2024-07-15T23:57:12Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "ListKeys",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "errorCode": "VpceAccessDenied",
  "errorMessage": "The request was denied due to a VPC endpoint policy",
  "requestID": "899003b8-abc4-42bb-ad95-EXAMPLE0c374",
  "eventID": "7c6e3d04-0c3b-42f2-8589-EXAMPLE826c0",

```

```
"eventType": "AwsVpceEvent",  
"recipientAccountId": "123456789012",  
"sharedEventID": "702f74c4-f692-4bfd-8491-EXAMPLEb1ac4",  
"vpceEndpointId": "vpce-EXAMPLE08c1b6b9b7",  
"vpceEndpointAccountId": "123456789012",  
"eventCategory": "NetworkActivity"  
}
```

## Eventos de Insights

Los eventos de CloudTrail Insights capturan una tasa de llamadas inusuales de API o una actividad de tasa de error en su cuenta de AWS mediante el análisis de la actividad de administración de CloudTrail. 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 capturados en un registro de seguimiento o un almacén de datos de eventos de CloudTrail, los eventos de Insights solo se registran cuando CloudTrail detecta cambios en el registro de la tasa de error o de uso de la API de su cuenta que difieren considerablemente de los patrones de uso típicos de la cuenta. Para obtener más información, consulte [Trabajar con CloudTrail Insights](#).

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 eventos de Insights de CloudTrail, debe habilitar explícitamente los eventos de Insights en un registro de seguimiento o almacén de datos de eventos nuevo o existente. Para obtener más información acerca de la creación de un registro de seguimiento, consulte [Creación de un registro de seguimiento con la consola de CloudTrail](#). Para obtener más información acerca de la creación de un almacén de datos de eventos, consulte [Creación de un almacén de datos de eventos para los eventos de Insights con la consola](#).

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](#).

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 [CloudTrail registra el contenido de los eventos de Insights para registros de seguimiento](#).

```
{
  "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"
}
```

## 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](#)
- [Eventos de lectura y escritura](#)
- [Registro de eventos de administración con la Consola de administración de AWS](#)
  - [Actualización de la configuración de los eventos de administración de un registro de seguimiento existente](#)
  - [Actualización de la configuración de eventos de administración de un almacén de datos de eventos existente](#)
- [Registro de eventos de administración con la AWS CLI](#)
  - [Ejemplos: Registro de eventos de administración para los registros de seguimiento](#)
    - [Ejemplos: Registro de eventos de administración para registros de seguimiento mediante selectores de eventos avanzados](#)
    - [Ejemplos: Registro de eventos de administración para registros de seguimiento mediante selectores de eventos básicos](#)
  - [Ejemplos: Registros de eventos de administración para los almacenes de datos de eventos](#)
    - [Ejemplo: excluir los eventos de administración de AWS KMS](#)
    - [Ejemplo: excluir los eventos de administración de Amazon RDS](#)
    - [Ejemplo: excluir los eventos de Servicio de AWS y eventos de las sesiones de la Consola de administración de AWS](#)

- [Ejemplo: excluir los eventos de administración para una identidad de IAM específica](#)
- [Registro de eventos de administración con los SDK de AWS](#)

## 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 `AWS CloudTrail de CreateTrail`)

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](#).

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos están configurados para registrar eventos de administración.

### Note

La característica Event history (Historial de eventos) de CloudTrail admite únicamente 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 eventos de CloudTrail](#).

## 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 `amzn-s3-demo-bucket1` 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 `amzn-s3-demo-bucket2` 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 a `amzn-s3-demo-bucket1`.

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 a `amzn-s3-demo-bucket2`.

## Registro de eventos de administración con la Consola de administración de AWS

En esta sección, se describe cómo actualizar la configuración de eventos de administración de un registro de seguimiento o almacén de datos de eventos existentes.

### Temas

- [Actualización de la configuración de los eventos de administración de un registro de seguimiento existente](#)
- [Actualización de la configuración de eventos de administración de un almacén de datos de eventos existente](#)

### Actualización de la configuración de los eventos de administración de un registro de seguimiento existente

Utilice los siguientes procedimientos para actualizar la configuración de eventos de administración de un registro de seguimiento existente.

1. Inicie sesión en la Consola de administración de AWS 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 y elija el nombre del registro de seguimiento.
3. En Management events (Eventos de administración), elija Edit (Editar).
  - Elija si quiere registrar eventos de Lectura, Escritura o ambos.
  - Elija Excluir eventos de AWS KMS para filtrar eventos de AWS Key Management Service (AWS KMS) del registro de seguimiento. 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. 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 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).

- 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.

4. Cuando haya terminado, seleccione Guardar cambios.

## Actualización de la configuración de eventos de administración de un almacén de datos de eventos existente

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. Abra la página Almacenes de datos de eventos de la consola de CloudTrail y seleccione el nombre del almacén de datos de eventos.
3. Para los Eventos de administración, elija Editar y, luego, configure los siguientes ajustes:
  - a. Elija entre la Recopilación de eventos simple o la Recopilación de eventos avanzada:
    - Elija Recopilación de eventos simple si desea registrar todos los eventos, registrar solo los eventos de lectura o registrar solo los eventos de escritura. También tiene la opción de elegir excluir los eventos de administración de AWS Key Management Service y la API de datos de Amazon RDS.

- Elija Recopilación avanzada de eventos si desea incluir o excluir los eventos de administración en función de los valores de los campos del selector de eventos avanzado, como los campos `eventName`, `eventType`, `eventSource` y `userIdentity.arn`.
- b. Si seleccionó la Recopilación de eventos simple, elija si quiere registrar todos los eventos, registrar solo los eventos de lectura o registrar solo los eventos de escritura. También tiene la opción de elegir excluir los eventos de administración de AWS KMS y de Amazon RDS.
- c. Si seleccionó la Recopilación de eventos avanzada, realice las siguientes selecciones:
  - i. En la Plantilla de selector de registros, elija una plantilla predefinida o Personalizada para crear una configuración personalizada basada en los valores de los campos del selector de eventos avanzado.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
  - Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
  - Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
  - Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
  - Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).
- ii. (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 administración de las sesiones de la Consola de administración de AWS”. El nombre del selector aparece como `Name` en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
  - iii. Si eligió Personalizado, en los Selectores de eventos avanzados cree una expresión basada en los valores de los campos del selector de eventos avanzado.

 Note

Los selectores no admiten el uso de caracteres comodín como \*. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

A. Elija uno de los siguientes campos.

- **readOnly**: `readOnly` se puede establecer en igual a un valor `true` o `false`. Cuando se establece en `false`, el almacén de datos de eventos registra eventos de administración de solo escritura. Los eventos de administración de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`. Para registrar los eventos Lectura y Escritura, no agregue un selector de `readOnly`.
- **eventName** – `eventName` puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de administración, como `CreateAccessPoint` o `GetAccessPoint`.
- **userIdentity.arn**: incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento `userIdentity` de CloudTrail](#).
- **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de Consola de administración de AWS. Este campo se puede establecer como igual o no igual con un valor de `true`.
- **eventSource**: puede usarlo para incluir o excluir orígenes de eventos específicos. El `eventSource` suele ser una forma abreviada del nombre del servicio sin espacios más `.amazonaws.com`. Por ejemplo, podría establecer el valor `eventSource` igual a `ec2.amazonaws.com` para registrar solo los eventos de administración de Amazon EC2.
- **eventType**: el [Tipo de evento](#) que se va a incluir o excluir. Por ejemplo, puede establecer este campo en no igual a `AwsServiceEvent` para excluir [eventos de Servicio de AWS](#).

- B. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- C. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
- iv. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
- d. Seleccione Habilitar la captura de eventos de Insights para activar 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. 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.



4. Cuando haya terminado, seleccione Guardar cambios.

## Registro de eventos de administración con la AWS CLI

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 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 básicos y avanzados.

## Temas

- [Ejemplos: Registro de eventos de administración para registros de seguimiento mediante selectores de eventos avanzados](#)
- [Ejemplos: Registro de eventos de administración para registros de seguimiento mediante selectores de eventos básicos](#)

## Ejemplos: Registro de eventos de administración para registros de seguimiento mediante selectores de eventos avanzados

En el siguiente ejemplo se crea un selector de eventos avanzados para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura (se omite el selector `readOnly`), pero excluye los eventos de AWS Key Management Service (AWS KMS). Como los eventos de AWS KMS se tratan como eventos de administración y puede haber una gran cantidad de ellos, su factura de CloudTrail se puede ver incrementada si tiene más de un registro de seguimiento que captura 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"] }
    ]
  }
]'
```

En el siguiente ejemplo se crea un selector de eventos avanzados para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura (se omite el selector `readOnly`), pero excluye los eventos de administración de la API de datos

de Amazon RDS. A fin de excluir eventos de administración de la API de datos de Amazon RDS, especifique el origen de los eventos de la API de datos de Amazon RDS en el valor de cadena del campo `eventSource: rdsdata.amazonaws.com`.

Si elige no registrar eventos de administración, no se registrarán los eventos de administración de la API de datos de Amazon RDS y no podrá cambiar la configuración del registro de eventos de la API de datos de Amazon RDS.

Para comenzar de nuevo a registrar eventos de administración de la API de datos de Amazon RDS en un registro de seguimiento, elimine 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 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: Registro de eventos de administración para registros de seguimiento 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:::amzn-s3-demo-bucket/prefix",
"arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket/prefix",
          "arn:aws:s3:::amzn-s3-demo-bucket2/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 ejemplo siguiente se crea un selector de eventos para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura, pero excluye los eventos de 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 del registro de seguimiento, ejecute el comando `put-event-selectors` y agregue el atributo `ExcludeManagementEventSources` con un valor de `rdsdata.amazonaws.com`. En el ejemplo siguiente se crea un selector de eventos para un registro de seguimiento denominado *TrailName* que incluye eventos de administración de solo lectura y de solo escritura, pero excluye los eventos de administración de la API de datos de Amazon RDS. Como la API de datos de Amazon RDS puede generar un gran volumen de eventos de administración, el usuario de este ejemplo debería limitar los eventos para administrar el costo de un registro de seguimiento.

```

{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "EventSelectors": [
    {
      "ReadWriteType": "All",
      "IncludeManagementEvents": true,
      "DataResources": [],
      "ExcludeManagementEventSources": [
        "rdsdata.amazonaws.com"
      ]
    }
  ]
}

```

Para comenzar de nuevo el registro de eventos de administración de la API de datos de AWS KMS o Amazon RDS en un registro de seguimiento, pase una cadena vacía como 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}]'

```

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

Los eventos de administración de los almacenes de datos de eventos se registran mediante la configuración de los selectores de eventos avanzados.

Los siguientes campos del selector de eventos avanzado son compatibles para registrar eventos de administración en los almacenes de datos de eventos:

- **eventCategory:** debe configurarse eventCategory igual a Management para registrar los eventos de administración. Este campo es obligatorio.
- **readOnly:** readOnly se puede establecer en Equals un valor de true o false. Cuando se establece en false, el almacén de datos de eventos registra eventos de administración de solo escritura. Los eventos de administración de solo lectura son eventos que no cambian el estado de un recurso, como los eventos Get\* o Describe\*. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos Put\*, Delete\* o Write\*. Para registrar los eventos Lectura y Escritura, no agregue un selector de readOnly.
- **eventName** – eventName puede utilizar cualquier operador. Puede usarlo para incluir o excluir cualquier evento de administración, como CreateAccessPoint o GetAccessPoint. Puede utilizar cualquier operador con este campo.
- **userIdentity.arn:** incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- **sessionCredentialFromConsole:** incluya o excluya los eventos que se originan en una sesión de Consola de administración de AWS. Este campo se puede establecer como igual o NotEquals con un valor de true.
- **eventSource:** puede usarlo para incluir o excluir orígenes de eventos específicos. El eventSource suele ser una forma abreviada del nombre del servicio sin espacios más .amazonaws.com. Por ejemplo, podría establecer el eventSource Equals en ec2.amazonaws.com para registrar solo los eventos de administración de Amazon EC2.



- **eventType**: el [Tipo de evento](#) que se va a incluir o excluir. Por ejemplo, puede establecer este campo en `NotEquals AwsServiceEvent` a fin de excluir [eventos de Servicio de AWS](#). Puede utilizar cualquier operador con este campo.

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"
}
```

Ejemplos:

- [Ejemplo: excluir los eventos de administración de AWS KMS](#)
- [Ejemplo: excluir los eventos de administración de Amazon RDS](#)

- [Ejemplo: excluir los eventos de Servicio de AWS y eventos de las sesiones de la Consola de administración de AWS](#)
- [Ejemplo: excluir los eventos de administración para una identidad de IAM específica](#)

### Ejemplo: excluir los eventos de administración de AWS KMS

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"
}

```

### Ejemplo: excluir los eventos de administración de Amazon RDS

Para crear un almacén de datos de eventos que excluya los eventos de administración de la API de datos de Amazon RDS, ejecute el comando `create-event-data-store` y especifique que `eventSource` no es igual que `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"
  }
}

```

Ejemplo: excluir los eventos de Servicio de AWS y eventos de las sesiones de la Consola de administración de AWS

En el siguiente ejemplo, se crea un almacén de datos de eventos que registra los eventos de administración, pero excluye los eventos de Servicio de AWS y eventos que se originan en las sesiones de Consola de administración de AWS.

```

aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-selectors '[
  {
    "Name": "Exclude Servicio de AWS and console events",
    "FieldSelectors": [
      {"Field": "eventCategory", "Equals": ["Management"]},
      {"Field": "eventType", "NotEquals": ["AwsServiceEvent"]}
    ]
  }
]'

```

```

        {"Field": "sessionCredentialFromConsole", "NotEquals": ["true"]}
    ]
}
]'

```

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": "Exclude Servicio de AWS and console events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        },
        {
          "Field": "eventType",
          "NotEquals": [
            "AwsServiceEvent"
          ]
        },
        {
          "Field": "sessionCredentialFromConsole",
          "NotEquals": [
            "true"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "BillingMode": "EXTENDABLE_RETENTION_PRICING",
  "RetentionPeriod": 366,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",

```

```
"UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

Ejemplo: excluir los eventos de administración para una identidad de IAM específica

En el siguiente ejemplo, se crea un almacén de datos de eventos que registra los eventos de administración, pero excluye los eventos que genera bucket-scanner-role userIdentity.

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
  {
    "Name": "Exclude events generated by bucket-scanner-role userIdentity",
    "FieldSelectors": [
      {"Field": "eventCategory", "Equals": ["Management"]},
      {"Field": "userIdentity.arn", "NotStartsWith":
["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
    ]
  }
]'
```

A continuación, se muestra un ejemplo de respuesta.

```
{
  "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
  "Name": "event-data-store-name",
  "Status": "CREATED",
  "AdvancedEventSelectors": [
    {
      "Name": "Exclude events generated by bucket-scanner-role userIdentity",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        },
        {
          "Field": "userIdentity.arn",
          "NotStartsWith": [
            "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
          ]
        }
      ]
    }
  ]
}
```

```
    }
  ]
},
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
"UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

## Registro de eventos de administración con los SDK de AWS

Utilice la operación [GetEventSelectors](#) para saber si el registro de seguimiento está registrando los eventos de administración para un registro de seguimiento. Puede configurar sus registros de seguimiento para que registren los eventos de administración con la operación [PutEventSelectors](#). Para obtener más información, consulte la [Referencia de la API de AWS CloudTrail](#).

Ejecute la operación [GetEventDataStore](#) para comprobar si su almacén de datos de eventos incluye los eventos de administración. Puede configurar sus almacenes de datos de eventos para incluir eventos de administración ejecutando las operaciones [CreateEventDataStore](#) o [UpdateEventDataStore](#). Para obtener más información, consulte [Creación, actualización y administración de almacenes de datos de eventos con la AWS CLI](#) y la [AWS CloudTrail API Reference](#).

## Registro de eventos de datos

En esta sección se describe cómo registrar eventos de datos a través de la [consola de CloudTrail](#) y la [AWS CLI](#).

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 más información, consulte [Precios de AWS CloudTrail](#).

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 el nivel de objeto de Amazon S3](#) (por ejemplo, las operaciones `GetObject`, `DeleteObject` y `PutObject` de la API) en objetos de los buckets de S3.
- Actividad de ejecución de funciones de AWS Lambda (la API `Invoke`).
- La actividad de [PutAuditEvents](#) de CloudTrail en un [canal de CloudTrail Lake](#) que se utiliza para registrar eventos externos a AWS.
- Operaciones de la API [Publish](#) y [PublishBatch](#) de Amazon SNS sobre temas.

Puede usar selectores de eventos avanzados para crear selectores detallados que le ayuden a controlar los costos al registrar únicamente los eventos específicos de interés para sus casos de uso. Por ejemplo, puede utilizar selectores de eventos avanzados para registrar llamadas a la API específicas si agrega un filtro en el campo `eventName`. Para obtener más información, consulte [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#).

#### Note

Los eventos que registran sus registros de seguimiento 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 relativos a estos objetos de S3 están disponibles en Amazon EventBridge. Para obtener más información, consulte [los eventos de servicio de AWS ofrecidos a través de CloudTrail](#) en la Guía del usuario de Amazon EventBridge y en la [Referencia de eventos de AWS](#).

## Contenido

- [Eventos de datos](#)
  - [Eventos de datos compatibles con AWS CloudTrail](#)
  - [Ejemplos: registrar eventos de datos para objetos de Amazon S3](#)
  - [Registrar eventos de datos para objetos de S3 en otras cuentas de AWS](#)
- [Eventos de solo lectura y de solo escritura](#)
- [Registrar eventos de datos con la Consola de administración de AWS](#)
- [Registrar eventos de datos con la AWS Command Line Interface](#)
  - [Registro de eventos de datos para registros de seguimiento con la AWS CLI](#)

- [Registrar los eventos de datos de los registros de seguimiento mediante selectores de eventos avanzados](#)
- [Registrar 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](#)
- [Registro de eventos de datos para los almacenes de datos de eventos con la AWS CLI](#)
  - [Incluir todos los eventos de Amazon S3 en un bucket específico](#)
  - [Incluir Amazon S3 en los eventos de AWS Outposts](#)
- [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#)
- [Cómo evalúa CloudTrail varias condiciones de un campo](#)
  - [Ejemplo que muestra varias condiciones para el campo resources.ARN](#)
- [Ejemplos de la AWS CLI para filtrar de eventos de datos](#)
  - [Ejemplo 1: filtrar en el campo eventName](#)
  - [Ejemplo 2: filtrar en los campos resources.ARN y userIdentity.arn](#)
  - [Ejemplo 3: filtrar los campos resources.type y eventName para excluir los objetos individuales eliminados por un evento DeleteObjects de Amazon S3](#)
- [Registrar eventos de datos para la conformidad con AWS Config](#)
- [Registro de eventos de datos con los SDK de AWS](#)

## Eventos de datos

En la siguiente tabla, se muestran los tipos de recursos disponibles para los registros de seguimiento y los almacenes de datos de eventos. En la columna Tipo de recurso (consola), se muestra la selección adecuada en la consola. En la columna resources.type value, se muestra el valor de resources.type que debe especificar para incluir eventos de datos de ese tipo en el registro de seguimiento o el almacén de datos de eventos por medio de la AWS CLI o las API de CloudTrail.

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

## Eventos de datos compatibles con AWS CloudTrail

| Servicio de AWS | Descripción                                                                                                                                                                                                                           | Tipo de recurso (consola)                     | resources.type value   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|------------------------|
| Amazon RDS      | <a href="#">Actividad de la API de Amazon RDS</a> en un clúster de base de datos.                                                                                                                                                     | API de datos de RDS: clúster de base de datos | AWS::RDS::DBCluster    |
| Amazon S3       | <a href="#">Actividad de la API en el nivel de objeto de Amazon S3</a> (por ejemplo, las operaciones <code>GetObject</code> , <code>DeleteObject</code> y <code>PutObject</code> de la API) en objetos de los buckets de uso general. | S3                                            | AWS::S3::Object        |
| Amazon S3       | <a href="#">Actividad de la API de Amazon S3</a> en los puntos de acceso.                                                                                                                                                             | Punto de acceso de S                          | AWS::S3::AccessPoint   |
| Amazon S3       | <a href="#">Actividad de la API en el nivel de objeto de Amazon S3</a> (por ejemplo, las operaciones <code>GetObject</code> , <code>DeleteObject</code> y                                                                             | S3 Express                                    | AWS::S3Express::Object |

| Servicio de AWS     | Descripción                                                                                                                                        | Tipo de recurso (consola) | resources.type value             |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------------------|
|                     | PutObject de la API) en objetos de los buckets de directorio.                                                                                      |                           |                                  |
| Amazon S3           | <a href="#">Actividad de la API en los puntos de acceso de Amazon S3 Object Lambda</a> , como las llamadas a CompleteMultipartUpload y GetObject . | S3 Object Lambda          | AWS::S3ObjectLambda::AccessPoint |
| Amazon S3           | Actividad de la API de Amazon FSx en volúmenes.                                                                                                    | Volumen de FSx            | AWS::FSx::Volume                 |
| Tablas de Amazon S3 | Actividad de la API de Amazon S3 en las <a href="#">tablas</a> .                                                                                   | Tabla de S3               | AWS::S3Tables::Table             |
| Tablas de Amazon S3 | Actividad de la API de Amazon S3 en los <a href="#">buckets de las tablas</a> .                                                                    | Bucket de tablas de S3    | AWS::S3Tables::TableBucket       |
| Amazon S3 Vectors   | Actividad de la API de Amazon S3 en los <a href="#">buckets de vectores</a> .                                                                      | Bucket de vector S3       | AWS::S3Vectors::VectorBucket     |
| Amazon S3 Vectors   | Actividad de la API de Amazon S3 en <a href="#">índices de vectores</a> .                                                                          | Índice de vector S3       | AWS::S3Vectors::Index            |

| Servicio de AWS       | Descripción                                                                                             | Tipo de recurso (consola)                 | resources.type value       |
|-----------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------|
| Amazon S3 en Outposts | <a href="#">Actividad de la API en cuanto a objetos de Amazon S3 en Outposts.</a>                       | S3 Outposts                               | AWS::S3Outposts::Object    |
| Amazon SNS            | Operaciones de la API <a href="#">Publish</a> de Amazon SNS en los puntos de conexión de la plataforma. | Punto de conexión de la plataforma de SNS | AWS::SNS::PlatformEndpoint |
| Amazon SNS            | Operaciones de la API <a href="#">Publish</a> y <a href="#">PublishBatch</a> de Amazon SNS sobre temas. | Tema de SNS                               | AWS::SNS::Topic            |
| Amazon SQS            | <a href="#">Actividad de la API de Amazon SQS</a> en los mensajes.                                      | SQS                                       | AWS::SQS::Queue            |
| AWS Supply Chain      | Actividad de la API de AWS Supply Chain en una instancia.                                               | Supply Chain                              | AWS::SCN::Instance         |
| Amazon SWF            | <a href="#">Actividad de la API de Amazon SWF</a> en los dominios.                                      | Dominio de SWF                            | AWS::SWF::Domain           |

| Servicio de AWS                 | Descripción                                                                                                                                                                                | Tipo de recurso (consola)           | resources.type value                       |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|--------------------------------------------|
| AWS AppConfig                   | <a href="#">Actividad de la API de AWS AppConfig</a> para operaciones de configuración, como las llamadas a <code>StartConfigurationSession</code> y <code>GetLatestConfiguration</code> . | AWS AppConfig                       | <code>AWS::AppConfig::Configuration</code> |
| AWS AppSync                     | <a href="#">Actividad de la API de AWS AppSync</a> en las API GraphQL de AppSync.                                                                                                          | AppSync Graph                       | <code>AWS::AppSync::GraphQLApi</code>      |
| Amazon Aurora DSQL              | Actividad de la API de Amazon Aurora DSQL en los recursos del clúster.                                                                                                                     | Amazon Aurora DSQL                  | <code>AWS::DSQL::Cluster</code>            |
| Intercambio de datos B2B de AWS | Actividad de la API de intercambio de datos entre empresas para operaciones de Transformer, como las llamadas a <code>GetTransformerJob</code> y <code>StartTransformerJob</code> .        | Intercambio de datos entre empresas | <code>AWS::B2BI::Transformer</code>        |

| Servicio de AWS | Descripción                                                                         | Tipo de recurso (consola)              | resources.type value        |
|-----------------|-------------------------------------------------------------------------------------|----------------------------------------|-----------------------------|
| AWS Backup      | Actividad de la API de datos de búsqueda de AWS Backup en trabajos de búsqueda.     | AWS Backup API de datos de búsqueda de | AWS::Backup::SearchJob      |
| Amazon Bedrock  | <a href="#">Actividad de la API de Amazon Bedrock</a> en un alias de agente.        | Alias de agente de Bedrock             | AWS::Bedrock::AgentAlias    |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en invocaciones asíncronas.                   | Invocación asíncrona de Bedrock        | AWS::Bedrock::AsyncInvoke   |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en un alias de flujo.                         | Alias de flujo de Bedrock              | AWS::Bedrock::FlowAlias     |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en barreras de protección.                    | Barrera de protección de Bedrock       | AWS::Bedrock::Guardrail     |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en un agente insertado                        | Agente insertado e invocado en Bedrock | AWS::Bedrock::InlineAgent   |
| Amazon Bedrock  | <a href="#">Actividad de la API de Amazon Bedrock</a> en una base de conocimientos. | Base de conocimientos de Bedrock       | AWS::Bedrock::KnowledgeBase |

| Servicio de AWS | Descripción                                                                                       | Tipo de recurso (consola)                                      | resources.type value                          |
|-----------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------|
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en modelos.                                                 | Modelo de Bedrock                                              | AWS::Bedrock::Model                           |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en peticiones.                                              | Petición de Bedrock                                            | AWS::Bedrock::PromptVersion                   |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en sesiones.                                                | Sesión de Bedrock                                              | AWS::Bedrock::Session                         |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en ejecuciones de flujo.                                    | Ejecución de flujo de Bedrock                                  | AWS::Bedrock::FlowExecution                   |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en una política de razonamiento automatizado.               | Política de razonamiento automatizado de Bedrock               | AWS::Bedrock::AutomatedReasoningPolicy        |
| Amazon Bedrock  | Actividad de la API de Amazon Bedrock en una versión de la política de razonamiento automatizado. | Versión de la política de razonamiento automatizado de Bedrock | AWS::Bedrock::AutomatedReasoningPolicyVersion |
| Amazon Bedrock  | Actividad de la API del proyecto de automatización de datos de Amazon Bedrock.                    | Proyectos de automatización de datos de Bedrock                | AWS::Bedrock::DataAutomationProject           |



| Servicio de AWS | Descripción                                                                  | Tipo de recurso (consola)                             | resources.type value                    |
|-----------------|------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------|
| Amazon Bedrock  | Actividad de la API de invocación de automatización de datos de Bedrock.     | Invocación de automatización de datos de Bedrock      | AWS::Bedrock::DataAutomationInvocation  |
| Amazon Bedrock  | Actividad de la API del perfil de automatización de datos de Amazon Bedrock. | Perfil de automatización de datos de Bedrock          | AWS::Bedrock::DataAutomationProfile     |
| Amazon Bedrock  | Actividad de la API del esquema de Amazon Bedrock.                           | Esquema de Bedrock                                    | AWS::Bedrock::Blueprint                 |
| Amazon Bedrock  | Actividad de la API de intérprete de código de Amazon Bedrock.               | Intérprete de código AgentCore de Bedrock             | AWS::BedrockAgentCore::CodeInterpreter  |
| Amazon Bedrock  | Actividad de la API del navegador Amazon Bedrock.                            | Navegador AgentCore de Bedrock                        | AWS::BedrockAgentCore::Browser          |
| Amazon Bedrock  | Actividad de la API de identidad de carga de trabajo de Amazon Bedrock.      | Identidad de carga de trabajo de AgentCore de Bedrock | AWS::BedrockAgentCore::WorkloadIdentity |

| Servicio de AWS | Descripción                                                                            | Tipo de recurso (consola)                                           | resources.type value                             |
|-----------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------|
| Amazon Bedrock  | Actividad de la API del directorio de identidad de carga de trabajo de Amazon Bedrock. | Directorio de identidad de carga de trabajo de AgentCore de Bedrock | AWS::BedrockAgentCore::WorkloadIdentityDirectory |
| Amazon Bedrock  | Actividad de la API de bóveda de token de Amazon Bedrock .                             | Bóveda de token de AgentCore de Bedrock                             | AWS::BedrockAgentCore::TokenVault                |
| Amazon Bedrock  | Actividad de la API de CredentialProvider de APIKey de Amazon Bedrock.                 | Credentia IProvider de APIKey de AgentCore de Bedrock               | AWS::BedrockAgentCore::APIKeyCredentialProvider  |
| Amazon Bedrock  | Actividad de la API de tiempo de ejecución de Amazon Bedrock.                          | Tiempo de ejecución de AgentCore de Bedrock                         | AWS::BedrockAgentCore::Runtime                   |
| Amazon Bedrock  | Actividad de la API del tiempo de ejecución del punto de conexión de Amazon Bedrock.   | Tiempo de ejecución de AgentCore del punto de conexión de Bedrock   | AWS::BedrockAgentCore::RuntimeEndpoint           |
| Amazon Bedrock  | Actividad de la API de la puerta de enlace de Amazon Bedrock.                          | Puerta de enlace AgentCore de Bedrock                               | AWS::BedrockAgentCore::Gateway                   |

| Servicio de AWS | Descripción                                                                  | Tipo de recurso (consola)                               | resources.type value                            |
|-----------------|------------------------------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------|
| Amazon Bedrock  | Actividad de la API de memoria de Amazon Bedrock.                            | Memoria de AgentCore de Bedrock                         | AWS::BedrockAgentCore::Memory                   |
| Amazon Bedrock  | Actividad de la API de CredentialProvider de Oauth2 de Amazon Bedrock.       | Credentia IProvider de Oauth2 de AgentCore de Bedrock   | AWS::BedrockAgentCore::OAuth2CredentialProvider |
| Amazon Bedrock  | Actividad de API personalizada del navegador Amazon Bedrock.                 | Navegador AgentCore personalizado de Bedrock            | AWS::BedrockAgentCore::BrowserCustom            |
| Amazon Bedrock  | Actividad de la API de intérprete de código personalizado de Amazon Bedrock. | Intérprete de código AgentCore personalizado de Bedrock | AWS::BedrockAgentCore::CodeInterpreterCustom    |
| Amazon Bedrock  | Actividad de la API de la herramienta de Amazon Bedrock.                     | Herramienta de Bedrock                                  | AWS::Bedrock::Tool                              |
| AWS Cloud Map   | <a href="#">Actividad AWS Cloud Map de la API en un espacio de nombres.</a>  | AWS Cloud Map Espacio de nombres de                     | AWS::ServiceDiscovery::Namespace                |

| Servicio de AWS                              | Descripción                                                                                                                                                       | Tipo de recurso (consola)                      | resources.type value             |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------|
| AWS Cloud Map                                | <a href="#">Actividad AWS Cloud Map de la API en un servicio.</a>                                                                                                 | AWS Cloud Map Servicio de                      | AWS::ServiceDiscovery::Service   |
| Amazon CloudFront                            | Actividad de la API de CloudFront en un <a href="#">KeyValueStore</a> .                                                                                           | CloudFront KeyValueStore                       | AWS::CloudFront::KeyValueStore   |
| AWS CloudTrail                               | La actividad de <a href="#">PutAuditEvents</a> de CloudTrail en un <a href="#">canal de CloudTrail Lake</a> que se utiliza para registrar eventos externos a AWS. | Canal de CloudTrail                            | AWS::CloudTrail::Channel         |
| Amazon CloudWatch                            | <a href="#">Actividad de la API de Amazon CloudWatch en las métricas.</a>                                                                                         | Métrica de CloudWatch                          | AWS::CloudWatch::Metric          |
| Monitor de flujo de red de Amazon CloudWatch | Actividad de la API del monitor de flujo de red de Amazon CloudWatch en los monitores.                                                                            | Monitor de flujo de red                        | AWS::NetworkFlowMonitor::Monitor |
| Monitor de flujo de red de Amazon CloudWatch | Actividad de la API del monitor de flujo de red de Amazon CloudWatch en el alcance.                                                                               | Agente del monitor de flujo de red del alcance | AWS::NetworkFlowMonitor::Scope   |

| Servicio de AWS                          | Descripción                                                                                           | Tipo de recurso (consola)        | resources.type value                  |
|------------------------------------------|-------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------|
| Amazon CloudWatch RUM                    | Actividad de la API de Amazon CloudWatch RUM en los monitores de aplicaciones.                        | Monitor de aplicaciones de RUM   | AWS::RUM::AppMonitor                  |
| Generador de perfiles de Amazon CodeGuru | Actividad de la API de perfiles de CodeGuru en grupos de creación de perfiles.                        | Grupo de perfiles de CodeGuru    | AWS::CodeGuruProfiler::ProfilingGroup |
| Amazon CodeWhisperer                     | Actividad de la API de Amazon CodeWhisperer en una personalización.                                   | Personalización de CodeWhisperer | AWS::CodeWhisperer::Customization     |
| Amazon CodeWhisperer                     | Actividad de la API de Amazon CodeWhisperer en un perfil.                                             | CodeWhisperer                    | AWS::CodeWhisperer::Profile           |
| Amazon Cognito                           | Actividad de la API de Amazon Cognito en los <a href="#">grupos de identidades</a> de Amazon Cognito. | Grupos de identidades de Cognito | AWS::Cognito::IdentityPool            |
| AWS Data Exchange                        | Actividad de la API de AWS Data Exchange en los activos.                                              | Activo de Data Exchange          | AWS::DataExchange::Asset              |
| Amazon Data Firehose                     | Actividad de la API del flujo de entrega de Amazon Data Firehose                                      | Amazon Data Firehose             | AWS::KinesisFirehose::DeliveryStream  |

| Servicio de AWS    | Descripción                                                                   | Tipo de recurso (consola)    | resources.type value  |
|--------------------|-------------------------------------------------------------------------------|------------------------------|-----------------------|
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en las flotas.       | Deadline Cloud Flota de      | AWS::Deadline::Fleet  |
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en los trabajos.     | Deadline Cloud Trabajo de    | AWS::Deadline::Job    |
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en las colas.        | Deadline Cloud Cola de       | AWS::Deadline::Queue  |
| AWS Deadline Cloud | <a href="#">Deadline Cloud</a><br>Actividad de la API de en los trabajadores. | Deadline Cloud Trabajador de | AWS::Deadline::Worker |

| Servicio de AWS | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Tipo de recurso (consola) | resources.type value |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|----------------------|
| Amazon DynamoDB | <p><a href="#">Actividad de la API en el nivel de elemento de Amazon DynamoDB</a> en las tablas (por ejemplo, las operacion es PutItem, DeleteItem y UpdateItem de la API).</p> <div>  <p><b>Note</b></p> <p>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 ,</p> </div> | DynamoDB                  | AWS::DynamoDB::Table |

| Servicio de AWS | Descripción                                                                                                                                                                                                 | Tipo de recurso (consola) | resources.type value  |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-----------------------|
|                 | registrará tanto los eventos de la tabla de DynamoDB como los de los flujos de DynamoDB de forma predeterminada. Para excluir <a href="#">eventos de flujos</a> , agregue un filtro en el campo eventName . |                           |                       |
| Amazon DynamoDB | Actividad de la API de <a href="#">Amazon DynamoDB</a> en los flujos.                                                                                                                                       | DynamoDB Streams          | AWS::DynamoDB::Stream |



| Servicio de AWS                   | Descripción                                                                                                                                                   | Tipo de recurso (consola)                    | resources.type value              |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------|
| Amazon Elastic Block Store        | API directas de <a href="#">Amazon Elastic Block Store (EBS)</a> , como PutSnapshotBlock, GetSnapshotBlock y ListChangedBlocks en instantáneas de Amazon EBS. | API directas de Amazon EBS                   | AWS::EC2::Snapshot                |
| Amazon Elastic Compute Cloud      | Actividad de la API del punto de conexión de Amazon EC2 Instance Connect                                                                                      | Punto de conexión a EC2 Instance Connect     | AWS::EC2::InstanceConnectEndpoint |
| Amazon Elastic Container Service  | Actividad de la API de Amazon Elastic Container en una instancia de contenedor.                                                                               | Instancia de contenedor de ECS               | AWS::ECS::ContainerInstance       |
| Amazon Elastic Kubernetes Service | Actividad de la API de Amazon Elastic Kubernetes Service en los paneles.                                                                                      | Paneles de Amazon Elastic Kubernetes Service | AWS::EKS::Dashboard               |

| Servicio de AWS                                         | Descripción                                                                                                                      | Tipo de recurso (consola)                                     | resources.type value                |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------|
| Amazon EMR                                              | <a href="#">Actividad de la API de Amazon EMR</a> en un espacio de trabajo de registros de escritura anticipada.                 | Espacio de trabajo de registro de escritura anticipada de EMR | AWS::EMRWAL::Workspace              |
| Mensajes SMS para usuarios finales de AWS               | Actividad de la API de <a href="#">Mensajes SMS para usuarios finales de AWS</a> en las identidades de origen.                   | Identidad de origen de SMS Voice                              | AWS::SMSVoice::OriginationIdentity  |
| Mensajes SMS para usuarios finales de AWS               | Actividad de la API de <a href="#">mensajes SMS para usuarios finales de AWS</a> en los mensajes.                                | Mensaje de voz de SMS                                         | AWS::SMSVoice::Message              |
| Mensajes de redes sociales para usuarios finales de AWS | Actividad de la API de <a href="#">Mensajes de redes sociales para usuarios finales de AWS</a> en los ID de números de teléfono. | ID de número de teléfono de mensajes de redes sociales        | AWS::SocialMessaging::PhoneNumberId |
| Mensajes de redes sociales para usuarios finales de AWS | Actividad de la API de Mensajes de redes sociales de AWS para usuarios finales en los ID de Waba.                                | ID de Waba ID de mensajes de redes sociales                   | AWS::SocialMessaging::WabaId        |

| Servicio de AWS         | Descripción                                                                                                 | Tipo de recurso (consola)                  | resources.type value              |
|-------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------|
| Amazon FinSpace         | <a href="#">Amazon FinSpace</a><br>Actividad de la API de entornos.                                         | FinSpace                                   | AWS::FinSpace::Environment        |
| Amazon GameLift Streams | <a href="#">Actividad de la API de transmisión</a> de Amazon GameLift Streams en las aplicaciones.          | Aplicación de GameLift Streams             | AWS::GameLiftStreams::Application |
| Amazon GameLift Streams | <a href="#">Actividad de la API de transmisión</a> de Amazon GameLift Streams en los grupos de transmisión. | Grupo de transmisiones de GameLift Streams | AWS::GameLiftStreams::StreamGroup |
| AWS Glue                | Actividad de la API de AWS Glue en tablas creadas por Lake Formation.                                       | Lake Formation                             | AWS::Glue::Table                  |
| Amazon GuardDuty        | Actividad de la API de Amazon GuardDuty para un <a href="#">detector</a> .                                  | Detector de GuardDuty                      | AWS::GuardDuty::Detector          |
| AWS HealthImaging       | Actividad de la API de AWS HealthImaging en los almacenes de datos.                                         | Almacén de datos de MedicalImaging         | AWS::MedicalImaging::Datastore    |

| Servicio de AWS              | Descripción                                                                                                                                                                                                                                                                                            | Tipo de recurso (consola)              | resources.type value                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------------|
| AWS HealthImaging            | Actividad de la API del conjunto de imágenes de AWS HealthImaging.                                                                                                                                                                                                                                     | Conjunto de imágenes de MedicalImaging | AWS::MedicalImaging::Imageset       |
| AWS IoT                      | <a href="#">Actividad de la API de AWS IoT en los certificados.</a>                                                                                                                                                                                                                                    | Certificado IoT                        | AWS::IoT::Certificate               |
| AWS IoT                      | <a href="#">Actividad de la API de AWS IoT en los objetos.</a>                                                                                                                                                                                                                                         | Objeto de IoT                          | AWS::IoT::Thing                     |
| AWS IoT Greengrass Version 2 | <a href="#">Actividad de la API de Greengrass</a> desde un dispositivo principal de Greengrass en una versión del componente. <div>  <b>Note</b><br/> Greengrass no registra los eventos de acceso denegado. </div> | Versión del componente IoT Greengrass  | AWS::GreengrassV2::ComponentVersion |

| Servicio de AWS               | Descripción                                                                                                                                                                                                                                                                                 | Tipo de recurso (consola)        | resources.type value                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|--------------------------------------|
| AWS IoT Greengrass Version 2  | <p><a href="#">Actividad de la API de Greengrass</a> desde un dispositivo principal de Greengrass en una implementación.</p> <div>  Note<br/>Greengrass no registra los eventos de acceso denegado. </div> | Implementación de IoT Greengrass | AWS::GreengrassV2::Deployment        |
| AWS IoT SiteWise              | <a href="#">Actividad de la API de IoT SiteWise</a> en los <a href="#">activos</a> .                                                                                                                                                                                                        | Activo de IoT SiteWise           | AWS::IoTSiteWise::Asset              |
| AWS IoT SiteWise              | <a href="#">Actividad de la API de IoT SiteWise</a> en las <a href="#">series temporales</a> .                                                                                                                                                                                              | Serie temporal de IoT SiteWise   | AWS::IoTSiteWise::TimeSeries         |
| AWS IoT SiteWise Assistant de | Actividad de la API de Sitewise Assistant en las conversaciones.                                                                                                                                                                                                                            | Conversación con Sitewise Assist | AWS::SitewiseAssistant::Conversation |
| AWS IoT TwinMaker             | Actividad de la API de IoT TwinMaker en una <a href="#">entidad</a> .                                                                                                                                                                                                                       | Entidad de IoT TwinMaker         | AWS::IoTTwinMaker::Entity            |

| Servicio de AWS                         | Descripción                                                                                                                  | Tipo de recurso (consola)           | resources.type value                |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| AWS IoT TwinMaker                       | Actividad de la API de IoT TwinMaker en un <a href="#">espacio de trabajo</a> .                                              | Espacio de trabajo de IoT TwinMaker | AWS::IoT::TwinMaker::Workspace      |
| Amazon Kendra Intelligent Ranking       | Actividad de la API de Amazon Kendra Intelligent Ranking en los <a href="#">planes de ejecución de nuevas puntuaciones</a> . | Kendra Ranking                      | AWS::Kendra::Ranking::ExecutionPlan |
| Amazon Keyspaces (for Apache Cassandra) | <a href="#">Actividad de la API de Amazon Keyspaces</a> en una tabla.                                                        | Tabla de Cassandra                  | AWS::Cassandra::Table               |
| Amazon Keyspaces (for Apache Cassandra) | Actividad de la API de Amazon Keyspaces (para Apache Cassandra) en transmisiones de Cassandra CDC.                           | Transmisiones de Cassandra CDC      | AWS::Cassandra::Stream              |
| Amazon Kinesis Data Streams             | Actividad de la API de Kinesis Data Streams en los <a href="#">flujos</a> .                                                  | Flujo de Kinesis                    | AWS::Kinesis::Stream                |
| Amazon Kinesis Data Streams             | Actividad de la API de Kinesis Data Streams en los <a href="#">consumidores de flujos</a> .                                  | Consumidor de flujos de Kinesis     | AWS::Kinesis::StreamConsumer        |

| Servicio de AWS              | Descripción                                                                                                  | Tipo de recurso (consola)                 | resources.type value                |
|------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------|
| Amazon Kinesis Video Streams | Actividad de la API de Kinesis Video Streams en transmisiones de video, como llamadas a GetMedia y PutMedia. | Kinesis Video Streams                     | AWS::KinesisVideo::Stream           |
| Amazon Kinesis Video Streams | Actividad de la API del canal de señalización de video de Kinesis Video Streams.                             | Canal de señalización de video de Kinesis | AWS::KinesisVideo::SignalingChannel |
| AWS Lambda                   | Actividad de ejecución de funciones de AWS Lambda (la API Invoke).                                           | Lambda                                    | AWS::Lambda::Function               |
| Mapas de Amazon Location     | Actividad de la API de mapas de Amazon Location                                                              | Mapas geográficos                         | AWS::GeoMaps::Provider              |
| Amazon Location Places       | Actividad de la API de Amazon Location Places.                                                               | Lugares geográficos                       | AWS::GeoPlaces::Provider            |
| Rutas de Amazon Location     | Actividad de la API de rutas de Amazon Location                                                              | Rutas geográficas                         | AWS::GeoRoutes::Provider            |
| Amazon Machine Learning      | Actividad de la API de machine learning en modelos de ML.                                                    | MLModel de machine learning               | AWS::MachineLearning::MLModel       |

| Servicio de AWS                              | Descripción                                                                                                                       | Tipo de recurso (consola) | resources.type value                  |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------------------|
| Amazon Managed Blockchain                    | Actividad de la API de Amazon Managed Blockchain en una red.                                                                      | Red de Managed Blockchain | AWS::ManagedBlockchain::Network       |
| Amazon Managed Blockchain                    | Llamadas JSON-RPC de <a href="#">Amazon Managed Blockchain</a> en nodos de Ethereum, como eth_getBalance o eth_getBlockByNumber . | Managed Blockchain        | AWS::ManagedBlockchain::Node          |
| Amazon Managed Blockchain Query              | Actividad de la API de Amazon Managed Blockchain Query.                                                                           | Managed Blockchain Query  | AWS::ManagedBlockchainQuery::QueryAPI |
| Amazon Managed Workflows para Apache Airflow | Actividad de la API de Amazon MWAA en entornos.                                                                                   | Managed Apache Airflow    | AWS::MWAA::Environment                |
| 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              |



| Servicio de AWS          | Descripción                                                                   | Tipo de recurso (consola)                     | resources.type value             |
|--------------------------|-------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------|
| Amazon One Enterprise    | Actividad de la API de Amazon One Enterprise en una clave de usuario.         | Clave de usuario de Amazon One                | AWS::One::UKey                   |
| Amazon One Enterprise    | Actividad de la API de Amazon One Enterprise en los usuarios.                 | Usuario de Amazon One                         | AWS::One::User                   |
| AWS Payment Cryptography | Actividad de la API de AWS Payment Cryptography en los alias.                 | Alias de Payment Cryptography                 | AWS::PaymentCryptography::Alias  |
| AWS Payment Cryptography | Actividad de la API de AWS Payment Cryptography en las claves.                | Clave de Payment Cryptography                 | AWS::PaymentCryptography::Key    |
| Amazon Pinpoint          | Actividad de la API de Amazon Pinpoint en aplicaciones de segmentación móvil. | Aplicación de segmentación móvil              | AWS::Pinpoint::App               |
| AWS Private CA           | Conector AWS Private CA para la actividad de la API de Active Directory.      | AWS Private CA Conector para Active Directory | AWS::PCAConnectorAD::Connector   |
| AWS Private CA           | Conector de AWS Private CA para la actividad de la API de SCEP.               | AWS Private CA Conector para SCEP             | AWS::PCAConnectorSCEP::Connector |

| Servicio de AWS    | Descripción                                                                      | Tipo de recurso (consola)            | resources.type value          |
|--------------------|----------------------------------------------------------------------------------|--------------------------------------|-------------------------------|
| Amazon Q Apps      | Actividad de la API de datos en <a href="#">Amazon Q Apps</a> .                  | Amazon Q Apps                        | AWS::QApps::QApp              |
| Amazon Q Apps      | Actividad de la API de datos en las sesiones de Amazon Q Apps.                   | Sesión de Amazon Q App               | AWS::QApps::QAppSession       |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en una aplicación.      | Aplicación de Amazon Q Business      | AWS::QBusiness::Application   |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en un origen de datos.  | Origen de datos de Amazon Q Business | AWS::QBusiness::DataSource    |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en un índice.           | Índice de Amazon Q Business          | AWS::QBusiness::Index         |
| Amazon Q Business  | <a href="#">Actividad de la API de Amazon Q Business</a> en una experiencia web. | Experiencia web de Amazon Q Business | AWS::QBusiness::WebExperience |
| Amazon Q Business  | Actividad de la API de integración de Amazon Q Business.                         | Integración de Amazon Q Business     | AWS::QBusiness::Integration   |
| Amazon Q Developer | Actividad de la API de Amazon Q Developer en una integración.                    | Integración para Q Developer         | AWS::QDeveloper::Integration  |

| Servicio de AWS     | Descripción                                                                                                 | Tipo de recurso (consola)                  | resources.type value             |
|---------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------|----------------------------------|
| Amazon Q Developer  | <a href="#">Actividad de la API de Amazon Q Developer en investigaciones operativas.</a>                    | Grupos de investigación de AIOps           | AWS::AIOps::InvestigationGroup   |
| Amazon Quick Suite  | Actividad de la API de Amazon Quick Suite en un conector de acciones.                                       | AWS Acciones de QuickSuite de              | AWS::Quicksight::ActionConnector |
| Amazon Quick Suite  | Actividad de la API de flujo de Amazon Quick Suite.                                                         | AWS::Quicksight::Flow                      | AWS::Quicksight::Flow            |
| Amazon Quick Suite  | Actividad de la API de FlowSession de Amazon Quick Suite.                                                   | AWS::Quicksight::FlowSession               | AWS::Quicksight::FlowSession     |
| Amazon SageMaker AI | Actividad de <a href="#">InvokeEndpointWithResponseStream</a> de Amazon SageMaker AI en puntos de conexión. | Punto de conexión de SageMaker AI          | AWS::SageMaker::Endpoint         |
| Amazon SageMaker AI | Actividad de la API de Amazon SageMaker AI en los almacenes de características.                             | Almacén de características de SageMaker AI | AWS::SageMaker::FeatureGroup     |

| Servicio de AWS             | Descripción                                                                                                              | Tipo de recurso (consola)                                        | resources.type value                     |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------|
| Amazon SageMaker AI         | Actividad de la API de Amazon SageMaker AI en los <a href="#">componentes del registro de seguimiento experimental</a> . | Componente de prueba del experimento de métricas de SageMaker AI | AWS::SageMaker::ExperimentTrialComponent |
| Amazon SageMaker AI         | Actividad de la API MLFlow de Amazon SageMaker AI.                                                                       | MLflow de Sagemaker                                              | AWS::SageMaker::MlflowTrackingServer     |
| AWS Signer                  | Actividad de la API de Signer sobre el trabajo de firma.                                                                 | Trabajo de firma de Signer                                       | AWS::Signer::SigningJob                  |
| AWS Signer                  | Actividad de la API de Signer sobre los trabajos de firma.                                                               | Perfil de firma del Signer                                       | AWS::Signer::SigningProfile              |
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en conjuntos de configuraciones.                         | Conjunto de configuración de SES                                 | AWS::SES::ConfigurationSet               |
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en identidades de correo electrónico.                    | Identidad de SES                                                 | AWS::SES::EmailIdentity                  |

| Servicio de AWS             | Descripción                                                                        | Tipo de recurso (consola)            | resources.type value             |
|-----------------------------|------------------------------------------------------------------------------------|--------------------------------------|----------------------------------|
| Amazon Simple Email Service | Actividad de la API de Amazon Simple Email Service (Amazon SES) en plantillas.     | Plantilla de SES                     | AWS::SES::Template               |
| Amazon SimpleDB             | Actividad de la API de Amazon SimpleDB en los dominios.                            | Dominio de SimpleDB                  | AWS::SDB::Domain                 |
| AWS Step Functions          | <a href="#">Actividad de la API de Step Functions</a> en las actividades.          | Step Functions                       | AWS::StepFunctions::Activity     |
| AWS Step Functions          | <a href="#">Actividad de la API de Step Functions</a> en una máquina de estado.    | Máquina de estado de Step Functions  | AWS::StepFunctions::StateMachine |
| AWS Systems Manager         | <a href="#">Actividad de la API de Systems Manager</a> en los canales de control.  | Systems Manager                      | AWS::SSMMessages::ControlChannel |
| AWS Systems Manager         | Actividad de la API de Systems Manager sobre las evaluaciones de impacto.          | Evaluación de impacto de SSM         | AWS::SSM::ExecutionPreview       |
| AWS Systems Manager         | <a href="#">Actividad de la API de Systems Manager</a> en los nodos administrados. | Nodo administrado de Systems Manager | AWS::SSM::ManagedNode            |

| Servicio de AWS                     | Descripción                                                                                    | Tipo de recurso (consola)                | resources.type value                  |
|-------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------------|
| Amazon Timestream                   | Actividad de la API <a href="#">Query</a> de Amazon Timestream en las bases de datos.          | Base de datos de Timestream              | AWS::Timestream::Database             |
| Amazon Timestream                   | Actividad de la API de Amazon Timestream en los puntos de conexión regionales.                 | Punto de conexión regional de Timestream | AWS::Timestream::RegionalEndpoint     |
| Amazon Timestream                   | Actividad de la API <a href="#">Query</a> 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 |
| Cliente ligero de Amazon WorkSpaces | Actividad de la API de cliente ligero de WorkSpaces en un dispositivo.                         | Dispositivo de cliente ligero            | AWS::ThinClient::Device               |
| Cliente ligero de Amazon WorkSpaces | Actividad de la API de cliente ligero de WorkSpaces en un entorno.                             | Entorno de cliente ligero                | AWS::ThinClient::Environment          |
| AWS X-Ray                           | <a href="#">Actividad de la API de X-Ray</a> en los <a href="#">registros de seguimiento</a> . | Registros de seguimiento de X-Ray        | AWS::XRay::Trace                      |

Para registrar eventos de datos de CloudTrail, debe agregar explícitamente cada tipo de recurso cuya actividad desee recopilar. Para obtener más información, consulte [Creación de un registro de seguimiento con la consola de CloudTrail](#) y [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#).

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, las funciones AWS Lambda y las tablas de DynamoDB son regionales.

Se aplican cargos adicionales para registrar eventos de datos. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## 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 `amzn-s3-demo-bucket`. En este ejemplo, el usuario de CloudTrail especificó un prefijo vacío y la opción que permite registrar eventos de datos de Read (Lectura) y Write (Escritura).

1. Un usuario carga un objeto en `amzn-s3-demo-bucket`.
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 usuario de CloudTrail especificó un bucket de S3 con un prefijo vacío, se registran los eventos que tienen lugar en cualquiera de los objetos de dicho bucket. El registro de seguimiento o almacén de datos de eventos procesa y registra el evento.
3. Otro usuario carga un objeto en `amzn-s3-demo-bucket2`.
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 usuario de CloudTrail especificó un bucket de S3 llamado `amzn-s3-demo-`

bucket3, con el prefijo *my-images* y la opción que únicamente permite registrar eventos de datos de Escritura.

1. Un usuario elimina un objeto que comienza con el prefijo *my-images* del bucket; por ejemplo `arn:aws:s3:::amzn-s3-demo-bucket3/my-images/example.jpg`.
2. La operación de API `DeleteObject` es una API de nivel de objetos de Amazon S3. Se registra como un evento de datos *Write* (Escritura) 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:::amzn-s3-demo-bucket3/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:::amzn-s3-demo-bucket3/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 datos de lectura en CloudTrail y el registro de seguimiento o almacén de datos de eventos no está configurado para 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 envía los registros, el evento `PutObject` 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 evitar registrar eventos de datos para el bucket de Amazon S3 en el que recibe los archivos de registros si configura un registro de seguimiento para registrar todos los eventos de datos de Amazon S3 de su cuenta de AWS, considere la posibilidad de configurar el envío de archivos de registros a un bucket de Amazon S3 que pertenezca a otra cuenta de AWS. Para obtener más información, consulte [Recepción de archivos de registro de CloudTrail de varias cuentas](#).

## Registrar eventos de datos para objetos de S3 en otras cuentas de AWS

Cuando configure el registro de seguimiento para que registre eventos de datos, también puede indicar los objetos de S3 que pertenecen a otras cuentas de AWS. Cuando un evento se produce en un objeto indicado, CloudTrail evalúa si el evento coincide con cualquier registro de seguimiento en 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 dos cuentas de AWS configuran 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 `amzn-s3-demo-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. Debido a que ahora hay dos copias del evento (una registrada en el registro de seguimiento de Bob y otra en el suyo), CloudTrail cobra 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. Dado que el evento no se produce en la cuenta de Bob, y que no posee el bucket de S3, el registro de seguimiento de Bob no registra el evento. CloudTrail cobra solo una copia de este evento de datos.

Ejemplo: registrar eventos de datos para todos los buckets, incluido un bucket de S3 utilizado por dos cuentas de AWS

En el ejemplo siguiente se muestra el comportamiento de registro cuando `Select all S3 buckets in your account` (Seleccionar todos los buckets de S3 en su cuenta) está habilitado para los registros de seguimiento que recopilan eventos de datos en una cuenta de AWS.

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. Dado que ahora

hay dos copias del evento (una registrada en el registro de seguimiento de Bob y otra en el suyo), 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. Dado que el evento no se produce en la cuenta de Bob, y que no posee el bucket de S3, el registro de seguimiento de Bob no registra el evento. CloudTrail cobra solo una copia de este evento de datos en su 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. Dado que ella es quien llama a la API, CloudTrail registra un evento de datos en su registro de seguimiento. 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, recibirá un evento en su registro de seguimiento sobre la operación `GetObject` que Mary llamó. CloudTrail cobra a su cuenta y a la cuenta de Mary cada copia del evento de datos: una en el registro de seguimiento de Mary y otra, en la suya.

## 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 llamado `amzn-s3-demo-bucket1` recibe los eventos de solo lectura y un segundo bucket, `amzn-s3-demo-bucket2`, aquellos de solo escritura.

1. Usted crea un registro de seguimiento y elige el bucket de S3 llamado `amzn-s3-demo-bucket1` 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 el bucket de S3 `amzn-s3-demo-bucket2` 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 `amzn-s3-demo-bucket1`.
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 `amzn-s3-demo-bucket2`.

## Registrar eventos de datos con la Consola de administración de AWS

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 Consola de administración de AWS. Para obtener información acerca de cómo crear un almacén de datos de eventos para registrar eventos de datos, consulte [Creación de un almacén de datos de eventos para eventos de CloudTrail con la consola](#). Para obtener más información sobre cómo crear un registro de seguimiento para registrar eventos de datos, consulte [Creación de un registro de seguimiento con la consola](#).

En el caso de los registros de seguimiento, los pasos para registrar los eventos de datos varían en función de si utiliza selectores de eventos avanzados o selectores de eventos básicos. Con los

selectores de eventos avanzados puede registrar eventos de datos de todos los tipos de recursos, pero si utiliza selectores de eventos básicos, solo podrá registrar eventos de datos de buckets de Amazon S3 y objetos de buckets, funciones de AWS Lambda y tablas de Amazon DynamoDB.

Actualizar un almacén de datos de eventos existente para registrar los eventos de datos mediante la consola

Utilice los siguientes procedimientos para actualizar un almacén de datos de eventos existente para registrar los eventos de datos. Para obtener más información sobre la utilización de selectores de eventos avanzados, consulte [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#) en este tema.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail 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 eventos de CloudTrail. No puede habilitar los eventos de datos en los almacenes de datos de eventos de CloudTrail para elementos de configuración de AWS Config, eventos de CloudTrail Insights ni eventos que no son de AWS.

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 Tipo de recurso, elija el tipo de recurso en el que desea registrar los eventos de datos.
7. Elija una plantilla de selector de registros. Puede elegir una plantilla predefinida o elegir Personalizar para definir sus propias condiciones de recopilación de eventos.

Puede elegir entre las siguientes plantillas predefinidas:

- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
- Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.

- Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
  - Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
  - Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).
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. Si seleccionó Personalizado, en los selectores de eventos avanzados se crea una expresión basada en los valores de los campos de los selectores de eventos avanzados.

 Note

Los selectores no admiten el uso de caracteres comodín como `*`. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

a. Elija uno de los siguientes campos.

- **readOnly**: `readOnly` se puede establecer en `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 utilizarlo para incluir o excluir cualquier evento de datos registrado en CloudTrail, como `PutBucket`, `GetItem` o `GetSnapshotBlock`.
- **eventSource**: el tipo de evento que se va a incluir o excluir. Este campo puede utilizar cualquier operador.

- **eventType**: el tipo de evento que se va a incluir o excluir. Por ejemplo, puede establecer este campo en no igual a `AwsServiceEvent` para excluir [Servicio de AWSEventos de](#) . Para obtener una lista de los tipos de eventos, consulte [eventType](#) en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).
- **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de la Consola de administración de AWS. Este campo se puede establecer como igual o no igual con un valor de `true`.
- **userIdentity.arn**: incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- **resources.ARN**: puede utilizar cualquier operador con `resources.ARN`, pero si utiliza es igual a o no es igual a, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo especificado en la plantilla como el valor de `resources.type`.

 Note

No puede usar el campo `resources.ARN` para filtrar los tipos de recursos que no tienen ARN.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte [Acciones, recursos y claves de condición para los Servicios de AWS](#) en la Referencia de autorizaciones de servicio.

- 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 eventos de datos de dos buckets de S3 de los eventos de datos registrados en su almacén de datos de eventos, puede establecer el campo en `resources.ARN`, configurar el operador en no comienza por y, a continuación, pegar un ARN de bucket 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.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- 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 **Agregar tipo de evento de datos**. Repita el paso 6 hasta este paso a fin de configurar selectores de eventos avanzados para otro tipo de recursos.
11. Una vez que haya revisado y verificado las elecciones, seleccione **Guardar cambios**.

Actualizar un registro de seguimiento para registrar eventos de datos con selectores de eventos avanzados mediante la consola

En la Consola de administración de AWS, si su registro de seguimiento utiliza selectores de eventos avanzados, puede seleccionar 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 sobre la utilización de selectores de eventos avanzados, consulte [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#) en este tema.

1. En las páginas **Panel** o **Registros de seguimiento** de la consola de CloudTrail, seleccione el registro de seguimiento que desea 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 **Tipo de recurso**, elija el tipo de recurso en el que desea registrar los eventos de datos.
5. Elija una plantilla de selector de registros. Puede elegir una plantilla predefinida o elegir **Personalizar** para definir sus propias condiciones de recopilación de eventos.

Puede elegir entre las siguientes plantillas predefinidas:



- Registrar todos los eventos: elija esta plantilla para registrar todos los eventos.
- Registrar solo eventos de lectura: elija esta plantilla para registrar solo eventos de lectura. Los eventos de solo lectura son eventos que no cambian el estado de un recurso, como los eventos `Get*` o `Describe*`.
- Registrar solo eventos de escritura: elija esta plantilla para registrar solo eventos de escritura. Los eventos de escritura agregan, cambian o eliminan recursos, atributos o artefactos, como eventos `Put*`, `Delete*` o `Write*`.
- Registrar solo eventos de la Consola de administración de AWS: elija esta plantilla para registrar solo los eventos que se originan en la Consola de administración de AWS.
- Excluir eventos iniciados de Servicio de AWS: elija esta plantilla para excluir los eventos de Servicio de AWS que tienen un `eventType` de `AwsServiceEvent` y los eventos iniciados con roles vinculados a Servicio de AWS (SLR).

#### Note

Elegir una plantilla predefinida para los buckets de S3 permite el registro de eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en un bucket que pertenezca a otra cuenta de 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 crea un registro de seguimiento en todas las regiones, elegir una plantilla predefinida para las funciones Lambda permite 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 un registro de seguimiento para una sola región (en el caso de los registros de seguimiento, solo puede hacerlo mediante la AWS CLI), esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función de

Lambda que cree en esa región después de crear el registro de seguimiento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones. El registrar eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en una función que pertenezca a otra cuenta de AWS.

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. Si seleccionó Personalizado, en los selectores de eventos avanzados se crea una expresión basada en los valores de los campos de los selectores de eventos avanzados.

 Note

Los selectores no admiten el uso de caracteres comodín como \*. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

- a. Elija uno de los siguientes campos.

- **readOnly**: `readOnly` se puede establecer en es igual a con el valor `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 utilizarlo para incluir o excluir cualquier evento de datos registrado en CloudTrail, como `PutBucket`, `GetItem` o `GetSnapshotBlock`.
- **eventSource**: el tipo de evento que se va a incluir o excluir. Este campo puede utilizar cualquier operador.
- **eventType**: el tipo de evento que se va a incluir o excluir. Por ejemplo, puede establecer este campo en no igual a `AwsServiceEvent` para excluir [Servicio de AWSEventos](#)

[de](#) . Para obtener una lista de los tipos de eventos, consulte [eventType](#) en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

- **sessionCredentialFromConsole**: incluya o excluya los eventos que se originan en una sesión de la Consola de administración de AWS. Este campo se puede establecer como igual o no igual con un valor de `true`.
- **userIdentity.arn**: incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- **resources.ARN**: puede utilizar cualquier operador con `resources.ARN`, pero si utiliza `es igual a` o `no es igual a`, el valor debe coincidir exactamente con el ARN de un recurso válido del tipo especificado en la plantilla como el valor de `resources.type`.

 Note

No puede usar el campo `resources.ARN` para filtrar los tipos de recursos que no tienen ARN.

Para obtener más información sobre los formatos del ARN de los recursos de eventos de datos, consulte [Acciones, recursos y claves de condición para los Servicios de AWS](#) en la Referencia de autorizaciones de servicio.

- 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 eventos de datos de dos buckets de S3 de los eventos de datos registrados en su almacén de datos de eventos, puede establecer el campo en `resources.ARN`, configurar el operador en `no comienza por` y, a continuación, pegar un ARN de bucket 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.

Para obtener información sobre cómo evalúa CloudTrail varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

 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.

- 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 **Agregar tipo de evento de datos**. Repita los 4 pasos hasta este paso a fin de configurar selectores de eventos avanzados para el tipo de recursos.
9. Una vez que haya revisado y verificado las elecciones, seleccione **Guardar cambios**.

Actualizar un registro de seguimiento para registrar eventos de datos con selectores de eventos básicos mediante la consola

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 Consola de administración de AWS 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 y elija el nombre del registro de seguimiento.

 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

Conservar la opción predeterminada All current and future S3 buckets (Todos los buckets de S3 actuales y futuros) permite registrar los eventos de datos de todos los buckets que haya actualmente en la cuenta de AWS, así como de cualquier otro bucket que pudiera crear después de generar el registro de seguimiento. Esta opción habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en un bucket que pertenezca a otra cuenta de AWS.

Si crea un registro de seguimiento para una única región (mediante la AWS CLI), la opción Select all S3 buckets in your account (Seleccionar todos los buckets de S3 de la cuenta) habilita el registro de eventos de datos de todos los buckets que estén en la misma región que el registro de seguimiento, así como de cualquier otro bucket que pudiera crear posteriormente en esa región. No registrará los eventos de datos de los buckets de Amazon S3 en otras regiones de la cuenta de AWS.

- 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 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 un registro de seguimiento para una sola región (mediante la AWS CLI), esta opción habilita el registro de eventos de datos de todas las funciones que se encuentran actualmente en esa región en la cuenta de AWS, así como de cualquier función Lambda que cree en esa región después de crear el registro de seguimiento. No habilita el registro de eventos de datos de las funciones Lambda creadas en otras regiones.

El registrar eventos de datos de todas las funciones habilita también el registro de la actividad de eventos de datos realizada por cualquier usuario o rol de su cuenta de AWS, aunque esta se realice en una función que pertenezca a otra cuenta de AWS.

- 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 en la consola de CloudTrail cuando cree un registro de seguimiento. 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 [Administración de registros de seguimiento con la AWS CLI](#).

7. Para agregar otro tipo de datos en el que registrar eventos de datos, elija 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. Seleccione Save changes (Guardar cambios).

## Registrar eventos de datos 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 datos con la AWS CLI.

### Temas

- [Registro de eventos de datos para registros de seguimiento con la AWS CLI](#)

- [Registro de eventos de datos para los almacenes de datos de eventos con la AWS CLI](#)

## Registro de eventos de datos para registros de seguimiento con la AWS CLI

Puede configurar sus registros de seguimiento para que registren los eventos de administración y los de datos con la AWS CLI.

### 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 compatibles del selector de eventos avanzados](#), así podrá registrar solo los eventos de datos que le interesen. Para obtener más información sobre la configuración de estos campos, consulte [AdvancedFieldSelector](#) en la Referencia de la API de AWS CloudTrail y [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#) en esta guía.



Para consultar si su registro de seguimiento está registrando los eventos de administración y de datos, ejecute el comando [get-event-selectors](#).

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

El comando devuelve los selectores de eventos del registro de seguimiento.

## Temas

- [Registrar los eventos de datos de los registros de seguimiento mediante selectores de eventos avanzados](#)
- [Registrar 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 de los registros de seguimiento 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 un registro de seguimiento denominado *TrailName* a fin de incluir eventos de administración de lectura y escritura (se omite el selector `readOnly`), eventos de datos `PutObject` y `DeleteObject` de todas las combinaciones de bucket/prefijo de Amazon S3, excepto para un bucket llamado `amzn-s3-demo-bucket` y eventos de datos para una función de AWS Lambda denominada `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:::amzn-s3-demo-bucket/"] }
    ]
  },
  {
    "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:::amzn-s3-demo-bucket/" ]
    },
  ],
},
{
  "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"

```

}

Registrar 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::amzn-s3-demo-bucket/"] }
    ]
  }
]
```

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::amzn-s3-demo-bucket/"
        ]
    }
]
}
]
}
}

```

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 se crea un registro de seguimiento mediante la AWS CLI, un registro de seguimiento registra todos los eventos de administración. De manera 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:::amzn-s3-demo-bucket1/prefix",
"arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket1/prefix",
            "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
          ],
          "Type": "AWS::S3::Object"
        }
      ],
    }
  ],
}

```

```
        "ReadWriteType": "All"
      }
    ]
  }
}
```

## Registro de eventos de datos para los almacenes de datos de eventos con la 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.

Puede configurar los selectores de eventos avanzados para que registren eventos de datos en un almacén de datos de eventos. Para obtener una lista con los campos compatibles, consulte [Filtrado de los eventos de datos mediante selectores de eventos avanzados](#).

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 específico](#)
- [Incluir Amazon S3 en los eventos de AWS Outposts](#)

### Incluir todos los eventos de Amazon S3 en un bucket específico

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 de uso general y para que excluya los eventos Servicio de AWS y los eventos que genera bucket-scanner-role userIdentity. 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::amzn-s3-
demo-bucket/"] },

```

```

        { "Field": "userIdentity.arn", "NotStartsWith":
["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]},
        { "Field": "eventType","NotEquals": ["AwsServiceEvent"]}
    ]
}
]'

```

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::amzn-s3-demo-bucket/"
          ]
        },
        {
          "Field": "resources.type",
          "Equals": [
            "AWS::S3::Object"
          ]
        },
        {
          "Field": "userIdentity.arn",
          "NotStartsWith": [
            "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
          ]
        }
      ]
    }
  ]
}

```

```

        "Field": "eventType",
        "NotEquals": [
            "AwsServiceEvent"
        ]
    }
]
},
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"BillingMode": "EXTENDABLE_RETENTION_PRICING",
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2024-11-04T15:57:33.701000+00:00",
"UpdatedTimestamp": "2024-11-20T20:49:21.766000+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"
}
```

## Filtrado de los eventos de datos mediante selectores de eventos avanzados

En esta sección se describe cómo puede usar los selectores de eventos avanzados para crear selectores detallados para registrar los eventos de datos que pueden ayudar a controlar los costos al registrar solo los eventos de datos específicos que le interesen.

Por ejemplo:

- Puede incluir o excluir llamadas a la API específicas si agrega un filtro en el campo `eventName`.
- Puede incluir o excluir el registro de recursos específicos si agrega un filtro en el campo `resources.ARN`. Por ejemplo, si estuviera registrando eventos de datos de S3, podría excluir el registro del bucket de S3 de su registro de seguimiento.
- Puede optar por registrar únicamente los eventos de solo escritura o los eventos de solo lectura si agrega un filtro en el campo `readOnly`.

En la siguiente tabla se describen los campos admitidos para filtrar los eventos de datos. Para obtener una lista de los campos compatibles para cada tipo de evento de CloudTrail, consulte [AdvancedEventSelector](#) en la Referencia de la API de AWS CloudTrail.

| Campo                 | Obligatorio | Operadores válidos                                                            | Descripción                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|-------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eventCategory</b>  | Sí          | Equals                                                                        | Este campo está configurado en Data para registrar eventos de datos.                                                                                                                                                                                                                                                                                                                                     |
| <b>resources.type</b> | Sí          | Equals                                                                        | Este campo se usa para seleccionar el tipo de recurso cuyos eventos de datos quiere registrar. La tabla <a href="#">Eventos de datos</a> muestra los valores posibles.                                                                                                                                                                                                                                   |
| <b>readOnly</b>       | No          | Equals                                                                        | Se trata de un campo opcional que se utiliza para incluir o excluir eventos de datos en función del valor readOnly. Un valor de true registra eventos de solo lectura. Un valor de false registra eventos de solo escritura. Si no agrega este campo, CloudTrail registra los eventos de lectura y escritura.                                                                                            |
| <b>eventName</b>      | No          | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | Se trata de un campo opcional que se usa para filtrar e incluir o excluir cualquier evento de datos registrado en CloudTrail, como PutBucket o GetSnapshotBlock .<br><br>Si utiliza la AWS CLI, puede especificar varios valores separando cada uno con una coma.<br><br>Si utiliza la consola, puede especificar varios valores creando una condición para cada eventName que quiera usar para filtrar. |

| Campo                | Obligatorio | Operadores válidos                                                            | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|-------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>resources.ARN</b> | No          | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | <p>Se trata de un campo opcional que se utiliza para excluir o incluir eventos de datos de un recurso específico proporcionando el <code>resources.ARN</code> . Puede utilizar cualquier operador con <code>resources.ARN</code> , pero si utiliza <code>Equals</code> o <code>NotEquals</code> , el valor debe coincidir exactamente con el ARN de un recurso válido del <code>resources.type</code> especificado. Para registrar todos los eventos de datos de todos los objetos en un bucket de S3 específico, utilice el operador <code>StartsWith</code> e incluya solo el ARN del bucket como valor coincidente.</p> <p>Si utiliza la AWS CLI, puede especificar varios valores separando cada uno con una coma.</p> <p>Si utiliza la consola, puede especificar varios valores creando una condición para cada <code>resources.ARN</code> que quiera usar para filtrar.</p> |

| Campo                               | Obligatorio | Operadores válidos                                                            | Descripción                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eventSource</b>                  | No          | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | Puede usarlo para incluir o excluir orígenes de eventos específicos. El <code>eventSource</code> suele ser una forma abreviada del nombre del servicio sin espacios más <code>.amazonaws.com</code> . Por ejemplo, puede establecer el <code>eventSource</code> <code>Equals</code> en <code>ec2.amazonaws.com</code> para registrar solo los eventos de datos de Amazon EC2. |
| <b>eventType</b>                    | No          | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | El <a href="#">eventType</a> que se va a incluir o excluir. Por ejemplo, puede establecer este campo en <code>NotEquals</code> <code>AwsServiceEvent</code> a fin de excluir <a href="#">eventos de Servicio de AWS</a> .                                                                                                                                                     |
| <b>sessionCredentialFromConsole</b> | No          | Equals<br>NotEquals                                                           | Incluya o excluya los eventos que se originan en una sesión de Consola de administración de AWS. Este campo se puede establecer como <code>Equals</code> o <code>NotEquals</code> con un valor de <code>true</code> .                                                                                                                                                         |

| Campo                   | Obligatorio | Operadores válidos                                                                    | Descripción                                                                                                                                                                             |
|-------------------------|-------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>userIdentity.arn</b> | No          | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br><br>NotStartsWith<br><br>StartsWith | Incluya o excluya eventos para las acciones realizadas por identidades de IAM específicas. Para obtener más información, consulte <a href="#">Elemento userIdentity de CloudTrail</a> . |

Para registrar eventos de datos mediante la consola de CloudTrail, elija la opción Eventos de datos y, a continuación, seleccione el Tipo de recurso que le interese al crear o actualizar un almacén de datos de eventos o registro de seguimiento. La tabla [Eventos de datos](#) muestra los posibles tipos de recurso que puede elegir en la consola de CloudTrail.



**Data events** Info  
 Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

*Advanced event selectors are enabled*  
 Use the following fields for fine-grained control over the data events captured by your trail.

Switch to basic event selectors

▼ Data event: S3 Remove

**Resource type**  
 Choose the resource type for which you want to log data events.
 

S3 ▼

**Log selector template**  

Log all events ▼

**Selector name - optional**  

Enter a name

1,000 character limit

► JSON view

Add data event type

Para registrar eventos de datos con la AWS CLI, configure el parámetro `--advanced-event-selector` para establecer la `eventCategory` igual a `Data` y el valor `resources.type` igual al valor del tipo de recurso cuyos eventos de datos quiere registrar. La tabla [Eventos de datos](#) muestra los tipos de recursos disponibles.

Por ejemplo, si quiere registrar los eventos de datos de todos los grupos de identidades de Cognito, debe configurar el parámetro `--advanced-event-selectors` como se muestra a continuación:

```
--advanced-event-selectors '[
  {
    "Name": "Log Cognito data events on Identity pools",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
    ]
  }
]
```

El ejemplo anterior registra todos los eventos de datos de Cognito en los grupos de identidades. Puede refinar aún más los selectores de eventos avanzados para filtrar por los campos `eventName`, `readOnly` y `resources.ARN` y registrar eventos específicos que le interesen o excluir los que no le interesen.

Puede configurar los selectores de eventos avanzados para filtrar eventos de datos en función de varios campos. Por ejemplo, puede configurar selectores de eventos avanzados para registrar todas las llamadas a las API `PutObject` y `DeleteObject` de Amazon S3, pero excluir el registro de eventos de un bucket de S3 específico, como se muestra en el siguiente ejemplo. Sustituya *amzn-s3-demo-bucket* por el nombre de su bucket.

```
--advanced-event-selectors
'[
  {
    "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:::amzn-s3-demo-
bucket/"] }
    ]
  }
]
```

También puede incluir varias condiciones para un campo. Para obtener información sobre cómo se evalúan varias condiciones, consulte [Cómo evalúa CloudTrail varias condiciones de un campo](#).

Puede utilizar los selectores de eventos avanzados para registrar tanto eventos de administración como de datos. Para registrar los eventos de datos para varios tipos de recursos, agregue una instrucción del selector de campos para cada tipo de recurso cuyos eventos de datos quiera registrar.

#### Note

Los registros de seguimiento pueden usar selectores de eventos avanzados básicos, pero no ambos. Si aplica selectores de eventos avanzados a un registro de seguimiento, se sobrescriben todos los selectores de eventos básicos existentes.

Los selectores no admiten el uso de caracteres comodín como \*. Para hacer coincidir varios valores con una sola condición, puede usar `StartsWith`, `EndsWith`, `NotStartsWith` o `NotEndsWith` a fin de hacer coincidir de manera explícita el principio o el final del campo de evento.

## Temas

- [Cómo evalúa CloudTrail varias condiciones de un campo](#)

- [Ejemplos de la AWS CLI para filtrar de eventos de datos](#)

## Cómo evalúa CloudTrail varias condiciones de un campo

En el caso de los selectores de eventos avanzados, CloudTrail evalúa varias condiciones de un campo de la siguiente manera:

- Los operadores DESELECT se agrupan con AND. Si se cumple alguna de las condiciones del operador DESELECT, el evento no se entrega. Estos son los operadores DESELECT válidos para los selectores de eventos avanzados:
  - NotEndsWith
  - NotEquals
  - NotStartsWith
- Los operadores SELECT se agrupan con OR. Estos son los operadores SELECT válidos para los selectores de eventos avanzados:
  - EndsWith
  - Equals
  - StartsWith
- Las combinaciones de operadores SELECT y DESELECT siguen las reglas anteriores y ambos grupos combinan con AND.

### Ejemplo que muestra varias condiciones para el campo **resources.ARN**

En el siguiente ejemplo, la instrucción del selector de eventos recopila eventos de datos para el tipo de recurso `AWS::S3::Object` y aplica varias condiciones en el campo `resources.ARN`.

```
{
  "Name": "S3Select",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": [
        "Data"
      ]
    },
    {
      "Field": "resources.type",
```

```
    "Equals": [
      "AWS::S3::Object"
    ],
  },
  {
    "Field": "resources.ARN",
    "Equals": [
      "arn:aws:s3:::amzn-s3-demo-bucket/object1"
    ],
    "StartsWith": [
      "arn:aws:s3:::amzn-s3-demo-bucket/"
    ],
    "EndsWith": [
      "object3"
    ],
    "NotStartsWith": [
      "arn:aws:s3:::amzn-s3-demo-bucket/deselect"
    ],
    "NotEndsWith": [
      "object5"
    ],
    "NotEquals": [
      "arn:aws:s3:::amzn-s3-demo-bucket/object6"
    ]
  }
]
```

En el ejemplo anterior, los eventos de datos de Amazon S3 para el recurso `AWS::S3::Object` se entregarán si:

1. No se cumple ninguna de estas condiciones del operador **DESELECT**:

- el campo `resources.ARN` **NotStartsWith** el valor `arn:aws:s3:::amzn-s3-demo-bucket/deselect`
- el campo `resources.ARN` **NotEndsWith** el valor `object5`
- el campo `resources.ARN` **NotEquals** el valor `arn:aws:s3:::amzn-s3-demo-bucket/object6`

2. Se cumple al menos una de estas condiciones del operador **SELECT**:

- el campo `resources.ARN` **Equals** el valor `arn:aws:s3:::amzn-s3-demo-bucket/object1`

- el campo `resources.ARN` `StartsWith` el valor `arn:aws:s3:::amzn-s3-demo-bucket/`
- el campo `resources.ARN` `EndsWith` el valor `object3`

Según la lógica de evaluación:

1. Los eventos de datos de `amzn-s3-demo-bucket/object1` se entregarán porque coincide con el valor del operador `Equals` y no coincide con ninguno de los valores de los operadores `NotStartsWith`, `NotEndsWith` y `NotEquals`.
2. El evento de datos de `amzn-s3-demo-bucket/object2` se entregará porque coincide con el valor del operador `StartsWith` y no coincide con ninguno de los valores de los operadores `NotStartsWith`, `NotEndsWith` y `NotEquals`.
3. Los eventos de datos de `amzn-s3-demo-bucket/object3` se entregarán porque coincide con el operador `EndsWith` y no coincide con ninguno de los valores de los operadores `NotStartsWith`, `NotEndsWith` y `NotEquals`.
4. Los eventos de datos de `arn:aws:s3:::amzn-s3-demo-bucket/deselectObject4` no se entregarán porque coincide con la condición de `NotStartsWith`, aunque coincida con la condición del operador `StartsWith`.
5. Los eventos de datos de `arn:aws:s3:::amzn-s3-demo-bucket/object5` no se entregarán porque coincide con la condición de `NotEndsWith`, aunque coincida con la condición del operador `StartsWith`.
6. Los eventos de datos de `arn:aws:s3:::amzn-s3-demo-bucket/object6` no se entregarán porque coincide con la condición del operador `NotEquals`, aunque coincida con la condición del operador `StartsWith`.

## Ejemplos de la AWS CLI para filtrar de eventos de datos

En esta sección, se ofrecen ejemplos de la AWS CLI en los que se muestran cómo filtrar los eventos de datos en distintos campos. Para ver otros ejemplos de la AWS CLI, consulte [Registrar los eventos de datos de los registros de seguimiento mediante selectores de eventos avanzados](#) y [Registro de eventos de datos para los almacenes de datos de eventos con la AWS CLI](#).

Para obtener información acerca de cómo registrar eventos de datos mediante la consola, consulte [Registrar eventos de datos con la Consola de administración de AWS](#).

Ejemplos:

- [Ejemplo 1: filtrar en el campo eventName](#)
- [Ejemplo 2: filtrar en los campos resources.ARN y userIdentity.arn](#)
- [Ejemplo 3: filtrar los campos resources.type y eventName para excluir los objetos individuales eliminados por un evento DeleteObjects de Amazon S3](#)

### Ejemplo 1: filtrar en el campo **eventName**

En el primer ejemplo, los `--advanced-event-selectors` para los registros de seguimiento están configurados para registrar solo las llamadas a la API de `GetObject`, `PutObject` y `DeleteObject` para los objetos de Amazon S3 en buckets de uso general.

```
aws cloudtrail put-event-selectors \  
--trail-name trailName \  
--advanced-event-selectors '[  
  {  
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Data"] },  
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },  
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }  
    ]  
  }  
'
```

En el siguiente ejemplo se crea un nuevo almacén de datos de eventos que registra los eventos de datos de las API directas de EBS, pero excluye las llamadas a las API `ListChangedBlocks`. Puede utilizar el comando [update-event-data-store](#) para actualizar un almacén de datos de eventos existente.

```
aws cloudtrail create-event-data-store \  
--name "eventDataStoreName"  
--advanced-event-selectors '[  
  {  
    "Name": "Log all EBS Direct API data events except ListChangedBlocks",  
    "FieldSelectors": [  
      { "Field": "eventCategory", "Equals": ["Data"] },  
      { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },  
      { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }  
    ]  
  }  
'
```

```
]'
```

## Ejemplo 2: filtrar en los campos **resources.ARN** y **userIdentity.arn**

En el ejemplo siguiente, se muestra cómo incluir todos los eventos de datos de todos los objetos de Amazon S3 en un bucket de S3 específico de uso general, pero excluir los eventos que genera bucket-scanner-role userIdentity. 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**.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
  {
    "Name": "S3EventSelector",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3::amzn-s3-demo-bucket/"] },
      { "Field": "userIdentity.arn", "NotStartsWith":
        ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
    ]
  }
]'
```

## Ejemplo 3: filtrar los campos **resources.type** y **eventName** para excluir los objetos individuales eliminados por un evento DeleteObjects de Amazon S3

En el ejemplo siguiente, se muestra cómo incluir todos los eventos de datos de todos los objetos de Amazon S3 en un bucket de Amazon S3 específico de uso general, pero excluir los objetos individuales por la operación DeleteObject. El valor de los eventos de S3 para el campo **resources.type** es **AWS::S3::Object**. El valor para el nombre del evento es **DeleteObject**.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \

{
```

```
"Name": "Exclude Events for DeleteObject operation",
"FieldSelectors": [
  {
    "Field": "eventCategory",
    "Equals": [
      "Data"
    ]
  },
  {
    "Field": "resources.type",
    "Equals": [
      "AWS::S3::Object"
    ]
  },
  {
    "Field": "eventName",
    "NotEquals": [
      "DeleteObject"
    ]
  }
],
{
  "Name": "Exclude DeleteObject Events for individual objects deleted by
DeleteObjects Operation",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": [
        "Data"
      ]
    },
    {
      "Field": "resources.type",
      "Equals": [
        "AWS::S3::Object"
      ]
    },
    {
      "Field": "eventName",
      "Equals": [
        "DeleteObject"
      ]
    }
  ],
```



```
{
  "Field": "eventType",
  "NotEquals": [
    "AwsServiceEvent"
  ]
}
]
}
```

] (edited)

## Registrar eventos de datos para la conformidad con AWS Config

Si utiliza paquetes de cumplimiento de AWS Config para ayudar a su empresa a mantener la conformidad con los estándares formalizados, como los requeridos por el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP) o el Instituto Nacional de Estándares y Tecnología (NIST), los paquetes de cumplimiento para los marcos de conformidad generalmente requieren que registre 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.

- [Prácticas operativas recomendadas 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 cumplimiento de muestra disponibles en AWS Config, consulte [Plantillas de ejemplo del paquete de cumplimiento](#) en la Guía para desarrolladores de AWS Config.

## Registro de eventos de datos con los SDK de AWS

Ejecute la operación [GetEventSelectors](#) para saber si el registro de seguimiento está registrando los eventos de datos. Para configurar sus registros de seguimiento para que registren eventos de datos, ejecute la operación [PutEventSelectors](#). Para obtener más información, consulte la [Referencia de la API de AWS CloudTrail](#).

Ejecute la operación [GetEventDataStore](#) para saber si el almacén de datos de eventos está registrando los eventos de datos. Puede configurar sus almacenes de datos de eventos para incluir eventos de datos ejecutando las operaciones [CreateEventDataStore](#) o [UpdateEventDataStore](#) y especificando los selectores de eventos avanzados. Para obtener más información, consulte [Creación, actualización y administración de almacenes de datos de eventos con la AWS CLI](#) y la [AWS CloudTrail API Reference](#).

## Registro de eventos de actividad de la red

Los eventos de actividad de la red de CloudTrail permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Los eventos de actividad de la red muestran información sobre las operaciones de recursos realizadas dentro de una VPC. Por ejemplo, registrar los eventos de actividad de la red puede ayudar a los propietarios de puntos de conexión de VPC a detectar intentos de acceso de credenciales ajenas a su organización a sus puntos de conexión de VPC.

Puede registrar los eventos de actividad de la red para los siguientes servicios:

- AWS AppConfig
- AWS App Mesh
- Amazon Athena
- Intercambio de datos de AWS B2B
- AWS Backup gateway
- Amazon Bedrock
- Administración de facturación y costos
- Calculadora de precios de AWS
- AWS Cost Explorer
- API de control de nube de AWS

- AWS CloudHSM
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Señales de aplicación de CloudWatch
- AWS CodeDeploy
- Amazon Comprehend Medical
- AWS Config
- Exportaciones de datos de AWS
- Amazon Data Firehose
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon EventBridge
- Programador de Amazon EventBridge
- Amazon Fraud Detector
- capa gratuita de AWS
- Amazon FSx
- AWS Glue
- AWS HealthLake
- AWS IoT FleetWise
- AWS IoT Secure Tunneling
- Facturación de AWS
- Amazon Keyspaces (for Apache Cassandra)
- AWS KMS

- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Amazon Personalize
- Amazon Q Business
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon S3

 Note

Amazon S3 no admite [puntos de acceso de varias regiones](#).

- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Storage Gateway
- Administrador de incidentes de AWS Systems Manager
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS Transform
- Amazon Verified Permissions
- Amazon WorkMail

Puede configurar tanto registros de seguimiento como almacenes de datos de eventos para registrar eventos de actividad de la red.

De forma predeterminada, los registros de seguimiento y los almacenes de datos de eventos no registran eventos de actividad de la red. Se aplican cargos adicionales por los eventos de actividad de la red. Para más información, consulte [Precios de AWS CloudTrail](#).

## Contenido

- [Campos de los selectores de eventos avanzados para eventos de actividad de la red](#)
- [Registro de eventos de actividad de la red con la Consola de administración de AWS](#)
  - [Actualización de un registro de seguimiento existente para registrar los eventos de actividad de red](#)
  - [Actualización de un almacén de datos de eventos existente para registrar los eventos de actividad de red](#)
- [Registro de eventos de actividad de la red con la AWS Command Line Interface](#)
- [Ejemplos: Registro de eventos de actividad de la red para registros de seguimiento](#)
  - [Ejemplo: Registrar eventos de actividad de red para las operaciones de CloudTrail](#)
  - [Ejemplo: Registrar eventos VpceAccessDenied de AWS KMS](#)
  - [Ejemplo: registrar los eventos de VpceAccessDenied para Amazon S3](#)
  - [Ejemplo: Registrar eventos VpceAccessDenied de EC2 en un punto de conexión de VPC específico](#)
  - [Ejemplo: registrar todos los eventos de administración y los eventos de actividad de la red para varios orígenes de los eventos](#)
- [Ejemplos: Registro de eventos de actividad de la red de los almacenes de datos de eventos](#)
  - [Ejemplo: Registrar todos los eventos de actividad de red para las operaciones de CloudTrail](#)
  - [Ejemplo: Registrar eventos VpceAccessDenied de AWS KMS](#)
  - [Ejemplo: Registrar eventos VpceAccessDenied de EC2 en un punto de conexión de VPC específico](#)
  - [Ejemplo: registrar los eventos de VpceAccessDenied para Amazon S3](#)
  - [Ejemplo: registrar todos los eventos de administración y los eventos de actividad de la red para varios orígenes de los eventos](#)
- [Registro de eventos con los SDK de AWS](#)

## Campos de los selectores de eventos avanzados para eventos de actividad de la red

Para configurar los selectores de eventos avanzados para registrar los eventos de actividad de la red, especifique el origen de los eventos para el que quiere registrar la actividad. Para configurar selectores de eventos avanzados, puede utilizar los SDK de AWS, la AWS CLI o la consola de CloudTrail.

Son necesarios los siguientes campos de los selectores de eventos avanzados para registrar eventos de actividad de la red:

- `eventCategory`: para registrar eventos de actividad de la red, el valor debe ser `NetworkActivity`. `eventCategory` solo puede usar el operador `Equals`.
- `eventSource`: origen cuyos eventos de actividad de la red quiere que se registren. `eventSource` solo puede usar el operador `Equals`. Si quiere registrar los eventos de actividad de la red para varios orígenes, debe crear un selector de campo independiente para cada origen de los eventos.

Los valores válidos son:

- `appconfig.amazonaws.com`
- `application-signals.amazonaws.com`
- `appmesh.amazonaws.com`
- `athena.amazonaws.com`
- `b2bi.amazonaws.com`
- `backup-gateway.amazonaws.com`
- `bcm-data-exports.amazonaws.com`
- `bcm-pricing-calculator.amazonaws.com`
- `bedrock.amazonaws.com`
- `billing.amazonaws.com`
- `cassandra.amazonaws.com`
- `ce.amazonaws.com`
- `cloudcontrolapi.amazonaws.com`
- `cloudformation.amazonaws.com`
- `cloudhsm.amazonaws.com`

- `cloudtrail.amazonaws.com`
- `codedeploy.amazonaws.com`
- `comprehend.amazonaws.com`
- `comprehendmedical.amazonaws.com`
- `config.amazonaws.com`
- `ds.amazonaws.com`
- `dynamodb.amazonaws.com`
- `ec2.amazonaws.com`
- `ecs.amazonaws.com`
- `elasticfilesystem.amazonaws.com`
- `elasticloadbalancing.amazonaws.com`
- `events.amazonaws.com`
- `firehose.amazonaws.com`
- `frauddetector.amazonaws.com`
- `freetier.amazonaws.com`
- `fsx.amazonaws.com`
- `glue.amazonaws.com`
- `healthlake.amazonaws.com`
- `invoicing.amazonaws.com`
- `iotfleetwise.amazonaws.com`
- `iotsecuredtunneling.amazonaws.com`
- `kms.amazonaws.com`
- `lakeformation.amazonaws.com`
- `lambda.amazonaws.com`
- `license-manager.amazonaws.com`
- `lookoutequipment.amazonaws.com`
- `lookoutvision.amazonaws.com`
- `monitoring.amazonaws.com`
- `personalize.amazonaws.com`
- `qbusiness.amazonaws.com`

- `rds.amazonaws.com`
- `rekognition.amazonaws.com`
- `rolesanywhere.amazonaws.com`
- `s3.amazonaws.com`
- `sagemaker.amazonaws.com`
- `scheduler.amazonaws.com`
- `secretsmanager.amazonaws.com`
- `servicediscovery.amazonaws.com`
- `sns.amazonaws.com`
- `sqs.amazonaws.com`
- `ssm-contacts.amazonaws.com`
- `storagegateway.amazonaws.com`
- `swf.amazonaws.com`
- `textract.amazonaws.com`
- `transcribe.amazonaws.com`
- `transcribestreaming.amazonaws.com`
- `transform.amazonaws.com`
- `translate.amazonaws.com`
- `user-subscriptions.amazonaws.com`
- `verifiedpermissions.amazonaws.com`
- `voiceid.amazonaws.com`
- `workmail.amazonaws.com`
- `workmailmessageflow.amazonaws.com`

Los siguientes campos del selector de eventos avanzado son opcionales:

- `eventName`: acción solicitada por la que quiere filtrar. Por ejemplo, `CreateKey` o `ListKeys`. `eventName` puede usar cualquier operador.
- `errorCode`: código de error solicitado por el que quiere filtrar. Actualmente, el único `errorCode` válido es `VpceAccessDenied`. Solo puede utilizar el operador `Equals` con `errorCode`.



- `vpcEndpointId`: identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con `vpcEndpointId`.

El registro de los eventos de actividad de la red está deshabilitado de forma predeterminada cuando crea un registro de seguimiento o un almacén de datos de eventos. A fin de registrar eventos de actividad de la red de CloudTrail, debe configurar explícitamente cada origen de los eventos cuya actividad desea recopilar.

Se aplican cargos adicionales por el registro de eventos de actividad de la red. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

## Registro de eventos de actividad de la red con la Consola de administración de AWS

Puede actualizar un registro de seguimiento o almacén de datos de eventos existente para registrar los eventos de actividad de red con la consola.

### Temas

- [Actualización de un registro de seguimiento existente para registrar los eventos de actividad de red](#)
- [Actualización de un almacén de datos de eventos existente para registrar los eventos de actividad de red](#)

### Actualización de un registro de seguimiento existente para registrar los eventos de actividad de red

Siga este procedimiento para actualizar un registro de seguimiento existente para registrar los eventos de actividad de red.

#### Note

Se aplican cargos adicionales por el registro de eventos de actividad de la red. Para conocer los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.

2. 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.
3. Si el registro de seguimiento registra eventos de datos mediante selectores de eventos básicos, tendrá que cambiar a selectores de eventos avanzados para registrar los eventos de actividad de la red.

Siga estos pasos para cambiar a selectores de eventos avanzados:

- a. En el área de Eventos de datos, anote los selectores de eventos de datos actuales. Al cambiar a selectores de eventos avanzados, se borrarán todos los selectores de eventos de datos existentes.
  - b. Seleccione Editar y, luego, seleccione Cambiar a selectores de eventos avanzados.
  - c. Vuelva a aplicar las selecciones de eventos de datos mediante selectores de eventos avanzados. Para obtener más información, consulte [Actualizar un registro de seguimiento para registrar eventos de datos con selectores de eventos avanzados mediante la consola](#).
4. En Eventos de actividad de la red, elija Editar.

Para registrar eventos de actividad de la red, aplique estos pasos:

- a. En Origen de eventos de actividad de la red, seleccione el origen de los eventos de actividad de la red.
- b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede optar por registrar todos los eventos de actividad de la red, registrar todos los eventos de acceso denegado a la actividad de la red o seleccionar Personalizar para crear un selector de registro personalizado que filtre por varios campos, como eventName y vpcEndpointId.
- c. (Opcional) Escriba un nombre para identificar el selector. El nombre del selector aparece como Nombre en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
- d. En Selectores de eventos avanzados, cree expresiones mediante la selección de valores para Campo, Operador y Valor. Puede omitir este paso si utiliza una plantilla de registro predefinida.
  - i. Para excluir o incluir eventos de actividad de la red, puede elegir entre los siguientes campos de la consola.

- **eventName** – puede utilizar cualquier operador con eventName. Puede utilizarlo para incluir o excluir cualquier evento, como CreateKey.
  - **errorCode** – puede usarlo para filtrar por un código de error. Actualmente, el único errorCode que se admite es VpceAccessDenied.
  - **vpcEndpointId** – identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con vpcEndpointId.
- ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.
  - iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
- e. Para agregar otro origen de eventos de actividad de la red que quiera registrar, seleccione Agregar selector de eventos de actividad de la red.
  - f. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
5. Elija Guardar cambios para guardar los cambios.

## Actualización de un almacén de datos de eventos existente para registrar los eventos de actividad de red

Siga este procedimiento para actualizar un almacén de datos de eventos existente y registrar los eventos de actividad de la red.

### Note

Solo puede registrar los eventos de actividad de red en los almacenes de datos de eventos de tipo Eventos de CloudTrail.

1. Inicie sesión en la Consola de administración de AWS y abra la consola de CloudTrail en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación izquierdo de la consola de CloudTrail y, en Lake, elija Almacenes de datos de eventos.
3. Elija el nombre del almacén de datos de eventos.
4. En Eventos de actividad de la red, elija Editar.

Para registrar eventos de actividad de la red, aplique estos pasos:

- a. En Origen de eventos de actividad de la red, seleccione el origen de los eventos de actividad de la red.
  - b. Elija una plantilla en la sección Log selector template (Plantilla de selector de registros). Puede optar por registrar todos los eventos de actividad de la red, registrar todos los eventos de acceso denegado a la actividad de la red o seleccionar Personalizar para crear un selector de registro personalizado que filtre por varios campos, como `eventName` y `vpcEndpointId`.
  - c. (Opcional) Escriba un nombre para identificar el selector. El nombre del selector aparece como Nombre en el selector de eventos avanzado y se puede ver si se amplía la vista JSON.
  - d. En Selectores de eventos avanzados, cree expresiones mediante la selección de valores para Campo, Operador y Valor. Puede omitir este paso si utiliza una plantilla de registro predefinida.
    - i. Para excluir o incluir eventos de actividad de la red, puede elegir entre los siguientes campos de la consola.
      - **eventName** – puede utilizar cualquier operador con `eventName`. Puede utilizarlo para incluir o excluir cualquier evento, como `CreateKey`.
      - **errorCode** – puede usarlo para filtrar por un código de error. Actualmente, el único `errorCode` que se admite es `VpceAccessDenied`.
      - **vpcEndpointId** – identifica el punto de conexión de VPC por el que pasó la operación. Puede utilizar cualquier operador con `vpcEndpointId`.
    - ii. En cada campo, seleccione + Condición para agregar tantas condiciones como necesite, hasta un máximo de 500 valores especificados para todas las condiciones.
    - iii. Elija + Field (+ campos) para agregar campos adicionales según sea necesario. Para evitar errores, no establezca valores contradictorios ni duplicados en los campos.
  - e. Para agregar otro origen de eventos de actividad de la red que quiera registrar, seleccione Agregar selector de eventos de actividad de la red.
  - f. De manera opcional, expanda JSON view (Vista JSON) para ver los selectores de eventos avanzados como un bloque JSON.
5. Elija Guardar cambios para guardar los cambios.

# Registro de eventos de actividad de la red con la AWS Command Line Interface

Puede configurar los registros de seguimiento o los almacenes de datos de eventos para que registren los eventos de actividad de la red con la AWS CLI.

## Temas

- [Ejemplos: Registro de eventos de actividad de la red para registros de seguimiento](#)
- [Ejemplos: Registro de eventos de actividad de la red de los almacenes de datos de eventos](#)

## Ejemplos: Registro de eventos de actividad de la red para registros de seguimiento

Puede configurar los registros de seguimiento para que registren los eventos de actividad de la red con la AWS CLI. Ejecute el comando [put-event-selectors](#) para configurar los selectores de eventos avanzados para su registro de seguimiento.

Para consultar si su registro de seguimiento está registrando los eventos de actividad de la red, ejecute el comando [get-event-selectors](#).

## Temas

- [Ejemplo: Registrar eventos de actividad de red para las operaciones de CloudTrail](#)
- [Ejemplo: Registrar eventos VpceAccessDenied de AWS KMS](#)
- [Ejemplo: registrar los eventos de VpceAccessDenied para Amazon S3](#)
- [Ejemplo: Registrar eventos VpceAccessDenied de EC2 en un punto de conexión de VPC específico](#)
- [Ejemplo: registrar todos los eventos de administración y los eventos de actividad de la red para varios orígenes de los eventos](#)

## Ejemplo: Registrar eventos de actividad de red para las operaciones de CloudTrail

En el siguiente ejemplo se muestra cómo configurar el registro de seguimiento para que incluya todos los eventos de actividad de la red de las operaciones de la API de CloudTrail, como las llamadas `CreateTrail` y `CreateEventDataStore`. El valor del campo `eventSource` es `cloudtrail.amazonaws.com`.

```
aws cloudtrail put-event-selectors /
```

```
--trail-name TrailName /
--region region /
--advanced-event-selectors '[
  {
    "Name": "Audit all CloudTrail API calls through VPC endpoints",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": ["NetworkActivity"]
      },
      {
        "Field": "eventSource",
        "Equals": ["cloudtrail.amazonaws.com"]
      }
    ]
  }
]
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "AdvancedEventSelectors": [
    {
      "Name": "Audit all CloudTrail API calls through VPC endpoints",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "NetworkActivity"
          ]
        },
        {
          "Field": "eventSource",
          "Equals": [
            "cloudtrail.amazonaws.com"
          ]
        }
      ]
    }
  ]
}
```

## Ejemplo: Registrar eventos **VpceAccessDenied** de AWS KMS

En el siguiente ejemplo se muestra cómo configurar el registro de seguimiento para incluir eventos VpceAccessDenied de AWS KMS. En este ejemplo, se establece el campo `errorCode` igual a los eventos VpceAccessDenied y el campo `eventSource` igual a `kms.amazonaws.com`.

```
aws cloudtrail put-event-selectors \  
--region region /  
--trail-name TrailName /  
--advanced-event-selectors '[  
  {  
    "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["NetworkActivity"]  
      },  
      {  
        "Field": "eventSource",  
        "Equals": ["kms.amazonaws.com"]  
      },  
      {  
        "Field": "errorCode",  
        "Equals": ["VpceAccessDenied"]  
      }  
    ]  
  }  
'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{  
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "NetworkActivity"  
          ]  
        },  
      ]  
    },  
  ]  
}
```

```

        {
            "Field": "eventSource",
            "Equals": [
                "kms.amazonaws.com"
            ]
        },
        {
            "Field": "errorCode",
            "Equals": [
                "VpceAccessDenied"
            ]
        }
    ]
}

```

### Ejemplo: registrar los eventos de **VpceAccessDenied** para Amazon S3

En el siguiente ejemplo se muestra cómo configurar el registro de seguimiento para incluir eventos `VpceAccessDenied` de Amazon S3. En este ejemplo, se establece el campo `errorCode` igual a los eventos `VpceAccessDenied` y el campo `eventSource` igual a `s3.amazonaws.com`.

```

aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]

```



```
    ]
  }
]'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
  "AdvancedEventSelectors": [
    {
      "Name": "Log S3 access denied network activity events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "NetworkActivity"
          ]
        },
        {
          "Field": "eventSource",
          "Equals": [
            "s3.amazonaws.com"
          ]
        },
        {
          "Field": "errorCode",
          "Equals": [
            "VpceAccessDenied"
          ]
        }
      ]
    }
  ]
}
```

Ejemplo: Registrar eventos **VpceAccessDenied** de EC2 en un punto de conexión de VPC específico

En el siguiente ejemplo se muestra cómo configurar el registro de seguimiento para incluir eventos VpceAccessDenied de Amazon EC2 para un punto de conexión de VPC específico. En este ejemplo, se establece el campo `errorCode` igual a los eventos VpceAccessDenied, el campo

eventSource igual a `ec2.amazonaws.com` y el `vpcEndpointId` igual al punto de conexión de VPC de interés.

```
aws cloudtrail put-event-selectors \  
--region region /  
--trail-name TrailName /  
--advanced-event-selectors '[  
  {  
    "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["NetworkActivity"]  
      },  
      {  
        "Field": "eventSource",  
        "Equals": ["ec2.amazonaws.com"]  
      },  
      {  
        "Field": "errorCode",  
        "Equals": ["VpceAccessDenied"]  
      },  
      {  
        "Field": "vpcEndpointId",  
        "Equals": ["vpce-example8c1b6b9b7"]  
      }  
    ]  
  }  
'
```

El comando devuelve el siguiente resultado de ejemplo.

```
{  
  "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",  
  "AdvancedEventSelectors": [  
    {  
      "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  
            "NetworkActivity"  
          ]  
        }  
      ]  
    }  
  ]  
}
```

```

    },
    {
      "Field": "eventSource",
      "Equals": [
        "ec2.amazonaws.com"
      ]
    },
    {
      "Field": "errorCode",
      "Equals": [
        "VpceAccessDenied"
      ]
    },
    {
      "Field": "vpcEndpointId",
      "Equals": [
        "vpce-example8c1b6b9b7"
      ]
    }
  ]
}

```

Ejemplo: registrar todos los eventos de administración y los eventos de actividad de la red para varios orígenes de los eventos

En el siguiente ejemplo se configura un registro de seguimiento para registrar los eventos de administración y todos los eventos de actividad de la red para las orígenes de eventos de CloudTrail, Amazon EC2, AWS KMS, AWS Secrets Manager y Amazon S3.

```

aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": ["Management"]
      }
    ]
  }
]

```

```
},
{
  "Name": "Log all network activity events for CloudTrail APIs",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    },
    {
      "Field": "eventSource",
      "Equals": ["cloudtrail.amazonaws.com"]
    }
  ]
},
{
  "Name": "Log all network activity events for EC2",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    },
    {
      "Field": "eventSource",
      "Equals": ["ec2.amazonaws.com"]
    }
  ]
},
{
  "Name": "Log all network activity events for KMS",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    },
    {
      "Field": "eventSource",
      "Equals": ["kms.amazonaws.com"]
    }
  ]
},
{
  "Name": "Log all network activity events for S3",
  "FieldSelectors": [
    {
```

```

        "Field": "eventCategory",
        "Equals": ["NetworkActivity"]
    },
    {
        "Field": "eventSource",
        "Equals": ["s3.amazonaws.com"]
    }
]
},
{
    "Name": "Log all network activity events for Secrets Manager",
    "FieldSelectors": [
        {
            "Field": "eventCategory",
            "Equals": ["NetworkActivity"]
        },
        {
            "Field": "eventSource",
            "Equals": ["secretsmanager.amazonaws.com"]
        }
    ]
}
]'

```

El comando devuelve el siguiente resultado de ejemplo.

```

{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [

```

```

        {
            "Field": "eventCategory",
            "Equals": [
                "NetworkActivity"
            ]
        },
        {
            "Field": "eventSource",
            "Equals": [
                "cloudtrail.amazonaws.com"
            ]
        }
    ]
},
{
    "Name": "Log all network activity events for EC2",
    "FieldSelectors": [
        {
            "Field": "eventCategory",
            "Equals": [
                "NetworkActivity"
            ]
        },
        {
            "Field": "eventSource",
            "Equals": [
                "ec2.amazonaws.com"
            ]
        }
    ]
},
{
    "Name": "Log all network activity events for KMS",
    "FieldSelectors": [
        {
            "Field": "eventCategory",
            "Equals": [
                "NetworkActivity"
            ]
        },
        {
            "Field": "eventSource",
            "Equals": [
                "kms.amazonaws.com"
            ]
        }
    ]
}

```

```

        ]
      }
    ]
  },
  {
    "Name": "Log all network activity events for S3",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "NetworkActivity"
        ]
      },
      {
        "Field": "eventSource",
        "Equals": [
          "s3.amazonaws.com"
        ]
      }
    ]
  },
  {
    "Name": "Log all network activity events for Secrets Manager",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "NetworkActivity"
        ]
      },
      {
        "Field": "eventSource",
        "Equals": [
          "secretsmanager.amazonaws.com"
        ]
      }
    ]
  }
]
}

```

## Ejemplos: Registro de eventos de actividad de la red de los almacenes de datos de eventos

Puede configurar los almacenes de datos de eventos para que incluyan los eventos de actividad de la red 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 actividad de la red. 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 actividad de la red, ejecute el comando [get-event-data-store](#).

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

### Temas

- [Ejemplo: Registrar todos los eventos de actividad de red para las operaciones de CloudTrail](#)
- [Ejemplo: Registrar eventos VpceAccessDenied de AWS KMS](#)
- [Ejemplo: Registrar eventos VpceAccessDenied de EC2 en un punto de conexión de VPC específico](#)
- [Ejemplo: registrar los eventos de VpceAccessDenied para Amazon S3](#)
- [Ejemplo: registrar todos los eventos de administración y los eventos de actividad de la red para varios orígenes de los eventos](#)

Ejemplo: Registrar todos los eventos de actividad de red para las operaciones de CloudTrail

En el siguiente ejemplo se muestra cómo crear un almacén de datos de eventos para que incluya todos los eventos de actividad de la red relacionados con las operaciones de CloudTrail, como las llamadas a CreateTrail y CreateEventDataStore. El valor del campo eventSource se establece en `cloudtrail.amazonaws.com`.

```
aws cloudtrail create-event-data-store \  
--name "EventDataStoreName" \  
--advanced-event-selectors '[  
  {  
    "Name": "Audit all CloudTrail API calls over VPC endpoint",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",
```



```

        "Equals": ["NetworkActivity"]
    },
    {
        "Field": "eventSource",
        "Equals": ["cloudtrail.amazonaws.com"]
    }
]
}
]'

```

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": "Audit all CloudTrail API calls over VPC endpoint",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "NetworkActivity"
          ]
        },
        {
          "Field": "eventSource",
          "Equals": [
            "cloudtrail.amazonaws.com"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "RetentionPeriod": 366,
  "TerminationProtectionEnabled": true,
  "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
  "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}

```

## Ejemplo: Registrar eventos **VpceAccessDenied** de AWS KMS

En el ejemplo siguiente, se muestra cómo crear un almacén de datos de eventos para que incluya eventos de VpceAccessDenied de AWS KMS. En este ejemplo, se establece el campo `errorCode` igual a los eventos VpceAccessDenied y el campo `eventSource` igual a `kms.amazonaws.com`.

```
aws cloudtrail create-event-data-store \  
--name EventDataStoreName \  
--advanced-event-selectors '[  
  {  
    "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["NetworkActivity"]  
      },  
      {  
        "Field": "eventSource",  
        "Equals": ["kms.amazonaws.com"]  
      },  
      {  
        "Field": "errorCode",  
        "Equals": ["VpceAccessDenied"]  
      }  
    ]  
  }  
'
```

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": "Audit AccessDenied AWS KMS events over VPC endpoints",  
      "FieldSelectors": [  
        {  
          "Field": "eventCategory",  
          "Equals": [  

```

```

        "NetworkActivity"
      ],
    },
    {
      "Field": "eventSource",
      "Equals": [
        "kms.amazonaws.com"
      ]
    },
    {
      "Field": "errorCode",
      "Equals": [
        "VpceAccessDenied"
      ]
    }
  ]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
"UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}

```

Ejemplo: Registrar eventos **VpceAccessDenied** de EC2 en un punto de conexión de VPC específico

En el ejemplo siguiente, se muestra cómo crear un almacén de datos de eventos para que incluya eventos de VpceAccessDenied de Amazon EC2 para un punto de conexión de VPC específico. En este ejemplo, se establece el campo `errorCode` igual a los eventos VpceAccessDenied, el campo `eventSource` igual a `ec2.amazonaws.com` y el `vpcEndpointId` igual al punto de conexión de VPC de interés.

```

aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
  {
    "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
    "FieldSelectors": [
      {
        "Field": "eventCategory",

```

```

        "Equals": ["NetworkActivity"]
    },
    {
        "Field": "eventSource",
        "Equals": ["ec2.amazonaws.com"]
    },
    {
        "Field": "errorCode",
        "Equals": ["VpceAccessDenied"]
    },
    {
        "Field": "vpcEndpointId",
        "Equals": ["vpce-example8c1b6b9b7"]
    }
]
}
]'

```

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": "Audit AccessDenied EC2 events over a specific VPC endpoint",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "NetworkActivity"
          ]
        },
        {
          "Field": "eventSource",
          "Equals": [
            "ec2.amazonaws.com"
          ]
        },
        {
          "Field": "errorCode",

```

```

        "Equals": [
            "VpceAccessDenied"
        ],
    },
    {
        "Field": "vpcEndpointId",
        "Equals": [
            "vpce-example8c1b6b9b7"
        ]
    }
]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
"UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}

```

### Ejemplo: registrar los eventos de **VpceAccessDenied** para Amazon S3

En el ejemplo siguiente, se muestra cómo crear un almacén de datos de eventos para que incluya eventos de VpceAccessDenied para Amazon S3. En este ejemplo, se establece el campo `errorCode` igual a los eventos VpceAccessDenied y el campo `eventSource` igual a `s3.amazonaws.com`.

```

aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    }
]

```

```

        "Field": "errorCode",
        "Equals": ["VpceAccessDenied"]
      }
    ]
  }
}'

```

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": "Log S3 access denied network activity events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "NetworkActivity"
          ]
        },
        {
          "Field": "eventSource",
          "Equals": [
            "s3.amazonaws.com"
          ]
        },
        {
          "Field": "errorCode",
          "Equals": [
            "VpceAccessDenied"
          ]
        }
      ]
    }
  ],
  "MultiRegionEnabled": true,
  "OrganizationEnabled": false,
  "RetentionPeriod": 366,
  "TerminationProtectionEnabled": true,
}

```

```
"CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",  
"UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"  
}
```

Ejemplo: registrar todos los eventos de administración y los eventos de actividad de la red para varios orígenes de los eventos

En los siguientes ejemplos, se actualiza un almacén de datos de eventos que actualmente solo registra eventos de administración para también registrar los eventos de actividad de la red de varios orígenes de eventos. Para actualizar un almacén de datos de eventos y agregar selectores de eventos nuevos, ejecute el comando `get-event-data-store` para volver a los selectores de eventos avanzados actuales. A continuación, ejecute el comando `update-event-data-store` y pase el `--advanced-event-selectors` que incluye los selectores actuales además de los selectores nuevos. Para registrar los eventos de actividad de la red para varios orígenes, incluya un selector para cada origen de los eventos que quiere registrar.

```
aws cloudtrail update-event-data-store \  
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-  
f852-4e8f-8bd1-bcf6cEXAMPLE \  
--advanced-event-selectors '[  
  {  
    "Name": "Log all management events",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["Management"]  
      }  
    ]  
  },  
  {  
    "Name": "Log all network activity events for CloudTrail APIs",  
    "FieldSelectors": [  
      {  
        "Field": "eventCategory",  
        "Equals": ["NetworkActivity"]  
      },  
      {  
        "Field": "eventSource",  
        "Equals": ["cloudtrail.amazonaws.com"]  
      }  
    ]  
  },  
]
```

```
{
  "Name": "Log all network activity events for EC2",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    },
    {
      "Field": "eventSource",
      "Equals": ["ec2.amazonaws.com"]
    }
  ]
},
{
  "Name": "Log all network activity events for KMS",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]},
    {
      "Field": "eventSource",
      "Equals": ["kms.amazonaws.com"]
    }
  ]
},
{
  "Name": "Log all network activity events for S3",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    },
    {
      "Field": "eventSource",
      "Equals": ["s3.amazonaws.com"]
    }
  ]
},
{
  "Name": "Log all network activity events for Secrets Manager",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": ["NetworkActivity"]
    }
  ]
}
```



```

    },
    {
      "Field": "eventSource",
      "Equals": ["secretsmanager.amazonaws.com"]
    }
  ]
}
]'

```

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": "Log all management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [
            "Management"
          ]
        }
      ]
    }
  ],
  {
    "Name": "Log all network activity events for CloudTrail APIs",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "NetworkActivity"
        ]
      },
      {
        "Field": "eventSource",
        "Equals": [
          "cloudtrail.amazonaws.com"
        ]
      }
    ]
  }
}

```

```

    ]
  },
  {
    "Name": "Log all network activity events for EC2",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "NetworkActivity"
        ]
      },
      {
        "Field": "eventSource",
        "Equals": [
          "ec2.amazonaws.com"
        ]
      }
    ]
  },
  {
    "Name": "Log all network activity events for KMS",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "NetworkActivity"
        ]
      },
      {
        "Field": "eventSource",
        "Equals": [
          "kms.amazonaws.com"
        ]
      }
    ]
  },
  {
    "Name": "Log all network activity events for S3",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "NetworkActivity"
        ]
      }
    ]
  }
]

```

```

    },
    {
      "Field": "eventSource",
      "Equals": [
        "s3.amazonaws.com"
      ]
    }
  ],
},
{
  "Name": "Log all network activity events for Secrets Manager",
  "FieldSelectors": [
    {
      "Field": "eventCategory",
      "Equals": [
        "NetworkActivity"
      ]
    },
    {
      "Field": "eventSource",
      "Equals": [
        "secretsmanager.amazonaws.com"
      ]
    }
  ]
}
],
"MultiRegionEnabled": true,
"OrganizationEnabled": false,
"RetentionPeriod": 366,
"TerminationProtectionEnabled": true,
"CreatedTimestamp": "2024-11-20T21:00:17.673000+00:00",
"UpdatedTimestamp": "2024-11-20T21:00:17.820000+00:00"
}

```

## Registro de eventos con los SDK de AWS

Ejecute la operación [GetEventSelectors](#) para saber si el registro de seguimiento está registrando los eventos de actividad de la red. Para configurar sus registros de seguimiento para que registren eventos de actividad de la red, ejecute la operación [PutEventSelectors](#). Para obtener más información, consulte la [Referencia de la API de AWS CloudTrail](#).

Ejecute la operación [GetEventDataStore](#) para saber si el almacén de datos de eventos está registrando los eventos de actividad de la red. Puede configurar sus almacenes de datos de eventos para incluir eventos de actividad de la red ejecutando las operaciones [CreateEventDataStore](#) o [UpdateEventDataStore](#) y especificando los selectores de eventos avanzados. Para obtener más información, consulte [Creación, actualización y administración de almacenes de datos de eventos con la AWS CLI](#) y la [AWS CloudTrail API Reference](#).

## Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM

Puede enriquecer los eventos de administración y de datos de CloudTrail si agrega claves de etiquetas de recursos, claves de etiqueta de entidad principal y claves de condición global de IAM al crear o actualizar un almacén de datos de eventos. Esto le permite clasificar, buscar y analizar los eventos de CloudTrail en función del contexto empresarial, como la asignación de costos y la gestión financiera, las operaciones y los requisitos de seguridad de los datos. Puede analizar los eventos mediante la ejecución de consultas en CloudTrail Lake. También puede elegir [federar](#) su almacén de datos de eventos y ejecutar consultas en Amazon Athena. Puede agregar claves de etiquetas de recursos y claves de condición global de IAM a un almacén de datos de eventos mediante la consola de [CloudTrail](#), [AWS CLI](#) y SDK.

### Note

Es posible que las etiquetas de recursos que agregue después de la creación o las actualizaciones de los recursos tengan un retraso antes de que se reflejen en los eventos de CloudTrail. Es posible que los eventos de CloudTrail para la eliminación de los recursos no incluyan información de etiquetas.

Las claves de condición global de IAM siempre estarán visibles en el resultado de una consulta, pero es posible que el propietario del recurso no las vea.

Cuando agregue claves de etiqueta de recurso para enriquecer los eventos, CloudTrail incluirá las claves de las etiquetas seleccionadas asociadas a los recursos que han participado en la llamada a la API.

Cuando agregue claves de condición global de IAM a un almacén de datos de eventos, CloudTrail incluirá información sobre las claves de condición seleccionadas que se evaluaron durante el

proceso de autorización, como los detalles adicionales sobre la entidad principal, la sesión y la propia solicitud.

 Note

Configurar CloudTrail para incluir una clave de condición o etiqueta de la entidad principal no significa que esta clave de condición o etiqueta de la entidad principal vaya a estar presente en todos los eventos. Por ejemplo, si configuró CloudTrail para incluir una clave de condición global específica, pero no la ve en un evento concreto, esto indica que la clave no era pertinente para la evaluación de la política de IAM para esa acción.

Después de agregar las claves de etiquetas de recursos o las claves de condición de IAM, CloudTrail incluye un campo `eventContext` en los eventos de CloudTrail que ofrece la información contextual seleccionada para la acción de la API.

Existen algunas excepciones en las que el evento no incluirá el campo `eventContext`, como las siguientes:

- Los eventos de la API relacionados con recursos eliminados pueden tener etiquetas de recurso o no tenerlas.
- El campo `eventContext` no tendrá datos sobre los eventos retrasados y no estará presente para los eventos que se hayan actualizado después de la llamada a la API. Por ejemplo, si se produce un retraso o una interrupción en Amazon EventBridge, es posible que las etiquetas de los eventos permanezcan desactualizadas durante algún tiempo después de que se resuelva la interrupción. Algunos servicios de AWS tendrán demoras más prolongadas. Para obtener más información, consulte [Actualizaciones de etiquetas de recursos en CloudTrail para los eventos enriquecidos](#).
- Si modifica o elimina el rol vinculado al servicio `AWSServiceRoleForCloudTrailEventContext` que se utiliza para los eventos enriquecidos, CloudTrail no completará ninguna etiqueta de recurso en `eventContext`.

 Note

El campo `eventContext` solo está presente en los eventos de los almacenes de datos de eventos que están configurados para incluir claves de etiquetas de recursos, claves de etiqueta de entidad principal y claves de condición global de IAM. Los eventos enviados al Historial de eventos de Amazon EventBridge, que se pueden ver con el comando `AWS`

CLI lookup-events y se envían a los registros de seguimiento, no incluirán el campo eventContext.

## Temas

- [Etiquetas de recursos compatibles de Servicios de AWS](#)
- [Servicios de AWS compatibles con las claves de condición global de IAM](#)
- [Ejemplos de evento](#)

## Etiquetas de recursos compatibles de Servicios de AWS

Todas las etiquetas de recursos compatibles de Servicios de AWS. Para obtener más información, consulte [Servicios que admiten AWS Resource Groups Tagging API](#).

### Actualizaciones de etiquetas de recursos en CloudTrail para los eventos enriquecidos

Cuando se configura para ello, CloudTrail captura información sobre las etiquetas de recursos y las utiliza para ofrecer información en los eventos enriquecidos. Al trabajar con etiquetas de recursos, existen ciertas condiciones en las que es posible que una etiqueta de recurso no se refleje con precisión en el momento en que el sistema solicita los eventos. Durante el funcionamiento estándar, las etiquetas aplicadas en el momento de la creación del recurso están siempre presentes y tendrán un retraso mínimo o nulo. Sin embargo, se espera que los servicios que se encuentran a continuación retrasen los cambios en las etiquetas de recursos que aparecen en los eventos de CloudTrail:

- Amazon Chime Voice Connector
- AWS CloudTrail
- AWS CodeConnections
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Keyspaces (for Apache Cassandra)
- Amazon Kinesis
- Amazon Lex
- Amazon MemoryDB
- Amazon S3

- Amazon Security Lake
- AWS Direct Connect
- AWS IAM Identity Center
- AWS Key Management Service
- AWS Lambda
- AWS Marketplace Vendor Insights
- AWS Organizations
- AWS Payment Cryptography
- Amazon Simple Queue Service

Las interrupciones del servicio también pueden ocasionar demoras en las actualizaciones de la información de las etiquetas de recursos. En caso de que se produzca un retraso en la interrupción del servicio, los eventos posteriores de CloudTrail incluirán un campo addendum con información sobre el cambio en la etiqueta de recurso. Esta información adicional se utilizará según lo especificado para ofrecer eventos enriquecidos de CloudTrail.

## Servicios de AWS compatibles con las claves de condición global de IAM

Los siguientes Servicios de AWS admiten claves de condición global de IAM para los eventos enriquecidos:

- AWS Certificate Manager
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon Cognito Sync
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect Voice ID
- AWS Control Tower

- Amazon Data Firehose
- Amazon Elastic Block Store
- Elastic Load Balancing
- AWS End User Messaging Social
- Amazon EventBridge
- Programador de Amazon EventBridge
- Amazon Data Firehose
- Amazon FSx
- AWS HealthImaging
- AWS IoT Events
- AWS IoT FleetWise
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS IoT Wireless
- Amazon Kendra
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- AWS Network Firewall
- AWS Payment Cryptography
- Amazon Personalize
- AWS Proton
- Amazon Rekognition
- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon SQS



- AWS Step Functions
- AWS Storage Gateway
- Amazon SWF
- AWS Supply Chain
- Amazon Timestream
- Amazon Timestream para InfluxDB
- Amazon Transcribe
- AWS Transfer Family
- AWS Trusted Advisor
- Amazon WorkSpaces
- AWS X-Ray

## Claves de condición global de IAM compatibles para los eventos enriquecidos

En la siguiente tabla se enumeran las claves de condición global de IAM compatibles para los eventos enriquecidos de CloudTrail, con valores de muestra:

### Claves de condición global y valores de muestra

| Clave                                   | Ejemplo de valor                                      |
|-----------------------------------------|-------------------------------------------------------|
| <code>aws:FederatedProvider</code>      | <code>"IdP"</code>                                    |
| <code>aws:TokenIssueTime</code>         | <code>"123456789 "</code>                             |
| <code>aws:MultiFactorAuthAge</code>     | <code>"99"</code>                                     |
| <code>aws:MultiFactorAuthPresent</code> | <code>"true"</code>                                   |
| <code>aws:SourceIdentity</code>         | <code>"UserName"</code>                               |
| <code>aws:PrincipalAccount</code>       | <code>"111122223333"</code>                           |
| <code>aws:PrincipalArn</code>           | <code>"arn:aws:iam::555555555555:role/myRole "</code> |
| <code>aws:PrincipalIsAWSService</code>  | <code>"false"</code>                                  |

| Clave                         | Ejemplo de valor                                  |
|-------------------------------|---------------------------------------------------|
| aws:PrincipalOrgID            | "o-rganization "                                  |
| aws:PrincipalOrgPaths         | ["o-rganization/path-of-org "]                    |
| aws:PrincipalServiceName      | "cloudtrail.amazonaws.com "                       |
| aws:PrincipalServiceNamesList | ["cloudtrail.amazonaws.com", "s3.amazonaws.com "] |
| aws:PrincipalType             | "AssumedRole "                                    |
| aws:userid                    | "userid"                                          |
| aws:username                  | "usuario"                                         |
| aws:RequestedRegion           | us-east-2 "                                       |
| aws:SecureTransport           | "true"                                            |
| aws:ViaAWSService             | "false"                                           |
| aws:CurrentTime               | "2025-04-30 15:30:00 "                            |
| aws:EpochTime                 | "1746049800 "                                     |
| aws:SourceAccount             | "111111111111 "                                   |
| aws:SourceOrgID               | "o-rganization "                                  |

## Ejemplos de evento

En el siguiente ejemplo, el campo eventContext incluye la clave de condición global de IAM aws:ViaAWSService con un valor de false, lo que indica que la llamada a la API no la realizó un Servicio de AWS.

```
{  
  "eventVersion": "1.11",  
  "userIdentity": {
```

```

    "type": "AssumedRole",
    "principalId": "ASIAIOSFODNN7EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/admin",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/admin",
        "accountId": "123456789012",
        "userName": "admin"
      },
      "attributes": {
        "creationDate": "2025-01-22T22:05:56Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2025-01-22T22:06:16Z",
  "eventSource": "cloudtrail.amazonaws.com",
  "eventName": "GetTrailStatus",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.168.0.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:133.0)
Gecko/20100101 Firefox/133.0",
  "requestParameters": {
    "name": "arn:aws:cloudtrail:us-east-1:123456789012:trail/myTrail"
  },
  "responseElements": null,
  "requestID": "d09c4dd2-5698-412b-be7a-example1a23",
  "eventID": "9cb5f426-7806-46e5-9729-exampled135d",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true",
  "eventContext": {

```

```
    "requestContext": {
      "aws:ViaAWSService": "false"
    },
    "tagContext": {}
  }
}
```

## CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red

En esta página, se describe el contenido del registro de un evento de administración, de datos o de actividad de la red.

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).

### Note

Los campos para eventos enriquecidos, por ejemplo `eventContext`, solo están disponibles para eventos de administración y de datos. No están disponibles para eventos de la red.

### **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 API `CreateBucket` que se ejecuta en la región EE. UU. Oeste (Oregón) obtendría su marca temporal desde el momento en que un host de AWS ejecuta el punto de enlace de Amazon S3, `s3.us-west-2.amazonaws.com`. En general, los servicios AWS utilizan el Network Time Protocol (NTP) para sincronizar sus relojes del sistema.

Desde: 1.0

Opcional: Falso

## eventVersion

La versión del formato del evento de registro. La versión actual es 1.11.

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 1.10, donde 1 es la versión principal y 10 es la versión secundaria.

CloudTrail incrementa la versión principal si se realiza un cambio en la estructura del evento que no es compatible con versiones anteriores. Esto incluye eliminar un campo JSON existente 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 agrega campos nuevos 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 tipos de eventos nuevos, pero la estructura del evento no se modifica de ninguna otra forma, 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 asegurarse de que los campos previstos por la aplicación están presentes, también recomendamos realizar una comparación mayor o igual que con 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 [Elemento userIdentity de CloudTrail](#).

Desde: 1.0

Opcional: Falso

## eventSource

El servicio 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:

- 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, el 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

La Región de AWS para la que se hizo la solicitud, como `us-east-2`. Consulte [Regiones compatibles con CloudTrail](#).

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. Para los servicios de 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, como la Consola de administración de AWS, un servicio de AWS, los SDK de AWS o la AWS CLI.

Este campo tiene un tamaño máximo de 1 KB; el contenido que supere ese límite se trunca. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se trunca si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

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 para Java.
- `aws-sdk-ruby` – la solicitud se realizó con AWS SDK para Ruby.
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`: la solicitud se realizó con la AWS CLI instalada en Linux.

 Note

Para los eventos originados por AWS, si CloudTrail sabe qué Servicio de AWS realizó la llamada, este campo es el origen del evento del servicio de llamadas (por ejemplo, `ec2.amazonaws.com`). De lo contrario, este campo es `#`, donde `AWS Internal/#` es un número que se usa para fines internos.

Desde: 1.0

Opcional: Verdadero

## **errorCode**

El error del servicio de AWS 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. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se trunca si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

En el caso de los eventos de actividad de la red, cuando se infringe la política de puntos de conexión de VPC, el código de error es `VpceAccessDenied`.

Desde: 1.0

Opcional: Verdadero

## **errorMessage**

Si la solicitud devuelve un error, la descripción del error. Este mensaje incluye mensajes de los errores de autorización. CloudTrail captura el mensaje registrado por el servicio cuando trata las excepciones. Para ver un ejemplo, consulta [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. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se trunca si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

En el caso de los eventos de actividad de la red, cuando se infringe la política de puntos de conexión de VPC, el `errorMessage` será siempre el siguiente mensaje: `The request was denied due to a VPC endpoint policy`. Para obtener más información sobre los eventos de acceso denegado por infracciones de la política de puntos de conexión de VPC, consulte [Ejemplos de mensajes de error de acceso denegado](#) en la Guía del usuario de IAM. Para ver un ejemplo de evento de actividad de la red que muestre una infracción de la política de puntos de conexión de VPC, consulte [Eventos de actividad de la red](#) en esta guía.



 **Note**

Algunos servicios de AWS proporcionan `errorCode` y `errorMessage` en los campos de nivel superior del evento. 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 explican en la documentación de referencia de la API del servicio de AWS correspondiente. Este campo tiene un tamaño máximo de 100 KB. Cuando el tamaño del campo supera los 100 KB, se omite el contenido de `requestParameters`. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se omite si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

Desde: 1.0

Opcional: Falso

## **responseElements**

Los elementos de respuesta, si los hay, de las acciones que realizaron cambios (acciones de creación, actualización o eliminación). En el caso de las API `readOnly`, este campo es `null`. Si la acción no devuelve elementos de respuesta, este campo es `null`. Los elementos de respuesta de las acciones se explican en la documentación de referencia de la API del correspondiente Servicio de AWS.

Este campo tiene un tamaño máximo de 100 KB. Cuando el tamaño del campo supera los 100 KB, se omite el contenido de `responseElements`. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se omite si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

El valor `responseElements` es útil para facilitar el seguimiento de una solicitud con AWS Support. Tanto `x-amz-request-id` como `x-amz-id-2` contienen información que ayuda a

rastrear una solicitud con Soporte. 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. Cuando el tamaño del campo supera los 28 KB, se omite el contenido de `additionalEventData`. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se omite si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

El contenido de `additionalEventData` es variable. Por ejemplo, para los [eventos de inicio de sesión de la Consola de administración de AWS](#), `additionalEventData` podría incluir el campo `MFAUsed` con el valor de `Yes` si la solicitud la realizó un usuario raíz o de IAM mediante la autenticación multifactor (MFA).

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. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se trunca si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

Desde: 1.01

Opcional: Verdadero

## eventID

GUID generado por CloudTrail para identificar de forma inequívoca 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 su cuenta (raíz, IAM, federado, SAML o SwitchRole) inició sesión en la Consola de administración de AWS.
- [AwsVpceEvents](#): los eventos de actividad de la red de CloudTrail permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Para registrar los eventos de actividad de la red, el propietario del punto de conexión de VPC debe habilitar los eventos de actividad de la red para el origen de los eventos.

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:

- Los 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`
- Identificador\* de cuenta: 123456789012
- Identificador de tipo de recurso: `AWS::IAM::Role`

Por ejemplo, para los registros con el campo `resources`, consulte [Evento de API AWS STS en un archivo de registros de CloudTrail](#) en la Guía del usuario de IAM o [Registro de llamadas a la API AWS KMS](#) en la AWS Key Management Service Guía para desarrolladores.

Desde: 1.01

Opcional: Verdadero

## **recipientAccountId**

Representa el ID de cuenta que recibió este evento. El `recipientAccountId` puede ser diferente de [Elemento userIdentity de CloudTrail](#). `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 de cifrado](#), 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 [Servicio de AWSEventos de](#). Este campo tiene un tamaño máximo de 100 KB. Cuando el tamaño del campo supera los 100 KB, se omite el contenido de `serviceEventDetails`. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se omite si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

Desde: 1.05

Opcional: Verdadero

## **sharedEventID**

GUID generado por CloudTrail para identificar de forma inequívoca eventos de CloudTrail de la misma acción de AWS que se envía a diferentes cuentas de AWS.

Por ejemplo, cuando una cuenta utiliza una [AWS KMS key](#) que pertenece a otra cuenta, la cuenta que utilizó la clave de KMS y la cuenta propietaria de la clave de KMS reciben eventos separados de CloudTrail para la misma acción. Cada evento de CloudTrail enviado para esta acción de AWS comparte el mismo `sharedEventID`, pero tiene `eventID` y `recipientAccountID` únicos.

Para obtener más información, consulte [Ejemplo de sharedEventID](#).

### Note

El campo `sharedEventID` solo aparece cuando se envían eventos de CloudTrail a varias cuentas. Si la persona que llama y el propietario son la misma cuenta de AWS, CloudTrail envía solo un evento y no se muestra el campo `sharedEventID`.

Desde: 1.03

Opcional: Verdadero

## **vpcEndpointId**

Identifica el punto de conexión de VPC en el que se realizaron las solicitudes desde una VPC a otro servicio de AWS, como Amazon EC2.

### Note

En el caso de los eventos originados por AWS y a través de una VPC de Servicio de AWS, este campo suele ser `AWS_Internal` o el nombre del servicio.

Desde: 1.04

Opcional: Verdadero

## vpcEndpointAccountId

Identifica el ID de la Cuenta de AWS del propietario del punto de conexión de VPC correspondiente por el que ha pasado una solicitud.

### Note

En el caso de los eventos originados por AWS y a través de una VPC de Servicio de AWS, este campo suele ser `AWS_Internal` o el nombre del servicio.

Desde: 1.09

Opcional: Verdadero

## eventCategory

Muestra la categoría del evento. La categoría del evento se usa en las llamadas de [LookupEvents](#) para filtrar los eventos de administración.

- Para los eventos de administración, el valor es `Management`.
- Para los eventos de datos de, el valor es `Data`.
- En el caso de los eventos de actividad de la red, el valor es `NetworkActivity`.

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 anexo muestra información sobre el motivo del retraso del evento. Si falta información de un evento existente, el campo anexo 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 podría deberse a un alto tráfico de red, problemas de conectividad o un problema de servicio de CloudTrail.
  - **UPDATED\_DATA** – faltó un campo en el registro de eventos o había un valor incorrecto.

- **SERVICE\_OUTAGE** – se interrumpió un servicio que registra eventos en CloudTrail y no pudo registrar eventos en 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**

Cadena con un valor de `true` o `false` que muestra si un evento se originó o no en una sesión de la Consola de administración de AWS. 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

### **eventContext**

Este campo está presente en los eventos enriquecidos registrados en los almacenes de datos de eventos que se configuraron para incluir claves de etiquetas de recursos o claves de condición global de IAM. Para obtener más información, consulte [Enriquecer los eventos de CloudTrail mediante la agregación de etiquetas de recurso y claves de condición global de IAM](#).

El contenido incluye lo siguiente:

- **requestContext**: incluye información sobre las claves de condición global de IAM que se evaluaron durante el proceso de autorización, como detalles adicionales sobre la entidad principal, la sesión, la red y la propia solicitud.
- **tagContext**: incluye las etiquetas asociadas a los recursos que participaron en la llamada a la API, así como las etiquetas asociadas a las entidades principales de IAM, como las funciones



o los usuarios. Para obtener más información, consulte [Control del acceso de las entidades principales de IAM](#).

Los eventos de la API relacionados con recursos eliminados no tendrán etiquetas de recurso.

 **Note**

El campo `eventContext` solo está presente en los eventos de los almacenes de datos de eventos que están configurados para incluir claves de etiquetas de recursos y claves de condición global de IAM. Los eventos enviados al Historial de eventos de Amazon EventBridge, que se pueden ver con el comando `AWS CLI lookup-events` y se envían a los registros de seguimiento, no incluirán el campo `eventContext`.

Desde: 1.11

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. En el caso de los almacenes de datos de eventos configurados para tener un tamaño de evento máximo de 1 MB, el contenido del campo solo se trunca si la carga útil del evento supera 1 MB y se supera el tamaño máximo del campo.

Desde: 1.08

Opcional: Verdadero

## **tlsDetails**

Muestra información sobre la versión de seguridad de la capa de transporte (TLS), los conjuntos de cifrado y el nombre de dominio completo (FQDN) del 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. CloudTrail sigue registrando detalles parciales de TLS si falta la información esperada o está vacía. Por ejemplo, si la versión de TLS y el conjunto de cifrado están presentes, pero el encabezado `HOST` está vacío, los detalles de TLS disponibles todavía se registran en el evento de 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 campo `tlsDetails` no está presente si la llamada a la API la hizo un 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

## Orden de truncamiento de campos para un tamaño máximo de evento de 1 MB

Puede ampliar el tamaño máximo del evento de 256 KB a 1 MB al crear o actualizar un almacén de datos de eventos mediante la [consola de CloudTrail](#), [AWS CLI](#) y SDK.

La ampliación del tamaño de evento es útil para analizar y solucionar problemas de eventos, ya que le permite ver el contenido completo de los campos que normalmente se truncarían u omitirían.

Cuando la carga útil del evento supera 1 MB, CloudTrail trunca los campos en el siguiente orden:

- `annotation`
- `requestID`
- `additionalEventData`

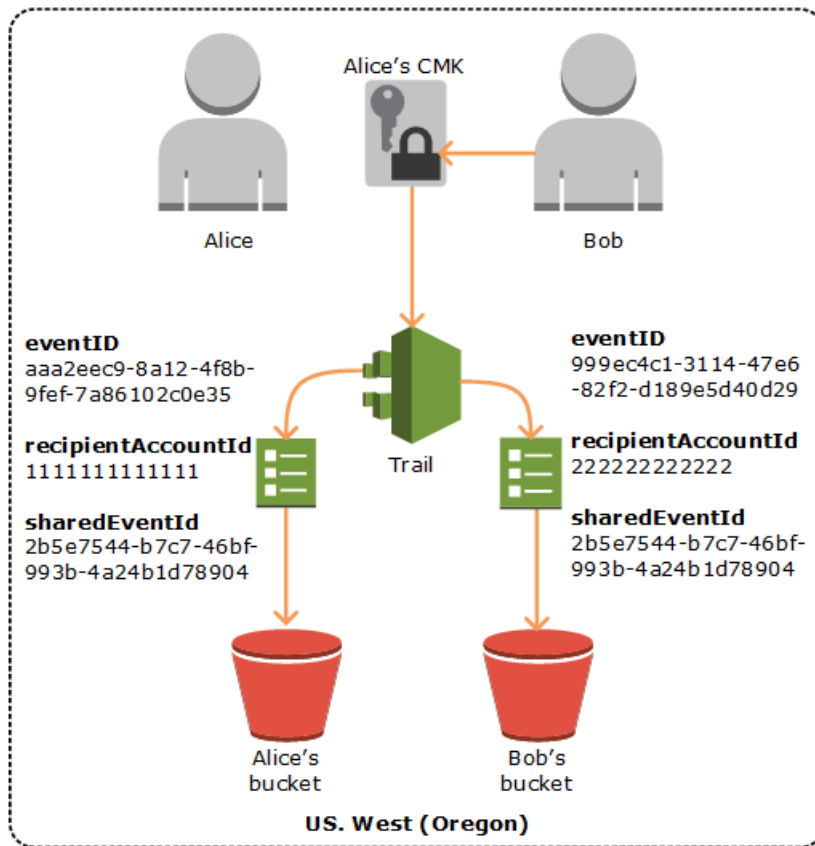
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `eventContext`
- `responseElements`
- `requestParameters`
- `errorMessage`

Si la carga útil de un evento no se puede reducir a menos de 1 MB incluso después del truncamiento, se producirá un error.

## Ejemplo de `sharedEventID`

A continuación, se muestra un ejemplo que describe cómo CloudTrail envía dos eventos para la misma acción:

1. Alice tiene la cuenta AWS (111111111111) y crea una AWS KMS key. Es la propietaria de esta clave de KMS.
2. Bob tiene la cuenta AWS (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 distintos.
  - 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.



## CloudTrail registra el contenido de los eventos de Insights para registros de seguimiento

Los registros de eventos de AWS CloudTrail Insights para los registros de seguimiento incluyen campos que son diferentes de otros eventos de CloudTrail en su estructura JSON, a veces llamados carga útil. Los eventos de CloudTrail Insights para registros de seguimiento contienen los campos siguientes:

- **eventVersion:** versión del evento.

Desde: 1.07

Opcional: Falso

- **eventType:** tipo de evento. El valor siempre es `AwsCloudTrailInsight` para los eventos de Insights.

Desde: 1.07

Opcional: Falso

- **eventID**: GUID generado por CloudTrail para identificar de forma inequívoca 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: 1.07

Opcional: Falso

- **eventTime**: la hora en que se inició o se detuvo el evento de Insights, en hora universal coordinada (UTC).

Desde: 1.07

Opcional: Falso

- **awsRegion**: la Región de AWS en la que se produjo el evento de Insights, por ejemplo us-east-2.

Desde: 1.07

Opcional: Falso

- **recipientAccountId**: representa el ID de cuenta que recibió este evento.

Desde: 1.07

Opcional: Verdadero

- **sharedEventID**: un GUID que es generado por CloudTrail Insights para identificar de forma inequívoca un evento de Insights. sharedEventID es igual en los eventos iniciales y finales de Insights, y ayuda a conectar ambos eventos para identificar de forma inequívoca la actividad inusual. sharedEventID puede considerarse como el ID general de evento de Insights.

Desde: 1.07

Opcional: Falso

- **insightDetails**: un registro de eventos de CloudTrail Insights para un registro de seguimiento incluye un bloque insightDetails que contiene información sobre los desencadenantes subyacentes de un evento de Insights, tal como el origen del evento, las identidades de usuario, los agentes de usuario, los promedios o las referencias históricos, las estadísticas, el nombre de la API y si se trata de un evento de Insights inicial o final.

Desde: 1.07

Opcional: Falso

- **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 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` o `ApiErrorRateInsight`.

Desde: 1.07

Opcional: Falso

- **errorCode**: el código de error de la actividad inusual. También consulte `errorCode` en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

Desde: 1.07

Opcional: Verdadero

- **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 o errores que desencadenaron el 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**: las llamadas a la API o los 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

- **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.

Desde: 1.07

Opcional: Falso

- **insight**: para un evento inicial de Insights, este valor es la cantidad promedio 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

- **average**: la cantidad promedio de llamadas a la API o errores registrados por minuto durante el periodo de actividad inusual.

Desde: 1.07

Opcional: Falso

- **insightDuration**: la duración, en minutos, de un evento de Insights (el periodo 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 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**: 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`. Si están presentes, estos valores solo aparecerán una vez en un atributo individual. Los distintos valores de atributo pueden tener valores `userIdentityArn`, `userAgent` o `errorCode` diferentes, pero cada instancia de atributo contendrá solo un valor para `userIdentityArn`, `userAgent` o `errorCode`.

Desde: 1.07

Opcional: Falso



- **insight**: un bloque que muestra hasta los cinco valores de atributo principales que contribuyeron a las llamadas a la API o los errores realizados durante el periodo de actividad inusual, en orden descendente desde la mayor cantidad de llamadas a la API o errores hasta la menor. También muestra el promedio de llamadas a la API o errores realizados por el valor del atributo durante el periodo de actividad inusual.

Desde: 1.07

Opcional: Falso

- **value**: el atributo que contribuyó a las llamadas a la API o errores realizados durante el periodo de actividad inusual.

Desde: 1.07

Opcional: falso Falso

- **average**: la cantidad de llamadas a la API o errores por minuto durante el periodo de actividad inusual para el atributo en el campo `value`.

Desde: 1.07

Opcional: falso Falso

- **baseline**: un bloque que muestra hasta los cinco valores de atributo principales que más contribuyeron a las llamadas a la API o los errores durante el periodo de actividad normal, en orden descendente desde la mayor cantidad de llamadas a la API o errores hasta la menor. También muestra el promedio de llamadas a la API o errores realizados por el valor del atributo durante el periodo de actividad normal.

Desde: 1.07

Opcional: falso Falso

- **value**: el atributo que contribuyó a las llamadas a la API o los errores durante el periodo de actividad normal.

Desde: 1.07

Opcional: falso 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 atributo en el

**campo value**

Desde: 1.07

Opcional: falso Falso

- **eventCategory**: la categoría del evento. El valor siempre es Insight para los eventos de Insights.

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 [Eventos de Insights](#).

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 `esnull`), 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
        }
      ]
    }
  ]
}
```

## CloudTrail registra el contenido de los eventos de Insights para los almacenes de datos de eventos

Los registros de eventos de AWS CloudTrail Insights para los almacenes de datos de eventos incluyen campos que son diferentes de otros eventos de CloudTrail en su estructura JSON, a veces llamados carga útil. Un registro de eventos de CloudTrail Insights para un almacén de datos de eventos incluye los siguientes campos:

### Note

Los campos `insightValue`, `insightAverage`, `baselineValue` y `baselineAverage` incluidos en el campo `attributions` de `insightContext` comenzarán a quedar obsoletos el 23 de junio de 2025.

- **eventVersion**: la versión del formato del evento de registro.

Opcional: Falso

- **eventCategory**: la categoría del evento. El valor siempre es `Insight` para los eventos de Insights.

Opcional: Falso

- **eventType**: el tipo de evento. El valor siempre es `AwsCloudTrailInsight` para los eventos de Insights.

Opcional: Falso

- **eventID**: GUID generado por CloudTrail para identificar de forma inequívoca 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.

Opcional: Falso

- **eventTime**: la hora en que se inició o se detuvo el evento de Insights, en hora universal coordinada (UTC).

Opcional: Falso

- **awsRegion**: la Región de AWS en la que se produjo el evento de Insights, por ejemplo `us-east-2`.

Opcional: Falso

- **recipientAccountId**: representa el ID de cuenta que recibió este evento.

Opcional: Verdadero

- **sharedEventID**: un GUID que es generado por CloudTrail Insights para identificar de forma inequívoca un evento de Insights. `sharedEventID` es igual en los eventos iniciales y finales de Insights, y ayuda a conectar ambos eventos para identificar de forma inequívoca la actividad inusual. `sharedEventID` puede considerarse como el ID general de evento de Insights.

Opcional: Falso

- **addendum**: si se retrasó la entrega de un evento o queda disponible información adicional sobre un evento existente después de registrar el evento, un campo anexo muestra información sobre el motivo del retraso del evento. Si falta información de un evento existente, el campo anexo

incluye la información que falta y un motivo. También consulte addendum en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

Opcional: Verdadero

- **insightSource**: el almacén de datos de eventos de origen que recopiló los eventos de administración que se analizaron.

Opcional: Falso

- **insightState** – si el evento es el evento inicial o final de Insights. El valor puede ser Start o End.

Opcional: Falso

- **insightEventSource**: el Servicio de AWS que fue la fuente de la actividad inusual, como `ec2.amazonaws.com`.

Opcional: Falso

- **insightEventName** – el nombre del evento de Insights, normalmente el nombre de la API que fue la fuente de la actividad inusual.

Opcional: Falso

- **insightErrorCode**: el código de error de la actividad inusual. También consulte `errorCode` en [CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

Opcional: Verdadero

- **insightType** – el tipo de evento de Insights. Este valor puede ser `ApiCallRateInsight` o `ApiErrorRateInsight`.

Opcional: Falso

- **insightContext**: contiene información sobre el desencadenante subyacente de un evento de Insights, como la identidad del usuario, el agente de usuario, la media o referencia histórica y la duración y el promedio de Insights.

Opcional: Falso

- **baselineAverage** – 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.

Opcional: Falso

- **insightAverage**: para un evento inicial de Insights, este valor es la cantidad media 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.

Opcional: Falso

- **baselineDuration**: la duración, en minutos, del periodo de referencia (el periodo 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.

Opcional: Falso

- **insightDuration**: la duración, en minutos, de un evento de Insights (el periodo 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.

Opcional: Falso

- **attributions**: incluye información sobre la identidad del usuario, agente de usuario o código de error correlacionados con la actividad inusual y de referencia.

Opcional: Verdadero

 Note

Los campos `insightValue`, `insightAverage`, `baselineValue` y `baselineAverage` incluidos en el campo `attributions` de `insightContext` comenzarán a quedar obsoletos el 23 de junio de 2025.

- **attribute** – contiene el tipo de atributo. Los valores pueden ser `userIdentityArn`, `userAgent` o `errorCode`. Si están presentes, estos valores solo aparecerán una vez en un atributo individual. Los distintos valores de atributo pueden tener valores `userIdentityArn`, `userAgent` o `errorCode` diferentes, pero cada instancia de atributo contendrá solo un valor para `userIdentityArn`, `userAgent` o `errorCode`.

Opcional: Falso

- **insightValue**: el valor de atributo principal que se produjo en las llamadas a la API o los errores que se realizaron durante el periodo de actividad inusual.

Opcional: Falso

- **insightAverage**: el número de llamadas a la API o errores por minuto durante el periodo de actividad inusual para el atributo en el campo `insightValue`.

Opcional: Falso

- **baselineValue**: el valor de atributo principal que contribuyó a las llamadas a la API o los errores registrados durante el periodo de actividad normal.

Opcional: Falso

- **baselineAverage**: 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 atributo en el campo `baselineValue`.

Opcional: Falso

- **insight**: los cinco valores de atributo principales que contribuyeron a las llamadas a la API o los errores realizados durante el periodo de actividad inusual. También muestra el promedio de llamadas a la API o errores realizados por el atributo durante el periodo de actividad inusual.

Opcional: Falso

- **value**: el atributo que contribuyó a las llamadas a la API o los errores realizados durante el periodo de actividad inusual.

Opcional: Falso

- **average**: la cantidad promedio de llamadas a la API o errores registrados por minuto durante el periodo de actividad inusual para el atributo en el campo `value`.

Opcional: Falso

- **baseline**: los cinco valores de atributo principales que más contribuyeron a las llamadas a la API o los errores durante el periodo de actividad normal. También muestra la cantidad promedio de llamadas a la API o errores registrados por el valor del atributo durante el periodo de actividad normal.

Opcional: Falso



- **value**: el atributo que contribuyó a las llamadas a la API o los errores realizados durante el periodo de actividad normal.

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 atributo en el campo `value`.

Opcional: Falso

## Elemento `userIdentity` de CloudTrail.

AWS Identity and Access Management (IAM) ofrece 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 de las API de AWS STS con SAML e identidad federada web](#)
- [AWS STSIdentidad fuente de](#)

## 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": "AROAI DPPEZS35WEXAMPLE:AssumedRoleSessionName",
  "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
  "accountId": "123456789012",
  "accessKeyId": "",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROAI DPPEZS35WEXAMPLE",
      "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
      "accountId": "123456789012",
      "userName": "RoleToBeAssumed"
    },
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "20131102T010628Z"
    }
  }
}
```

## **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": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYc0YcxFV1lWR_Whr1fEXAMPLE"
```

```
}
```

Para obtener más información sobre cómo utilizar `userId`, `identityStoreArn` y `credentialId`, consulte [Identificación del usuario y la sesión en los eventos de CloudTrail iniciados por los usuarios de IAM Identity Center](#) en la Guía del usuario de IAM Identity Center.

## 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 hizo con las credenciales de Cuenta de AWS. 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 hizo con credenciales de seguridad temporales que se obtuvieron de una llamada a la API de AWS STS [GetFederationToken](#). 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 Amazon WorkDocs y Amazon Quick Suite.
- **AWSAccount**: la solicitud la hizo otra Cuenta de AWS.
- **AWSService**: la solicitud la hizo otra Cuenta de AWS que pertenece a un Servicio de AWS. Por ejemplo, AWS Elastic Beanstalk adopta un rol de IAM en su cuenta para llamar a otros Servicios de AWS en su nombre.

- **IdentityCenterUser**: la solicitud se hizo en nombre de un usuario de IAM Identity Center.
- **Unknown**: la solicitud se hizo con un tipo de identidad que CloudTrail no 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 cuenta de AWS cambia a ese rol para asumir el rol de su 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, consulte [Evento de la API de AWS STS en el archivo de registro de CloudTrail](#).

Ejemplo: acceso entre cuentas iniciado por un servicio de AWS

1. Usted es propietario de un rol de IAM en su cuenta.
2. Una cuenta de AWS propiedad de un servicio de AWS asume ese rol.
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**:

| <b>type</b>               | <b>userName</b> | Descripción                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root (sin alias definido) | No presente     | Si no ha creado un alias para su Cuenta de AWS, no aparecerá el campo <b>userName</b> . Para obtener más información sobre los alias de cuenta, consulte <a href="#">Su ID de Cuenta de AWS y su alias</a> . Tenga en cuenta que el campo <b>userName</b> no puede contener Root porque Root es un tipo de identidad, no un nombre de usuario. |

| type                      | userName                                | Descripción                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root (con alias definido) | El alias de la cuenta                   | Para obtener más información sobre los alias de Cuenta de AWS, consulte <a href="#">Su ID de Cuenta de AWS y su alias</a> .                                                                                         |
| 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 <a href="#">sessionIsuer</a> . Para ver una entrada de ejemplo, consulte <a href="#">Ejemplos</a> . |
| Role                      | Definido por el usuario                 | Las secciones sessionContext y sessionIsuer contienen información sobre la identidad que emitió la sesión para el rol.                                                                                              |
| FederatedUser             | No presente                             | Las secciones sessionContext y sessionIsuer contienen información sobre la identidad que emitió la sesión para el usuario federado.                                                                                 |
| Directory                 | Puede estar presente                    | Por ejemplo, el valor puede ser el <a href="#">alias de cuenta</a> o la dirección de correo electrónico del <a href="#">ID de Cuenta de AWS</a> asociado.                                                           |
| AWSService                | No presente                             |                                                                                                                                                                                                                     |
| AWSAccount                | No presente                             |                                                                                                                                                                                                                     |

| type               | userName             | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IdentityCenterUser | No presente*         | <p>La sección <code>onBehalfOf</code> 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 sobre cómo utilizar estos dos campos, consulte <a href="#">Identificación del usuario y la sesión en los eventos de CloudTrail iniciados por los usuarios de IAM Identity Center</a> en la Guía del usuario de IAM Identity Center.</p> <p>* El IAM Identity Center emite el campo <code>userName</code> que se encuentra debajo del elemento <code>additionalEventData</code> en dos eventos de CloudTrail de inicio de sesión. Para obtener más información, consulte <a href="#">Nombre de usuario en los eventos de inicio de sesión de CloudTrail</a> en la Guía del usuario de IAM Identity Center.</p> |
| Unknown            | Puede estar presente | <p>Por ejemplo, el valor puede ser el <a href="#">alias de cuenta</a> o la dirección de correo electrónico del <a href="#">ID de Cuenta de AWS</a> asociado.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

 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 registra el contenido en este caso, ya que el texto podría contener información confidencial, como en los siguientes ejemplos:

- Un usuario escribe por error una contraseña en el campo de nombre de usuario.
- Un usuario hace clic en el enlace de una página de inicio de sesión de una cuenta de AWS, pero escribe el número de una cuenta diferente.
- 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 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](#). Pueden aparecer los siguientes atributos en `sessionContext`:

-

**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`, `IAMUser` o `Role`.
- **userName**: el nombre descriptivo del usuario o el rol que emitió la sesión. El valor que aparece depende del valor **sessionIssuer** de la identidad **type**. En la tabla siguiente se muestra la relación entre **sessionIssuer**, **type** y **userName**:

| Tipo de <b>sessionIssuer</b> | <b>userName</b>                         | Descripción                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root (sin alias definido)    | No presente                             | Si no ha creado un alias para su cuenta, no aparece el campo <b>userName</b> . Para obtener más información sobre los alias de Cuenta de AWS, consulte <a href="#">Su ID de Cuenta de AWS y su alias</a> . Tenga en cuenta que el campo <b>userName</b> no puede contener <code>Root</code> porque <code>Root</code> 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 alias de Cuenta de AWS, consulte <a href="#">Su ID de cuenta de AWS y sus alias</a> .                                                                                                                                                                                                                                           |
| <code>IAMUser</code>         | El nombre de usuario del usuario de IAM | Esto también se aplica cuando un usuario federado utiliza una sesión emitida por <code>IAMUser</code> .                                                                                                                                                                                                                                                                |
| <code>Role</code>            | El nombre del rol                       | Un rol que adoptó un usuario de IAM, un Servicio de AWS o un usuario federado de identidad web en una sesión de rol.                                                                                                                                                                                                                                                   |



- `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.
- `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 o la presencia de este campo con un valor vacío significa que no hay información sobre el proveedor de identidades.

- `assumedRoot`: el valor corresponde a `true` para una sesión temporal cuando un administrador delegado o una cuenta de administración llama a AWS STS [AssumedRoot](#). Para obtener más información, consulte [Seguimiento de tareas privilegiadas en CloudTrail](#) en la Guía del usuario de IAM. Se trata de un campo opcional.
- `attributes`: los atributos de la sesión.
  - `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 fuente de](#) 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 cómo configurar AWS STS para recopilar información sobre la identidad de la fuente, consulte [Monitoreo y control de las acciones realizadas con roles adoptados](#) 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.

Las credenciales de AWS proporcionadas por el servicio de metadatos de instancia de Amazon EC2 (IMDS) incluyen una clave de contexto de IAM `ec2:RoleDelivery`. Esta clave de contexto facilita la aplicación del nuevo esquema servicio por servicio o recurso por recurso al utilizar la clave de contexto como condición en las políticas de IAM, las políticas de recursos o las políticas de control de servicios de AWS Organizations. Para obtener más información, consulte [Metadatos de instancia y datos de usuario](#) en la Guía del usuario de Amazon EC2.

Opcional: Verdadero

### **invokedBy**

Nombre del Servicio de AWS que hizo la solicitud, cuando la solicitud la hace un Servicio de AWS como Amazon EC2 Auto Scaling o AWS Elastic Beanstalk. Este campo solo está presente cuando la solicitud la hace un Servicio de AWS. Esto incluye las solicitudes realizadas por los servicios que utilizan sesiones de acceso directo (FAS), las entidades principales del Servicio de AWS, los roles vinculados al servicio o los roles de servicio utilizados por un Servicio de AWS.

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

## **inScopeOf**

Si la solicitud se realizó en el ámbito de Servicio de AWS, como Lambda o Amazon ECS, se ofrece información sobre el recurso o las credenciales relacionadas con la solicitud. Este elemento puede contener los siguientes atributos:

- **sourceArn**: el ARN del recurso que invocó la solicitud de servicio a servicio.
- **sourceAccount**: el ID de la cuenta del propietario para el **sourceArn**. Aparece junto con **sourceArn**.
- **issuerType**: tipo de recurso de **credentialsIssuedTo**. Por ejemplo, **AWS::Lambda::Function**.
- **credentialsIssuedTo**: el recurso relacionado con el entorno en el que se emitieron las credenciales.

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

## Valores de las API de AWS STS con SAML e identidad federada web

AWS CloudTrail admite el registro de llamadas a la API de AWS Security Token Service (AWS STS) realizadas con el lenguaje de marcado para confirmaciones de seguridad (SAML) y las Identidades web federadas. Cuando un usuario hace una llamada a las API [AssumeRoleWithSAML](#) y [AssumeRoleWithWebIdentity](#), CloudTrail registra 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 archivos de registro de ejemplo de cómo aparece el elemento `userIdentity` para los tipos `SAMLUser` y `WebIdentityUser`, consulte [Registro de IAM y de llamadas a la API de AWS STS con la AWS CloudTrail](#).

## AWS STSIdentidad fuente de

Un administrador de IAM puede configurar AWS Security Token Service para requerir que los usuarios especifiquen su identidad cuando utilicen credenciales temporales para adoptar roles. 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). Después de que el administrador de IAM configura AWS STS, CloudTrail registra información de `sourceIdentity` en los siguientes eventos y ubicaciones dentro del registro de evento:

- Las llamadas AWS STS `AssumeRole`, `AssumeRoleWithSAML` o `AssumeRoleWithWebIdentity` que una identidad de usuario realiza cuando adopta un rol. `sourceIdentity` se encuentra en el bloque `requestParameters` de las llamadas AWS STS.
- Las llamadas de AWS STS `AssumeRole`, `AssumeRoleWithSAML` o `AssumeRoleWithWebIdentity` que una identidad de usuario realiza si utiliza un rol para adoptar otro rol, conocido como [encadenamiento de roles](#). `sourceIdentity` se encuentra en el bloque `requestParameters` de las llamadas a AWS STS.
- Las llamadas a la API del servicio AWS que realiza la identidad del usuario mientras adopta un rol y utiliza 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 para recopilar información sobre la identidad de la fuente, consulte [Monitoreo y control de las acciones realizadas con roles adoptados](#) en la Guía del usuario de IAM. Para obtener más información sobre los eventos de AWS STS que se registran en CloudTrail, consulte [Registrar IAM y llamadas a la API AWS STS con 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 ejemplo de fragmento de evento, un usuario hace una solicitud AWS STS AssumeRole y establece una identidad de origen, representada aquí por *source-identity-value-set*. El usuario adopta un rol representado por el ARN del rol `arn:aws:iam::123456789012:role/Assumed_Role`. 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 ejemplo de fragmento de evento, un usuario realiza una solicitud AWS STS AssumeRole para adoptar un rol llamado `Developer_Role` y establece la identidad de una fuente, `Admin`. El usuario adopta un rol representado por el ARN del rol `arn:aws:iam::111122223333:role/Developer_Role`. 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": "AR0ACKCEVSQ6C2EXAMPLE:Session_Name",
      "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
    },
    "sourceIdentity": "Admin"
  }
}
...

```

### Ejemplo de sección de **sessionContext**

En el siguiente ejemplo de fragmento de evento, un usuario adopta un rol denominado DevRole para llamar a una API de servicio AWS. El usuario establece la identidad de la fuente, 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": "AR0AJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AR0AJ45Q7YFFAREXAMPLE",
        "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"
  }
}
```

## 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.

- [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`.
- [Eventos de inicio de sesión de Consola de administración de AWS](#): los registros de CloudTrail intentan iniciar sesión en la Consola de administración de AWS, los foros de discusión de AWS y el centro de asistencia de AWS. Todos los eventos de inicio de sesión de usuarios raíz y de usuarios de IAM, así como todos los eventos de inicio de sesión de usuarios federados, generan registros en CloudTrail. En el caso de los eventos de inicio de sesión, el campo `eventType` es `AwsConsoleSignIn`.

## Servicio de AWSEventos de

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": "1.08",
"userIdentity": {
  "accountId": "111122223333",
  "invokedBy": "AWS Internal"
},
"eventTime": "2021-01-14T01:41:59Z",
"eventSource": "kms.amazonaws.com",
"eventName": "RotateKey",
"awsRegion": "us-west-2",
"sourceIPAddress": "AWS Internal",
"userAgent": "AWS Internal",
"requestParameters": null,
"responseElements": null,
"eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
"readOnly": false,
"resources": [
  {
    "accountId": "111122223333",
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "111122223333",
"serviceEventDetails": {
  "rotationType": "AUTOMATIC",
  "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
},
"eventCategory": "Management"
}
```

## Consola de administración de AWSEventos de inicio de sesión en la

Los registros de CloudTrail intentan iniciar sesión en la Consola de administración de AWS, los foros de discusión de AWS y el centro de asistencia de AWS. Todos los eventos de inicio de sesión de usuarios raíz y de usuarios de IAM, así como todos los eventos de inicio de sesión de usuarios federados, generan archivos de registro de CloudTrail. Para obtener más información acerca de cómo buscar y visualizar registros, consulte [Búsqueda de los archivos de registros de CloudTrail](#) y [Descarga de los archivos de registros de CloudTrail](#).

Puede usar [AWS User Notifications](#) para configurar los canales de entrega a fin de recibir notificaciones sobre los eventos de AWS CloudTrail. Recibirá una notificación cuando un evento coincida con una regla que especifique. Puede recibir notificaciones de eventos a través de varios canales, como correo electrónico, notificaciones por chat de [Amazon Q Developer en aplicaciones de chat](#) o notificaciones push de [AWS Console Mobile Application](#). También puede ver las notificaciones en el [Centro de notificaciones de la consola](#). Las Notificaciones de usuario admiten la agregación, lo que puede reducir el número de notificaciones que recibe durante eventos específicos.

#### Note

La región registrada en un evento de ConsoleLogin varía en función del tipo de usuario y de si utiliza un punto de conexión global o regional para iniciar sesión.

- Si inicia sesión con usuario raíz, CloudTrail registra el evento en us-east-1.
- Si inicia sesión con un usuario de IAM y usa el punto de conexión global, CloudTrail registra la región del evento de ConsoleLogin de la siguiente manera:
  - Si hay una cookie de alias de cuenta en el navegador, CloudTrail registra el evento ConsoleLogin 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 en el navegador no hay ninguna cookie de alias de cuenta, CloudTrail registra el evento ConsoleLogin 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 de conexión regional](#), CloudTrail registra el evento ConsoleLogin en la región correspondiente para el punto de conexión. Para más información sobre los puntos de conexión de AWS Sign-In, consulte [Cuotas y puntos de conexión de AWS Sign-In](#).

## 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

En el siguiente registro, se muestra que un usuario llamado Anaya ha iniciado sesión correctamente en la Consola de administración de AWS 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

En el siguiente registro, se muestra que un usuario de IAM llamado Anaya ha iniciado sesión correctamente en la Consola de administración de AWS con la autenticación multifactor (MFA).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLE6E4XEGITWATV6R",
    "arn": "arn:aws:iam::999999999999:user/Anaya",
    "accountId": "999999999999",
    "userName": "Anaya"
  },
  "eventTime": "2023-07-19T22:01:30Z",
  "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 raíz, CloudTrail registra el evento ConsoleLogin en us-east-1.

### 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 recursos de AWS 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.

### Note

En este ejemplo, el valor `mfaAuthenticated` es `false` y el valor `MFAUsed` es `No` debido a que la solicitud la realizó un usuario federado. Estos campos solo se establecerán en verdadero si la solicitud la realizó un usuario de IAM o un usuario raíz mediante MFA.

```
{  
  "eventVersion": "1.08",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "EXAMPLEUU4MH70YK5ZCOA:JohnDoe",  
    "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",  
    "accountId": "123456789012",  
    "accessKeyId": "originalAccessKeyID",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "EXAMPLEUU4MH70YK5ZCOA",  
        "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"
    }
  }

```



```
}
```

# Trabajar con archivos de registros de CloudTrail

Puede realizar tareas más avanzadas con sus archivos de CloudTrail.

- 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](#).

- [Eventos de actividad de la red](#): los eventos de actividad de la red de CloudTrail permiten a los propietarios del punto de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Los eventos de actividad de la red muestran información sobre las operaciones de recursos realizadas dentro de una VPC.
- [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 [Trabajar con CloudTrail 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 servicio 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

- [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 registro de CloudTrail de varias cuentas](#)
- [Compartir archivos de registro de CloudTrail entre cuentas de AWS](#)

- [Validar la integridad de los archivos de registros de CloudTrail](#)
- [Ejemplos de archivos de registros de CloudTrail](#)
- [Uso de la biblioteca de procesamiento de CloudTrail](#)

## Recepción de archivos de registro de CloudTrail de varias regiones

Cuando crea un registro de seguimiento de varias regiones, en CloudTrail se registran los eventos de todas las regiones habilitadas en 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.

Aunque la mayoría de Regiones de AWS están habilitadas por defecto en su Cuenta de AWS, debe habilitar manualmente determinadas regiones (también denominadas regiones optativas). Para obtener información sobre qué regiones están habilitadas por defecto, consulte [Considerations before enabling and disabling Regions](#) en la Guía de referencia de AWS Account Management. Para ver la lista de las regiones que admite CloudTrail, consulte [Regiones compatibles con CloudTrail](#).

Después de habilitar una región optativa, en CloudTrail se crea una copia idéntica de cada registro de seguimiento de varias regiones de la región optativa que habilitó. Para obtener más información, consulte [¿Qué sucede cuando se habilita una región optativa?](#).

Si más adelante deshabilita una región optativa, se conservará la copia del registro de seguimiento de varias regiones de esa región. Como su cuenta puede tener actividad en la región que desactivó, como acciones de Servicios de AWS para eliminar recursos, en CloudTrail se seguirá registrando la actividad e intentando enviar eventos al bucket de S3 para cualquier registro de seguimiento que no se elimine antes de deshabilitar la región.

Para convertir un registro de seguimiento de una sola región existente en un registro de seguimiento de varias regiones, debe utilizar la AWS CLI.

Para cambiar un registro de seguimiento existente de forma que se aplique a todas las regiones habilitadas, 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 es ahora uno de varias regiones, compruebe que el elemento `IsMultiRegionTrail` de la salida muestre `true`.

```
{
  "IncludeGlobalServiceEvents": true,
  "Name": "my-trail",
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
  "LogFileValidationEnabled": false,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "S3BucketName": "amzn-s3-demo-bucket"
}
```

Para obtener más información, consulte los siguientes recursos:

- [Cómo entender los registros de seguimiento de varias regiones y las regiones optativas](#)
- [Creación de un registro de seguimiento para su Cuenta de AWS](#)
- [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 en los resultados se debe en parte al tiempo que se tarda en enviar los datos de un servidor a otro 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 [habilitar una región de inclusión](#), 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 utilizar los [registros de Amazon CloudWatch](#) para supervisar, almacenar y acceder a los archivos de registro desde CloudTrail.

Los registros de CloudWatch le permiten centralizar los registros de todos los sistemas, aplicaciones y los Servicios de AWS que utilice, en un único servicio de gran escalabilidad. De este modo, los puede consultar fácilmente, buscar códigos de error o patrones específicos, filtrarlos en función de campos específicos o archivarlos de forma segura para análisis futuros. Registros de CloudWatch le permite ver todos los registros, independientemente de su origen, como un flujo único y consistente de eventos ordenados de manera temporal.

Siga estos pasos para configurar CloudTrail con Registros de CloudWatch 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 para que CloudTrail utilice CloudWatch Logs para el monitoreo.](#)

## 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 consola de CloudTrail](#).
- 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 Consola de administración de AWS 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 consola 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.

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 de varias 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 de varias regiones envía archivos de registro desde todas las regiones habilitadas en su Cuenta de AWS 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 para que CloudTrail utilice CloudWatch Logs para el monitoreo](#).

 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. Seleccione Save changes (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 para que CloudTrail utilice CloudWatch Logs para el monitoreo..](#)

## 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`.

### 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.

### JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
      ]
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",

```

```

        "Effect": "Allow",
        "Action": [
            "logs:PutLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
        ]
    }
]
}

```

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*:

## JSON

```

{
    "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-aa111bb222_*"
            ]
        },
        {

```

```
    "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-aa111bb222_*"
    ]
  }
}
```

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 Consola de administración de AWS](#)
- [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 con la consola de CloudTrail](#).
- 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 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 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 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 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 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 Consola de administración de AWS

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 Consola de administración de AWS 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 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 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 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 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 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 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 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 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 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 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 notificaciones de Amazon SNS](#) en la Guía del usuario 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 Consola de administración de AWS 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. Seleccione 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 registro 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 para que CloudTrail utilice CloudWatch Logs para el monitoreo.

Esta sección describe la política de permisos necesaria para que el rol de CloudTrail envíe eventos de registro a CloudWatch Logs. Puede adjuntar un documento de políticas a un rol cuando configure CloudTrail para enviar eventos, como se describe en [Envío de eventos a Amazon CloudWatch Logs](#). También puede crear un rol con IAM. Para obtener más información, consulte [Crear un rol para delegar permisos a un Servicio de AWS](#) o [Crear un rol de IAM \(AWS CLI\)](#).

El siguiente ejemplo de documento de políticas contiene los permisos necesarios para crear un flujo de registro de CloudWatch en el grupo de registro que especifique y para enviar eventos de CloudTrail a dicho flujo de registro en la región Este de EE. UU. (Ohio). (Esta es la política predeterminada para el rol de IAM predeterminado ). CloudTrail\_CloudWatchLogs\_Role.)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
```

```

        "arn:aws:logs:us-east-2:111122223333: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-2:111122223333: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 concede a CloudTrail los permisos necesarios para crear una secuencia de registros de CloudWatch Logs en el grupo de registros que especifique como el valor *log\_group\_name* y para enviar eventos de CloudTrail a esa secuencia de registros tanto para los registros de seguimiento en la cuenta 111111111111 de AWS como para los registros de seguimiento de organización creados en la cuenta 111111111111 que se aplican a la organización de AWS Organizations con el ID de *o-exampleorgid*:

JSON

```

{
    "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 registro de CloudTrail de varias cuentas

Puede hacer que CloudTrail envíe los archivos de registro desde varias Cuentas de AWS a un solo bucket de Amazon S3. Por ejemplo, tiene cuatro Cuentas de AWS con los ID 111111111111, 222222222222, 333333333333 y 444444444444 y quiere configurar CloudTrail para que envíe los archivos de registro de las cuatro cuentas a un bucket que pertenece a la cuenta 111111111111. 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 con 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 que CloudTrail utilice la clave para cifrar los archivos de registro y de resumen, y que los usuarios especificados lean los archivos de registro y de resumen 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](#).

## Eliminación de los ID de las cuentas de los propietarios de los buckets para eventos de datos llamados por otras cuentas

Históricamente, si los eventos de datos de CloudTrail estaban habilitados en la Cuenta de AWS de un intermediario de la API de eventos de datos de Amazon S3, CloudTrail mostraba el ID de la 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 la cuenta del propietario del bucket de S3 del bloque `resources` si se cumplen las dos condiciones siguientes:

- La llamada a la API de eventos de datos proviene de una Cuenta de AWS distinta a la del propietario 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:::amzn-s3-demo-bucket2/"
  },
  {
    "accountId": "123456789012",
    "type": "AWS::S3::Bucket",
    "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
  }
]
```

El siguiente es el comportamiento actual.

```
# Current

"resources": [
  {
    "type": "AWS::S3::Object",
    "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
  },
  {
    "accountId": "",
    "type": "AWS::S3::Bucket",
    "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
  }
]
```

## 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 Consola de administración de AWS 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 condición `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.

### JSON

```
{  
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Sid": "AWSCloudTrailAclCheck20131101",
        "Effect": "Allow",
        "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
        "Action": "s3:GetBucketAcl",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
        "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:::amzn-s3-demo-bucket/optionalLogFilePrefix/AWSLogs/111111111111/*",
          "arn:aws:s3:::amzn-s3-demo-bucket/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 AWS CLI para crear registros de seguimiento en Cuentas de AWS adicionales y agregar sus archivos de registro a un bucket de Amazon S3. Como alternativa, es posible crear un registro de seguimiento de la organización para registrar todas las Cuentas de AWS que forman parte de una organización de AWS Organizations. Para obtener más información, consulte [Creación de un registro de seguimiento para una organización](#).

### 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 Consola de administración de AWS con la cuenta para la que desea crear un registro de seguimiento. Siga los pasos de [Creación de un registro de seguimiento con 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](#).

Storage location [Info](#)

☐ Create new S3 bucket  
Create a bucket to store logs for the trail.

☒ Use existing S3 bucket  
Choose an existing bucket to store logs for this trail.

## Trail log bucket name

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.



[Browse](#)

## Prefix - optional

Logs will be stored in cross-account-bucket-name/cross-account-bucket-prefix/

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 [Cloudtrail](#) en la Referencia de los comandos de la AWS CLI.

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 amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

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`.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333: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.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

```
]
}
```

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:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333: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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111111111111: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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],

```

```
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:Get*",
            "s3:List*"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
]
```

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.

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/Test"
    }
  ]
}
```

Para editar una política administrada por el cliente (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione 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. Realice una de las siguientes acciones:

- 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 Siguiente.

 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 al 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.

## Funcionamiento

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 Amazon 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 Consola de administración de AWS, 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 para validar la integridad de los archivos de registros de CloudTrail](#).

## 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 Consola de administración de AWS, 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.

### Consola de administración de AWS

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.
- El rol que ejecuta el comando debe tener permisos para llamar a `ListObjects`, `GetObject` y `GetBucketLocation` para cada bucket de S3 al que haga referencia el registro de seguimiento.

### 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 para validar la integridad de los archivos de registros de CloudTrail](#).

## 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 <amzn-s3-demo-bucket>] [--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 correspondientes 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<br><i>Huella digital</i> | No se ha encontrado la clave pública correspondiente a la huella digital registrada 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 no se pueden hacer afirmaciones sobre la actividad de la API en dichos archivos. |

| Tipo de archivo | Mensaje de validación                                                      | Descripción                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Digest file     | INVALID: Unable to load PKCS #1 key with fingerprint <i>Huella digital</i> | Dado que no se ha podido cargar la clave pública codificada DER en formato PKCS #1 que contiene la huella digital especificada, 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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1915Z_P0uvV87nu6pfAV2W.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1920Z_eQJteBBrfpBCq0qw.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz` valid

Digest file `s3://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-east-2_20150901T1910Z YYSFiuFQk4nrtnEW.json.gz` valid

[...]

Log file `s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz` valid

Log file `s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-east-2_20150901T1040Z_lLa3QzVLp0ed7igR.json.gz` valid



```
Digest file      s3://amzn-s3-demo-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://amzn-s3-demo-bucketAWSLogs/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://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFv03dwHo4NCqqc.json.gz valid
```

```
Digest file      s3://amzn-s3-demo-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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkE05kNcDnVhGh.json.gz valid
```

```
Log file         s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPR.json.gz valid
```

```
Log file         s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
```

```
Log file         s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
```

```
Digest file      s3://amzn-s3-demo-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://amzn-s3-demo-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://amzn-s3-demo-bucket/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://amzn-s3-demo-bucket/optional-prefix/AWSLogs/0-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": "amzn-s3-demo-bucket",  
  "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": "amzn-s3-demo-bucket",  
  "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": "amzn-s3-demo-bucket",
    "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHfT.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 se describe cada campo del archivo de resumen:

### awsAccountId

El ID de la cuenta de AWS para 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 de la AWS CLI [list-public-keys](#) 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": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
  "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  
28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af532229  
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 de 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 la [política de buckets de S3](#) de su registro de seguimiento está mal configurada o si CloudTrail sufre una interrupción inesperada del servicio, es posible que no reciba todos los archivos de resumen o algunos de ellos. Para confirmar si su registro de seguimiento presenta algún error en la entrega de resúmenes, ejecute el comando [get-trail-status](#) y compruebe si hay errores en el

parámetro LatestDigestDeliveryError. Una vez resuelto el problema de entrega (por ejemplo, corrigiendo la política de buckets), CloudTrail intentará volver a entregar los archivos de resumen que falten. Durante el período de reenvío, es posible que los archivos de resumen se entreguen desordenados, por lo que temporalmente podría parecer que la cadena está rota.

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 para validar la integridad de los archivos de registros de CloudTrail

Dado que CloudTrail utiliza funciones hash y algoritmos criptográficos estándar del sector, puede crear sus propias herramientas para validar la integridad de los archivos de registros de CloudTrail. Cuando se habilita la validación de la integridad de los archivos de registros, CloudTrail entrega 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.

### Cómo se firman los archivos de resumen de CloudTrail

Los archivos de resumen de CloudTrail 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 objetos de CloudTrail están incluidos 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. Sírvese 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 [GetObject](#) de S3 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 para validar el archivo de resumen, puede utilizar 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 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**

Dado que CloudTrail utiliza diferentes pares de claves pública/privada por región, cada archivo de resumen se firma con una clave privada única para 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": "MIIBCgKCAQEA11L2YZ9h7onug2ILi1MwyHiMRsTQjfWE
+phVRLk1QjfWhirG+lp0a8NrwQ/r7Ah5bNL6Hepzn0U9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8i0PFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuW07S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGndFtkS/4YSKcgqW0YDcawP9GGGDAeCIqPWIXDLG1j0jRRzWfCmD0iJUkz8vTsn4hq
      "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
    },
    {
      "ValidityStartTime": "1434589460.0",
      "ValidityEndTime": "1437181460.0",
      "Value": "MIIBCgKCAQEApfYL2FiZhpn74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDu02MDTZNIzNvBNzaBJ+r2WIWAJ/
```

```

Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BShrSM8RWuJIw7MXwF9iQncg9jYzU1NJomozQzAG5wSRfbplcCYNY40xvGd/aAm00m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
    "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
  },
  {
    "ValidityStartTime": "1434589370.0",
    "ValidityEndTime": "1437181370.0",
    "Value":
      "MIIBIjANBgkqhkiG9w0BAQEFAAA0CAQ8AMIIBCgKCAQEAlzPjbvZJ42UdcmLfPUqXYNf0s6I8lCfao/
t0s8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBaEXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMf0LN65PdLFudLP7Gat0Z9p5jw/
rjpcLKfo9Bfc3heeBxWGKwBB0KnFAa9V57p0aosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAE1DMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
    "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
  }
]
}

```

Utilice la API de CloudTrail para recuperar claves públicas

Para recuperar las claves públicas de los archivos de resumen 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 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 la solicitud

| Nombre    | Descripción                                                                                                                                                                                                                                                                 |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StartTime | Opcionalmente, especifique el inicio del intervalo de tiempo (en UTC) para buscar las claves públicas para los archivos de resumen de CloudTrail. Si StartTime no está especificado, se utiliza la hora actual y se devuelve la clave pública actual.<br><br>Tipo: DateTime |
| EndTime   | Opcionalmente, especifique el fin del intervalo de tiempo (en UTC) para buscar las claves públicas para los archivos de resumen de CloudTrail. Si EndTime no está especificado, se utiliza la hora actual.<br><br>Tipo: DateTime                                            |

## Elementos de respuesta

PublicKeyList, una matriz de objetos PublicKey que contiene:

| Name              | Descripción                                                                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Value             | El valor de clave pública codificado de DER en formato PKCS # 1.<br><br>Tipo: Blob                                                                                |
| ValidityStartTime | La hora de inicio de la validez de la clave pública.<br><br>Tipo: DateTime                                                                                        |
| ValidityEndTime   | La hora de finalización de la validez de la clave pública.<br><br>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.<br><br>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  
amzn-s3-demo-bucket/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 registros se ha modificado después de que CloudTrail lo haya entregado, los hashes 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:

- Dado que la firma digital del archivo de resumen anterior se encuentra en el archivo de resumen actual, empiece la validación desde el archivo de resumen que esté junto al último. 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 código de ejemplo muestra el código básico para validar archivos de resumen y archivos de registros 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 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"));
    }
}
}
}

```

## 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_Mu0Ks0htH1ar15ZZ.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 registra el contenido de los eventos de administración, de datos y de actividad de la red](#).

### 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. Para obtener más información, consulte la [Guía del usuario de Amazon EC2](#).

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-EXAMPLEaaff4840c22`.

```
{
  "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-EXAMPLEaaff4840c22"
          }
        ]
      }
    },
    "responseElements": {
      "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
      "instancesSet": {
        "items": [
          {
            "instanceId": "i-EXAMPLEaaff4840c22",
            "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-EXAMPLEaaff4840c22"
            }
        ]
    },
    "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-EXAMPLEaaff4840c22",
                "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": "AIDA60N6E4XEGIEEXAMPLE",
    "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": "AIDA60N6E4XEGITEXAMPLE",
    "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.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": "AIDA60N6E4XEP7EXAMPLE",
      "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": "AIDA60N6E4XEGIEEXAMPLE",
        "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": "{\n\"Version\":\n\"2012-10-17\",          \n\"Statement\n\":[{\n\"Effect\":\n\"Allow\", \n\"Action\":[\n\"sts:AssumeRole\"], \n\"Principal\":{\n\"Service\":\n[\n\"ec2.amazonaws.com\" ]\n}}]}\n",
    },
    "responseElements": {
      "role": {
        "assumeRolePolicyDocument": "policy-statement",
        "arn": "arn:aws:iam::777777777777:role/TestRole",
        "roleId": "AROAG0N6E4XEFFEXAMPLE",
        "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": "AIDA60N6E4XEGIEEXAMPLE",
    "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 [Trabajar con CloudTrail 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"
  }
}
```

## 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 para 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 -Dpgp.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 -Dpgp.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 -Dpgp.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` – identificador único de su cuenta, como `AKIAIOSFODNN7EXAMPLE`.
- `secretKey`: identificador único de su 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 `Builder` de `build()` 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 =
        LoggerFactory.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](#).

# Seguridad en AWS CloudTrail

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y el usuario. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puedes 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 de la sustitución confusa entre servicios](#)
- [Prácticas recomendadas de seguridad de AWS CloudTrail](#)
- [Cifrado de archivos de registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS \(SSE-KMS\)](#)

# Protección de los datos en AWS CloudTrail

El [modelo de responsabilidad compartida](#), y 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. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres 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, consulta las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta [Working with CloudTrail trails](#) en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

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 texto 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 y de resumen de CloudTrail se cifran mediante el cifrado del servidor (SSE) de Amazon S3. También puede optar por cifrar los archivos de registro y de resumen con una clave AWS Key Management Service (AWS KMS). Puede almacenar sus archivos de registro en su bucket 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 registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS \(SSE-KMS\)](#)
- [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 los 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 está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de CloudTrail. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

### Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo AWS CloudTrail funciona con IAM](#)
- [Ejemplos de políticas basadas en identidades de AWS CloudTrail](#)
- [AWS CloudTrailEjemplos de políticas basadas en recursos de](#)
- [Política de bucket de Amazon S3 para CloudTrail](#)
- [Política de bucket de Amazon S3 para resultados de consultas de CloudTrail Lake](#)
- [Política de temas de Amazon SNS para CloudTrail](#)
- [Solución de problemas de identidades de AWS CloudTrail y accesos](#)
- [Uso de roles vinculados a servicios para CloudTrail](#)
- [AWS Políticas de administradas por para AWS CloudTrail](#)

## Público

La forma en que utiliza AWS Identity and Access Management (IAM) varía en función del rol:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Solución de problemas de identidades de AWS CloudTrail y accesos](#))
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo AWS CloudTrail funciona con IAM](#))
- Administrador de IAM: escriba políticas para administrar el acceso (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 como Usuario raíz de la cuenta de AWS, un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de un origen de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales de Google/Facebook. Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In.

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

## Usuario raíz de la Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión llamada Cuenta de AWS del usuario raíz que tiene acceso completo a todos los Servicios de AWS y recursos. Recomendamos encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

## Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS con credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, proveedor de identidades web o Directory Service que accede a Servicios de AWS mediante credenciales de un origen de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center.

## Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte [Solicitar que los usuarios humanos utilicen la federación con un proveedor de identidades para acceder a AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

## Roles de IAM

Un [rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un usuario a un rol de IAM \(consola\)](#) o llamando a una operación

de la API de la AWS CLI o AWS. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) 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 define permisos cuando se asocia con una identidad o recurso. AWS evalúa estas políticas cuando una entidad principal realiza una solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

Mediante políticas, los administradores especifican quién tiene acceso a qué definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a los roles, que luego los usuarios pueden asumir. Las políticas de IAM definen permisos independientemente del método utilizado para realizar la operación.

### Políticas basadas en identidades

Las políticas basadas en identidad son documentos JSON de políticas de permisos que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, 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 la identidad pueden ser políticas integradas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, 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 políticas JSON que se asocian a un recurso. Los ejemplos incluyen 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. Debe [especificar una entidad principal](#) en una política en función de recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

## Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer el máximo de permisos concedidos por los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en la identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): establecen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCP\)](#) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. 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 acerca de cómo AWS decide si permitir 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 AWS CloudTrail funciona con IAM

Antes de utilizar IAM para administrar el acceso a CloudTrail, obtenga información sobre qué características de IAM se pueden utilizar con CloudTrail.



## Características de IAM que puede utilizar con AWS CloudTrail

| Característica de IAM                                                      | Compatibilidad con CloudTrail |
|----------------------------------------------------------------------------|-------------------------------|
| <a href="#">Políticas basadas en identidades</a>                           | Sí                            |
| <a href="#">Políticas basadas en recursos</a>                              | Parcial                       |
| <a href="#">Acciones de políticas</a>                                      | Sí                            |
| <a href="#">Recursos de políticas</a>                                      | Sí                            |
| <a href="#">Claves de condición de política (específicas del servicio)</a> | No                            |
| <a href="#">ACL</a>                                                        | No                            |
| <a href="#">ABAC (etiquetas en políticas)</a>                              | Sí                            |
| <a href="#">Credenciales temporales</a>                                    | Sí                            |
| <a href="#">Sesiones de acceso directo (FAS)</a>                           | Sí                            |
| <a href="#">Roles de servicio</a>                                          | Sí                            |
| <a href="#">Roles vinculados al servicio</a>                               | Sí                            |

Para obtener una perspectiva general sobre cómo funcionan CloudTrail y otros servicios de AWS con la mayoría de características de IAM, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

## Políticas basadas en identidades para CloudTrail

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. 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. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de las políticas de JSON de IAM](#) en la Guía del usuario de IAM.

## Ejemplos de políticas basadas en identidades para CloudTrail

Para ver ejemplos de políticas basadas en identidad de CloudTrail, consulte [Ejemplos de políticas basadas en identidades de AWS CloudTrail](#).

## Políticas basadas en recursos dentro de CloudTrail

### Compatibilidad con las políticas basadas en recursos: parcial

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los 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.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

CloudTrail admite los tipos de políticas basadas en recursos que se encuentran a continuación:

- Políticas basadas en recursos en los canales utilizados para las integraciones de CloudTrail Lake con orígenes de eventos externos a 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 acerca de la creación de integraciones con CloudTrail Lake, consulte [Creación de una integración con un origen de eventos externo a AWS](#).
- Las políticas basadas en recursos para controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Puede utilizar las políticas basadas en recursos para ofrecer acceso entre cuentas a los almacenes de datos de eventos.

- Las políticas basadas en recursos en los paneles para permitir que CloudTrail actualice un panel de CloudTrail Lake en el lapso que defina al establecer un programa de actualización para un panel. Para obtener más información, consulte [Establezca un programa de actualización de un panel personalizado con la consola de CloudTrail](#).

## Ejemplos

Para ver ejemplos de políticas basadas en recursos de CloudTrail, consulte [AWS CloudTrailEjemplos de políticas basadas en recursos de](#).

## Acciones de política para CloudTrail

Compatibilidad con las 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 conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de CloudTrail, consulte [Acciones definidas por AWS CloudTrail](#) en la Referencia de autorizaciones de servicio.

Las acciones de políticas de 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 se pueden 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 política para CloudTrail

Compatibilidad con los 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. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Para las acciones que no admiten permisos por recurso, utilice un carácter comodín (\*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de CloudTrail y sus ARN, consulte [Recursos definidos por AWS CloudTrail](#) en la Referencia de autorizaciones 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 cuatro tipos de recursos: registros de seguimiento, almacenes de datos de eventos, paneles y canales. Cada recurso tiene asociado un nombre de recurso de Amazon (ARN) único. En las políticas se emplean los nombres de recurso de Amazon (ARN) para identificar los recursos a los que se aplican las políticas. CloudTrail no admite otros tipos de recursos, que a veces se denominan subrecursos.

El recurso de registro de seguimiento de CloudTrail tiene el siguiente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

El recurso de almacén de datos de eventos de CloudTrail tiene el siguiente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

El recurso de panel de CloudTrail tiene el siguiente ARN:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/{DashboardName}
```

El recurso de canal de CloudTrail 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 acciones de CloudTrail, tales como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (\*).

```
"Resource": ""
```

En muchas acciones de la API de CloudTrail se utilizan 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 política para CloudTrail

Compatibilidad con 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` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puedes crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. 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 permite la utilización 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 las claves de condición de CloudTrail, consulte [Claves de condición para AWS CloudTrail](#) en la Referencia de autorizaciones 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

Compatibilidad con 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): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede asociar etiquetas a entidades de IAM y recursos de AWS y, a continuación, diseñar políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso.

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 [Definición de permisos con la autorización de 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.

Puede adjuntar etiquetas a los recursos de CloudTrail o transferirlas en una solicitud a CloudTrail. Para obtener más información sobre el etiquetado de CloudTrail, consulte [Creación de un registro de seguimiento con la consola de CloudTrail](#) y [Creación, actualización y administración de registros de seguimiento con la AWS CLI](#).

## Uso de credenciales temporales con CloudTrail

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a corto plazo a los recursos de AWS y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda que genere de forma dinámica credenciales temporales en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#) y [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

## Sesiones de acceso directo para CloudTrail

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan 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. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

## Roles de servicio para CloudTrail

Compatibilidad 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

Es posible que cambiar los permisos de un rol de servicio interrumpa la funcionalidad de CloudTrail. Edite los roles de servicio solo cuando CloudTrail proporcione orientación para hacerlo.

## Roles vinculados a servicios para CloudTrail

Admite roles vinculados a servicios: sí

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puedes 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 a un servicio para la 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 cómo crear o administrar roles vinculados a servicios de CloudTrail, consulte [Uso de roles vinculados a servicios para CloudTrail](#).

## Ejemplos de políticas basadas en identidades de AWS CloudTrail

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de CloudTrail. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por CloudTrail, incluido el formato de los ARN para cada tipo de recurso, consulte [Acciones, recursos y claves de condición para AWS CloudTrail](#) en la Referencia de autorizaciones de servicio.



## 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](#)
- [Conceder permisos personalizados a los usuarios de CloudTrail](#)

## Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos de CloudTrail de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comienza con las políticas administradas por AWS y continúa con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de tarea, utiliza las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas gestionadas por el cliente de AWS específicas para sus 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 tarea](#) en la Guía de 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 del 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, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, CloudFormation.

Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.

- Utiliza 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. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesite usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para obtener una mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

CloudTrail no tiene claves de contexto específicas de servicios que pueda utilizar en el elemento `Condition` de las instrucciones de política.

## 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*.

### JSON

```
{
  "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"
    ]
}
]
}
```

En el siguiente ejemplo se muestra una política que deniega explícitamente las acciones de CloudTrail para cualquier registro de seguimiento que no se denomine *My-First-Trail*.

## JSON

```

{
  "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

Puede utilizar los permisos y las políticas para controlar la capacidad de un usuario para realizar acciones específicas en el registro de seguimiento de CloudTrail.

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`.

JSON

```
{
  "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, las acciones `DescribeTrails` y `GetTrailStatus` están permitidas en todos los recursos de CloudTrail:

JSON

```
{
  "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": "amzn-s3-demo-bucket",
      "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.

### JSON

```
{
  "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.

## JSON

```
{
  "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 registrar y consultar los detalles acerca de los recursos de CloudTrail en su Cuenta 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 el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.



## Concesión de permisos para la administración de CloudTrail

Para permitir a los usuarios o roles de IAM administrar un recurso de CloudTrail, como un registro de seguimiento, un almacén de datos de eventos o un canal, debe conceder permisos de manera explícita para que lleven a cabo las acciones asociadas a las tareas de CloudTrail. En la mayoría de las situaciones, puede utilizar una política administrada de AWS que contenga los permisos predefinidos.

### Note

Los permisos que conceda a los usuarios para hacer tareas de administración de CloudTrail no son los mismos que los permisos que CloudTrail requiere para enviar los archivos de registro a buckets de Amazon S3 o enviar notificaciones a 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 requiere un rol que pueda adoptar para enviar los eventos a un grupo de registros de CloudWatch Logs. Debe crear el rol que usa CloudTrail. Para obtener más información, consulte [Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la consola de CloudTrail](#) y [Envío de eventos a Amazon CloudWatch Logs](#).

Las siguientes políticas administradas de AWS están disponibles para CloudTrail:

- [AWSCloudTrail\\_FullAccess](#) – esta política proporciona acceso completo a las acciones de CloudTrail en los recursos de CloudTrail, como los registros de seguimiento, los almacenes de datos de eventos y los canales. Esta política proporciona los permisos necesarios para crear, actualizar y eliminar registros de seguimiento, almacenes de datos de eventos y canales de CloudTrail.

Esta política también ofrece permisos para administrar el bucket de Amazon S3, el grupo de registro de Registros de CloudWatch y un tema de Amazon SNS para un registro de seguimiento. Sin embargo, la política administrada `AWSCloudTrail_FullAccess` no proporciona permisos para eliminar el bucket de Amazon S3, el grupo de registro de Registros de CloudWatch 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 concede permisos para ver la consola de CloudTrail, incluidos los últimos eventos 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 gestionados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en [Creación de un rol para un proveedor de identidad 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 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 llevar a cabo 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": "*"
    }
  ]
}
```

```
}
```

## Conceder permisos personalizados a los usuarios de CloudTrail

Las políticas de CloudTrail conceden permisos a los usuarios que trabajan con CloudTrail. Si necesita conceder diferentes permisos a los usuarios, puede adjuntar una política de CloudTrail a un grupo o a un usuario de IAM. 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](#)
- [Concesión de permisos para ver la información de AWS Config en la consola de CloudTrail](#)
- [Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la consola de CloudTrail](#)
- [Información adicional](#)

### Acceso de solo lectura

En el siguiente ejemplo se muestra una política que concede acceso de solo lectura al registro de seguimiento de 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.

### JSON

```
{
  "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. Para las políticas que controlan el acceso a las acciones de CloudTrail, el elemento `Resource` está establecido en `*`, un carácter 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 las acciones de CloudTrail que finalizan con “Logging” Registrar (`StartLogging`, `StopLogging`).

- `"Action": ["cloudtrail:*"]`

Esto permite todas las acciones de CloudTrail, pero no las acciones para otros servicios de AWS.

- `"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 completa de acciones de CloudTrail, consulte [Referencia de la API de AWS CloudTrail](#).

### Acceso completo

En el siguiente ejemplo se muestra una política que concede acceso completo a CloudTrail. Equivale a la política administrada `AWSCloudTrail_FullAccess`. Se concede a los usuarios el permiso para

realizar todas las acciones de CloudTrail. También permite a los usuarios registrar eventos de datos en Amazon S3 y AWS Lambda, administrar archivos en buckets de Amazon S3, administrar cómo CloudWatch Logs monitorea los eventos de registro de CloudTrail y administrar 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.

## JSON

```
{
  "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:::amzn-s3-demo-logging-bucket1*"
        ]
    },
    {
        "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": "*"
}
]
}

```

## Concesión de permisos para ver la información de AWS Config en la consola de CloudTrail

Puede consultar la información del evento en la consola de CloudTrail, 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.

## JSON

```
{
  "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 con AWS Config](#).

Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la consola de CloudTrail

Puede ver y configurar el envío de eventos a CloudWatch Logs en la consola de CloudTrail si tiene los permisos necesarios. Estos permisos pueden ser más amplios que los que se conceden a los administradores de CloudTrail. Adjunte esta política a los administradores que van a configurar y administrar la integración de CloudTrail con CloudWatch Logs. La política no les concede permisos en CloudTrail o en CloudWatch Logs directamente, sino que concede los permisos necesarios para crear y configurar el rol que CloudTrail adoptará para enviar los eventos correctamente al grupo de CloudWatch Logs.

## JSON

```
{
  "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.

## AWS CloudTrailEjemplos de políticas basadas en recursos de

En esta sección se ofrecen ejemplos de las políticas basadas en recursos para los paneles de CloudTrail Lake, los almacenes de datos de eventos y los canales.

CloudTrail admite los tipos de políticas basadas en recursos que se encuentran a continuación:

- Políticas basadas en recursos en los canales utilizados para las integraciones de CloudTrail Lake con orígenes de eventos externos a 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 acerca de la creación de integraciones con CloudTrail Lake, consulte [Creación de una integración con un origen de eventos externo a AWS](#).
- Las políticas basadas en recursos para controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos. Puede utilizar las políticas basadas en recursos para ofrecer acceso entre cuentas a los almacenes de datos de eventos.
- Las políticas basadas en recursos en los paneles para permitir que CloudTrail actualice un panel de CloudTrail Lake en el lapso que defina al establecer un programa de actualización para un

panel. Para obtener más información, consulte [Establezca un programa de actualización de un panel personalizado con la consola de CloudTrail](#).

Ejemplos:

- [Ejemplos de política basada en recursos para los canales](#)
- [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#)
- [Ejemplo de política basada en recursos para un panel](#)

## Ejemplos de política basada en recursos para los canales

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.

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 Cuenta de AWS del socio y requiere que introduzca 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 introducir un ID externo para evitar un suplente confuso.

Estos son los requisitos de la política basada en recursos:

- La política contiene como mínimo una instrucción. La política puede tener como máximo 20 instrucciones.
- Cada instrucción contiene como mínimo una entidad principal. Una entidad principal es una cuenta, un rol o un usuario federado. Una instrucción puede tener como máximo 50 entidades principales.
- 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`

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 las entidades principales con `arn:aws:iam::111122223333:root`, `arn:aws:iam::444455556666:root` y `arn:aws:iam::123456789012:root` del ARN para llamar a la API [PutAuditEvents](#) del canal de CloudTrail con el ARN `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`.

## JSON

```
{
  "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 las entidades principales con `arn:aws:iam::111122223333:root`, `arn:aws:iam::444455556666:root` y `arn:aws:iam::123456789012:root` del ARN para llamar a la API [PutAuditEvents](#) en el recurso del canal de CloudTrail si la llamada a la API `PutAuditEvents` incluye el valor del ID externo definido en la política.

JSON

```
{
  "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"
    }
  ]
}
```

## Ejemplos de políticas basadas en recursos para almacenes de datos de eventos

Las políticas basadas en recursos le permiten controlar qué entidades principales pueden realizar acciones en el almacén de datos de eventos.

Puede utilizar políticas basadas en recursos para ofrecer acceso entre cuentas y permitir que las entidades principales seleccionadas consulten al almacén de datos de eventos, enumeren y cancelen consultas y vean los resultados de las consultas.

Para el panel de CloudTrail Lake, se utilizan políticas basadas en recursos para permitir que CloudTrail ejecute consultas en los almacenes de datos de eventos para completar los datos de los widgets del panel cuando este se actualiza. CloudTrail Lake le ofrece la opción de adjuntar una política basada en recursos predeterminada a sus almacenes de datos de eventos cuando [crea un panel personalizado](#) o [habilita el panel de Highlights](#) en la consola de CloudTrail.

Las políticas basadas en recursos para los almacenes de datos de eventos admiten las siguientes acciones:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Al [crear](#) o [actualizar](#) almacén de datos de eventos, o al administrar paneles en la consola de CloudTrail, tiene la opción de agregar una política basada en recursos al almacén de datos de eventos. También puede ejecutar el comando [put-resource-policy](#) para asociar una política basada en recursos a un almacén de datos de eventos.

Una política basada en recursos consta de una o varias instrucciones. Por ejemplo, puede incluir una instrucción que permita a CloudTrail consultar el almacén de datos de eventos para un panel y otra que permita el acceso entre cuentas para consultar el almacén de datos de eventos. Puede [actualizar](#) la política basada en recursos de un almacén de datos de eventos existente desde la página de detalles del almacén de datos de eventos en la consola de CloudTrail.

Para los [almacenes de datos de eventos de la organización](#), CloudTrail crea una [política basada en los recursos predeterminada](#) que enumera las acciones que las cuentas del administrador delegado pueden realizar en los almacenes de datos de eventos de la organización. Los permisos de esta política se obtienen de los permisos del administrador delegado en AWS Organizations. Esta política se actualiza de manera automática tras los cambios en el almacén de datos de eventos de la organización o en la organización (por ejemplo, si se registra o elimina una cuenta de administrador delegado de CloudTrail).

Ejemplos:

- [Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel](#)
- [Ejemplo: permitir que otras cuentas consulten un almacén de datos de eventos y vean los resultados de la consulta](#)

Ejemplo: permitir que CloudTrail ejecute consultas para actualizar un panel

Para completar los datos en un panel de CloudTrail Lake durante una actualización, debe permitir que CloudTrail ejecute consultas en su nombre. Para que esto suceda, adjunte una política basada en recursos a cada almacén de datos de eventos asociado a un widget de panel que incluya una declaración que permita a CloudTrail realizar la operación `StartQuery` para completar los datos del widget.

A continuación, se muestran los requisitos para la instrucción:

- La única `Principal` es `cloudtrail.amazonaws.com`.
- La única `Action` permitida es `cloudtrail:StartQuery`.
- La `Condition` solo incluye los ARN y el ID de la Cuenta de AWS del panel. Para `AWS:SourceArn`, puede ofrecer una variedad de ARN del panel.

El siguiente ejemplo de política incluye una instrucción que permite a CloudTrail ejecutar consultas en un almacén de datos de eventos para dos paneles personalizados denominados `example-dashboard1` y `example-dashboard2` y el panel de Highlights denominado `AWSCloudTrail-Highlights` para la cuenta `123456789012`.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "cloudtrail:StartQuery"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
                "StringLike": {
                    "AWS:SourceArn": [
                        "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/example-dashboard1",
                        "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/example-dashboard2",
                        "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/AWSCloudTrail-Highlights"
                    ]
                },
                "AWS:SourceAccount": "123456789012"
            }
        }
    ]
}

```

Ejemplo: permitir que otras cuentas consulten un almacén de datos de eventos y vean los resultados de la consulta

Puede utilizar las políticas basadas en recursos para ofrecer acceso entre cuentas a los almacenes de datos de eventos para permitir que otras cuentas puedan ejecutar consultas en los almacenes de datos de eventos.

El siguiente ejemplo de política incluye una instrucción que permite a los usuarios raíz en las cuentas 111122223333, 777777777777, 999999999999 y 111111111111 ejecutar consultas y obtener los resultados de las consultas en el almacén de datos de eventos propiedad del ID de la cuenta 555555555555.



## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "policy1",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::777777777777:root",
          "arn:aws:iam::999999999999:root",
          "arn:aws:iam::111111111111:root"
        ]
      },
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetQueryResults"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:555555555555:eventdatastore/example80-699f-4045-a7d2-730dbf313ccf"
    }
  ]
}
```

## Ejemplo de política basada en recursos para un panel

Puede establecer un programa de actualización para un panel de CloudTrail Lake, lo que permite a CloudTrail actualizar el panel en su nombre en el plazo que defina cuando configure el programa de actualización. Para ello, debe adjuntar una política basada en recursos al panel para permitir que CloudTrail realice la operación `StartDashboardRefresh` en su panel.

Estos son los requisitos de la política basada en recursos:

- La única `Principal` es `cloudtrail.amazonaws.com`.
- La única `Action` permitida en la política es `cloudtrail:StartDashboardRefresh`.
- La `Condition` solo incluye el ARN y el ID de la Cuenta de AWS del panel.

El siguiente ejemplo de política permite a CloudTrail actualizar un panel denominado `exampleDash` de la cuenta `123456789012`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": [
        "cloudtrail:StartDashboardRefresh"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/exampleDash",
          "AWS:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

## 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 [Creación de un registro de seguimiento para una organización con la AWS CLI](#).

Para enviar archivos de registros a un bucket de S3, CloudTrail debe tener los permisos necesarios y no se puede configurar 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.
- El nombre de la carpeta donde se almacenan los archivos de registro, incluido el nombre del bucket, un prefijo (si se ha especificado) y su ID de cuenta de AWS.

Como práctica recomendada de seguridad, agregue una clave de condición `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 una traza o trazas 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.

#### 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.

La siguiente política permite a CloudTrail escribir archivos de registros en el bucket desde Regiones de AWS compatibles. Reemplace *amzn-s3-demo-bucket*, *[optionalPrefix]/*, *myAccountID*, *region* y *trailName* con los valores adecuados para la configuración.

Política de bucket de S

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "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:::amzn-s3-demo-
        bucket/[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 acerca de Regiones de AWS, consulte [Regiones compatibles con CloudTrail](#).

## Contenido

- [Especificar un bucket existente para el envío de registros de CloudTrail](#)

- [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](#)

## Especificar un bucket existente para el envío de registros de CloudTrail

Si especificó un bucket de S3 como ubicación de almacenamiento para el envío de archivos de registros, debe adjuntar una política al bucket que permita a CloudTrail escribir en él.

### Note

Es recomendable que utilice un bucket de S3 dedicado para los archivos de registro 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 archivos de registros y, a continuación, seleccione Permissions (Permisos).
3. Seleccione 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 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 van a tener acceso al bucket.

## Recibir archivos de registro de otras cuentas

Puede configurar CloudTrail para que envíe los archivos de registro de varias cuentas de AWS a un único bucket de S3. Para obtener más información, consulte [Recepción de archivos de registro de CloudTrail 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 bucket debe tener una política que permita a CloudTrail guardar los archivos de registros de la organización en el bucket.

A continuación, se muestra un ejemplo de política para un bucket de Amazon S3 denominado *amzn-s3-demo-bucket*, que es propiedad de la cuenta de administración de la organización. Reemplace *amzn-s3-demo-bucket*, *region*, *managementAccountID*, *trailName* y *o-organizationID* por los valores de su organización.

Esta política de bucket contiene tres instrucciones.

- La primera instrucción permite a CloudTrail hacer una llamada a la acción `GetBucketAcl` 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 CloudTrail escribe en el bucket de S3 solo para una traza o trazas 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.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "cloudtrail.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "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:::amzn-s3-demo-bucket/
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:::amzn-s3-demo-bucket/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.

### 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.



## Errores comunes en la configuración de la política de Amazon S3

Cuando crea un bucket nuevo como parte de la creación o actualización de un registro de seguimiento, CloudTrail adjunta los permisos necesarios al bucket. La política de bucket utiliza el nombre de la entidad principal del servicio, "cloudtrail.amazonaws.com", que permite a CloudTrail enviar archivos de registro de todas las regiones.

Si CloudTrail no envía registros para una región, es posible que el bucket tenga una política antigua que especifique los ID de cuenta de CloudTrail de cada región. Esta política concede a CloudTrail permiso para enviar registros solo de las regiones especificadas.

Recomendamos que actualice la política para utilizar un permiso con el nombre principal del servicio de CloudTrail. Para ello, sustituya los ARN del ID de cuenta por el nombre principal del servicio: "cloudtrail.amazonaws.com". De este modo, se concederá a CloudTrail permiso para enviar registros de las regiones nuevas y actuales. 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: Reemplace *amzn-s3-demo-bucket*, *[optionalPrefix]/*, *myAccountID*, *region* y *trailName* con los valores adecuados para la configuración.

Example Ejemplo de política de bucket con nombre principal del servicio

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20150319",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "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:::amzn-s3-demo-
bucket/[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 solucionar este problema, utilice la consola de Amazon S3 para actualizar el prefijo en la política del bucket y, a continuación, utilice la consola de CloudTrail para especificar el mismo prefijo para el bucket en el registro de seguimiento.

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. Seleccione 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:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*",

```

5. Seleccione Save.
6. Abra la consola de CloudTrail 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 Save.

## 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 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 condición `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 *amzn-s3-demo-bucket*, *myAccountID* y

*myQueryRunningRegion* 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 S

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailLake1",
      "Effect": "Allow",
      "Principal": {"Service": "cloudtrail.amazonaws.com"},
      "Action": [
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:sourceAccount": "111111111111"
        }
      }
    }
  ]
}
```

```

        "ArnLike": {
            "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
        }
    },
    {
        "Sid": "AWSCloudTrailLake2",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "s3:GetBucketAcl",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
        "Condition": {
            "StringEquals": {
                "aws:sourceAccount": "111111111111"
            },
            "ArnLike": {
                "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111: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. Seleccione 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 de temas de Amazon SNS para CloudTrail

Para enviar notificaciones a un tema de SNS, CloudTrail debe tener los permisos necesarios. CloudTrail adjunta de forma automática los permisos necesarios al bucket cuando crea un tema de Amazon SNS como parte de la creación o actualización de un registro de seguimiento en la consola de CloudTrail.

**⚠ 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 agrega de forma automática la siguiente instrucción a la política con los siguientes campos:

- Los SID permitidos
- El nombre principal del servicio para CloudTrail.
- El tema de SNS, incluida la región, el ID de cuenta y el nombre del tema.

La siguiente política permite que CloudTrail envíe notificaciones sobre el envío de archivos de registro desde las regiones admitidas. Para obtener más información, consulte [Regiones compatibles con CloudTrail](#). 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

#### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailSNSPolicy20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:111111111111:SNSTopicName"
    }
  ]
}
```

```
]
}
```

Si desea utilizar un tema de Amazon SNS cifrado con AWS KMS para enviar notificaciones, también debe habilitar la compatibilidad entre la fuente del evento (CloudTrail) y el tema cifrado al agregar la siguiente instrucción a la política de AWS KMS key.

## Política de claves de KMS

### JSON

```
{
  "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 los orígenes de eventos de los servicios de AWS 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 a una región](#)
  - [CloudTrail no envía notificaciones a una cuenta de miembro de una organización](#)



- [Recursos adicionales](#)

## Práctica recomendada de seguridad para la política de temas SNS

De forma predeterminada, la instrucción de política de IAM que CloudTrail adjunta al tema de Amazon SNS permite que la entidad de servicio de CloudTrail publique en un tema SNS, identificado por un ARN. Para evitar que un atacante obtenga acceso al tema de SNS y envíe notificaciones en nombre de CloudTrail a los destinatarios del tema, edite de forma manual la política de temas de CloudTrail SNS para agregar una clave de condición `aws:SourceArn` o a la instrucción 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 agregar claves de condición a la política de temas de SNS, obtenga el nombre del tema de SNS de la configuración del registro de seguimiento en la consola de 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 registro de seguimiento de CloudTrail. En este ejemplo se restringe el acceso al tema de SNS solo a los usuarios que pueden iniciar sesión en la cuenta 123456789012 de AWS.

```
{
  "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 agregar de forma manual los permisos para 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 de 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. Seleccione **Editar** y, a continuación, desplácese hacia abajo hasta **Política de acceso**.
4. Elija la instrucción de [SNS topic policy](#) con los valores adecuados para la región, el ID de cuenta y el nombre del tema.

5. Si su tema es cifrado, debe conceder a CloudTrail los permisos `kms:GenerateDataKey*` y `kms:Decrypt`. Para obtener más información, consulte [Encrypted SNS topic KMS key policy](#).
6. Elija Save changes (Guardar cambios).
7. Vuelva a la consola de CloudTrail y especifique el tema para el registro de seguimiento.

## 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 a una región](#)
- [CloudTrail no envía notificaciones a una cuenta de miembro de una organización](#)

### CloudTrail no envía notificaciones a una región

Al crear un tema nuevo como parte de la creación o actualización de un registro de seguimiento, CloudTrail adjunta los permisos necesarios al tema. La política de temas utiliza el nombre de la entidad principal del servicio, `"cloudtrail.amazonaws.com"`, que permite a CloudTrail enviar notificaciones a todas las regiones.

Si CloudTrail no envía notificaciones para una región, es posible que el tema tenga una política antigua que especifique los ID de cuenta de CloudTrail para cada región. Este tipo de política concede a CloudTrail permiso para enviar notificaciones solo a las regiones especificadas.

Recomendamos que actualice la política para utilizar un permiso con el nombre principal del servicio de CloudTrail. Para ello, sustituya los ARN del ID de cuenta por el nombre principal del servicio: `"cloudtrail.amazonaws.com"`.

El siguiente ejemplo de política permite que CloudTrail envíe notificaciones para las regiones nuevas y actuales:

Example política del tema con el nombre principal del servicio

JSON

```
{  
  "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 a una cuenta de miembro de una organización

Si una cuenta de miembro con un registro de seguimiento de la organización de AWS Organizations no envía notificaciones de Amazon SNS, podría haber un problema con la configuración de la política de temas de SNS. CloudTrail crea registros de seguimiento de la organización en las cuentas de miembros incluso si hay algún error durante la validación de un recurso; por ejemplo, el tema de SNS del registro de seguimiento de la organización no incluye todos los ID de las cuentas de 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 un registro de seguimiento tiene un error de autorización:

- Desde la consola de CloudTrail, consulte la página de detalles del registro de seguimiento. Si se produce un error en la autorización, la página de detalles incluye una advertencia de SNS `authorization failed` e indica que hay que corregir la política de temas de SNS.
- Desde AWS CLI, ejecute el comando [get-trail-status](#). Si se produce un error de autorización, el resultado del comando incluye el campo `LastNotificationError` con un valor de `AuthorizationError`.

## Recursos adicionales

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 para diagnosticar y solucionar los problemas comunes que pueden surgir al trabajar con CloudTrail y IAM.

## Temas

- [No tengo autorización para realizar una acción en CloudTrail](#)
- [No tengo autorización para llevar a cabo iam:PassRole](#)
- [Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de 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 tengo autorización para realizar una 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 gestor de AWS. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

Si la Consola de administración de AWS le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su gestor para recibir ayuda. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente error de ejemplo se produce cuando el usuario de IAM mateojackson intenta utilizar la consola para ver los detalles de un registro de seguimiento, pero no tiene la política administrada

correspondiente de CloudTrail (AWSCloudTrail\_FullAccess o AWSCloudTrail\_ReadOnlyAccess) o los permisos equivalentes aplicados a la cuenta.

```
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 inició sesión con un usuario o un rol de IAM que tiene la política administrada AWSCloudTrail\_FullAccess o los permisos equivalentes y no puede configurar la integración de AWS Config o Registros de Amazon CloudWatch con un registro de seguimiento; es posible que no tenga los permisos necesarios para la integración con dichos servicios. Para obtener más información, consulte [Concesión de permisos para ver la información de AWS Config en la consola de CloudTrail](#) y [Concesión de permisos para ver y configurar la información de Amazon CloudWatch Logs en la consola de CloudTrail](#).

## No tengo autorización para llevar a cabo **iam:PassRole**

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar 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 llevar a cabo una acción en CloudTrail. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen 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 gestor de AWS. El gestor es la persona que le proporcionó las credenciales de inicio de sesión.

## Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de CloudTrail

Puede crear un rol y compartir la información de CloudTrail entre varias Cuentas 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 obtener más información, consulte lo siguiente:

- Para saber si CloudTrail admite estas características, consulte [Cómo AWS CloudTrail funciona con IAM](#).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Acceso para un usuario de IAM en otra Cuenta de AWS propia](#) en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulta [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 una federación de identidades, consulta [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) 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 llevar a cabo la acción `iam:PassRole`, las políticas se deben actualizar 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 llevar a cabo una acción en CloudTrail. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen 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 gestor de AWS. El gestor 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 CLI de AWS Organizations o la operación de la API, los roles vinculados al servicio de CloudTrail no se crean de manera automática si no existen. Los roles vinculados al servicio solo se crean al realizar una llamada desde la cuenta de administración directamente al servicio de CloudTrail. Por ejemplo, cuando agrega un administrador delegado o crear un registro de seguimiento de la organización o un almacén de datos de eventos con la consola de CloudTrail, AWS CLI o la API de CloudTrail, se crea el rol vinculado al servicio de `AWSServiceRoleForCloudTrail`.

Al agregar un administrador delegado mediante la AWS CloudTrail, operación de CLI o API, CloudTrail crea los roles vinculados al servicio de `AWSServiceRoleForCloudTrail` y `AWSServiceRoleForCloudTrailEventContext`.

Cuando utiliza la cuenta de administración de su organización para agregar un administrador delegado o crear un registro de seguimiento de la organización o un almacén de datos de eventos en la consola de CloudTrail, o si utiliza la AWS CLI o la API de CloudTrail, CloudTrail crea de manera automática un rol vinculado a un servicio `AWSServiceRoleForCloudTrail` para su cuenta de administración si aún no existe. Para obtener más información, consulte [Uso de roles vinculados a servicios para CloudTrail](#).

Si no ha agregado un administrador delegado, utilice la consola de CloudTrail, la AWS CLI o la API de CloudTrail para agregar el administrador delegado. Para obtener más información acerca de cómo agregar un administrador delegado, consulte [Cómo agregar un administrador delegado de CloudTrail](#) y [RegisterOrganizationDelegatedAdmin](#) (API).

Si ya ha agregado el administrador delegado, utilice la cuenta de administración para crear el registro de seguimiento de la organización o el almacén de datos de eventos en la consola de CloudTrail o mediante la AWS CLI o la API de CloudTrail. Para obtener más información sobre la creación de un registro de seguimiento de la organización, consulte [Creación de un registro de seguimiento para la organización en la consola](#), [Creación de un registro de seguimiento para una organización con la AWS CLI](#) y [CreateTrail](#) (API).

## Uso de roles vinculados a servicios para CloudTrail

AWS CloudTrail utiliza [roles vinculados a servicios](#) de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está 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.

### Temas

- [Utilizar roles para crear y administrar registros de seguimiento de la organización de CloudTrail y almacenes de datos de eventos de la organización de CloudTrail Lake en CloudTrail](#)
- [Regiones admitidas para roles vinculados a servicios de CloudTrail](#)
- [Utilizar los roles para crear y administrar el contexto de eventos de CloudTrail en CloudTrail](#)
- [Regiones admitidas para roles vinculados a servicios de CloudTrail](#)

## Utilizar roles para crear y administrar registros de seguimiento de la organización de CloudTrail y almacenes de datos de eventos de la organización de CloudTrail Lake en 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.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de CloudTrail, ya que se evita que usted pueda eliminar de manera accidental los permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte [Servicios de AWS que funcionan con IAM](#) y busque aquellos para los que aparezca Sí en la columna Roles vinculados al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

### Permisos de roles vinculados a servicios para 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`

La política de permisos del rol conocida como `CloudTrailServiceRolePolicy` 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 los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Para obtener más información sobre la política administrada que se asocia a `AWSServiceForCloudTrail`, consulte [AWS Políticas de administradas por para AWS CloudTrail](#).

### 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, en la Consola de administración de AWS, la AWS CLI o la API AWS, CloudTrail crea el rol vinculado al servicio por usted.

Si elimina este rol vinculado a servicios 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 en la consola de CloudTrail, CloudTrail vuelve a crear el rol vinculado al servicio por usted.

### Edición de un rol vinculado a un servicio para CloudTrail

CloudTrail no permite editar el rol `AWSServiceRoleForCloudTrail` vinculado al servicio. 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 [Editar 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:

- Elimine 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 con la consola de CloudTrail](#).
- 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 con la consola](#).
- Eliminar el registro de seguimiento. Para obtener más información, consulte [Eliminación de un registro de seguimiento con la consola de CloudTrail](#).
- Elimine el almacén de datos de eventos. Para obtener más información, consulte [Eliminar un almacén de datos de eventos con la consola](#).

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a un servicio de `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 [Regiones y puntos de enlace de AWS](#) en la Referencia general de AWS.

## Utilizar los roles para crear y administrar el contexto de eventos de CloudTrail en 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.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de CloudTrail, ya que se evita que se puedan eliminar de manera accidental los permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte [Servicios de AWS que funcionan con IAM](#) y busque aquellos para los que aparezca Sí en la columna Roles vinculados al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

### Permisos de roles vinculados a servicios para CloudTrail

CloudTrail utiliza el rol vinculado al servicio denominado `AWSServiceRoleForCloudTrailEventContext`: este rol vinculado al servicio se utiliza para administrar las reglas de CloudTrail Event Context y EventBridge.

El rol vinculado al servicio `AWSServiceRoleForCloudTrailEventContext` confía en los siguientes servicios para asumir el rol:

- `context.cloudtrail.amazonaws.com`

La política de permisos del rol conocida como `CloudTrailEventContext` permite que CloudTrail realice las siguientes acciones en los recursos especificados:

- Acciones en las etiquetas de recursos:
  - `tag:GetResources`

- Acciones en todos los recursos de Amazon EventBridge para que la entidad principal del servicio de CloudTrail cree reglas:
  - `events:PutRule`
- Acciones en todos los recursos de Amazon EventBridge para que la entidad principal del servicio de CloudTrail administre las reglas que crea:
  - `events:PutTargets`
  - `events>DeleteRule`
  - `events:RemoveTargets`
  - `events:RemoveTargets`
- Acciones en todos los recursos de Amazon EventBridge para que la entidad principal del servicio de CloudTrail describa las reglas que crea:
  - `events:DescribeRule`
  - `events:DeRegisterResource`
- Acciones en todos los recursos de Amazon EventBridge:
  - `events:ListRules`

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Para obtener más información acerca de la política administrada que se asocia a `AWSServiceRoleForCloudTrailEventContext`, consulte [AWS Políticas de administradas por para AWS CloudTrail](#).

### Creación de un rol vinculado a un servicio para CloudTrail

No necesita crear manualmente un rol vinculado a servicios. Cuando comience a utilizar la característica de eventos de contexto en la Consola de administración de AWS, la AWS CLI o la API AWS, CloudTrail creará el rol vinculado al servicio por usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando comience a utilizar la característica de eventos de contexto, CloudTrail vuelve a crear el rol vinculado al servicio por usted.

## Edición de un rol vinculado a un servicio para CloudTrail

CloudTrail no permite editar el rol vinculado al servicio `AWSServiceRoleForCloudTrailEventContext`. 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 [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Eliminar el rol vinculado al servicio `AWSServiceRoleForCloudTrailEventContext` de CloudTrail

Si ya no necesita usar una característica o servicio que requieran un rol vinculado al servicio `AWSServiceRoleForCloudTrailEventContext`, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo de manera manual mediante la eliminación de la clave `TagContext` de los almacenes de datos de eventos.

### 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 los recursos de CloudTrail que utiliza el rol vinculado al servicio `AWSServiceRoleForCloudTrailEventContext`

1. En el terminal o la línea de comandos, ejecute el comando `put-event-configuration` del almacén de eventos del que quiera eliminar la clave de `TagContext`. Por ejemplo, para eliminar la clave de `TagContext` de un almacén de eventos de la cuenta **11112223333** de la región Este de EE. UU. (Ohio) con un ARN de **`arn:aws:cloudtrail:us-east-2:11112223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`**, en el que `TagContext` es el único selector de claves de contexto, usted utilizaría el comando `put-event-configuration` sin especificar ningún valor para `--context-key-selectors`:

```
aws cloudtrail put-event-configuration --event-data-store arn:aws:cloudtrail:us-east-2:11112223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --max-event-size Large --context-key-selectors
```



2. Repita este comando para todos los almacenes de datos de todas las regiones de la división. Para obtener más información, consulte [Identificar los recursos de AWS con nombres de recursos de Amazon \(ARN\)](#).

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilizar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForCloudTrailEventContext. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Regiones admitidas para roles vinculados a servicios de CloudTrail

CloudTrail permite el uso de roles vinculados al servicios en todas las regiones en las que tanto CloudTrail como EventBridge estén disponibles. Para obtener más información, consulte [Puntos de conexión y Regiones de AWS](#).

## AWS Políticas de administradas por 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 gestionadas 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 ReadOnlyAccess proporciona acceso de solo lectura a todos los servicios y los 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 descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

## AWS Política administrada por: **AWSCloudTrail\_FullAccess**

Una identidad de usuario que tiene la política de [AWSCloudTrail\\_FullAccess](#) asociada a su rol tiene acceso administrativo completo en CloudTrail.

Para obtener información de una lista de JSON de la política, consulte [AWSCloudTrail\\_FullAccess](#) en la Guía de referencia de políticas administradas por AWS.

## AWS Política administrada por: **AWSCloudTrail\_ReadOnlyAccess**

Una identidad de usuario que tenga asociada la política de [AWSCloudTrail\\_ReadOnlyAccess](#) a su rol puede realizar acciones de solo lectura en CloudTrail, tales como las acciones `Get*`, `List*` y `Describe*` en los registros de seguimiento, los almacenes de datos de eventos de CloudTrail Lake o las consultas de Lake.

Para obtener información de una lista de JSON de la política, consulte [AWSCloudTrail\\_ReadOnlyAccess](#) en la Guía de referencia de políticas administradas por AWS.

## AWS Política administrada por: **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.

Para obtener información de una lista de JSON de la política, consulte [CloudTrailServiceRolePolicy](#) en la Guía de referencia de políticas administradas por AWS.

## AWS Política administrada por: **CloudTrailEventContext**

La política de [CloudTrailEventContext](#) permite que AWS CloudTrail administre el contexto de eventos de CloudTrail y las reglas de EventBridge en su nombre. La política incluye los permisos de EventBridge necesarios para crear, administrar y describir las reglas que crea para usted.

Esta política va adjunta a un rol vinculado a un servicio `AWSServiceRoleForCloudTrailEventContext` que permite a CloudTrail realizar acciones en su nombre. No puede asociar esta política a los usuarios, grupos o roles.

Para obtener información de una lista de JSON de la política, consulte [CloudTrailEventContext](#) en la Guía de referencia de políticas administradas por AWS.

### 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 de documentos](#) de CloudTrail.

| Cambio                                                                                                                                                  | Descripción                                                                                                                                                                                                                                                                                           | Fecha                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">CloudTrailEventContext</a> : política nueva que utiliza el rol vinculado al servicio <code>AWSServiceRoleForCloudTrailEventContext</code> . | Se agregó una política nueva y un rol nuevo para la característica de eventos enriquecidos de CloudTrail.                                                                                                                                                                                             | 19 de mayo de 2025      |
| <a href="#">CloudTrailServiceRolePolicy</a> – actualización de una política actual                                                                      | Se actualizó la política para permitir las siguientes acciones en el almacén de datos de eventos de una organización cuando la federación está deshabilitada: <ul style="list-style-type: none"><li>• <code>glue:DeleteTable</code></li><li>• <code>lakeformation:DeregisterResource</code></li></ul> | 26 de noviembre de 2023 |

| Cambio                                                                              | Descripción                                                                                                                                                                                                                                                                                                  | Fecha              |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">AWSCloudTrail_ReadOnlyAccess</a> – actualización de una política actual | CloudTrail ha cambiado el nombre de la política <code>AWSCloudTrailReadOnlyAccess</code> por <code>AWSCloudTrail_ReadOnlyAccess</code> . 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

Audidores 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 incluidos por programa de conformidad](#) y escoja el programa de conformidad que le interese. Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puedes 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 confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. Para obtener más información sobre la responsabilidad de conformidad al usar Servicios de AWS, consulte la [Documentación de seguridad de AWS](#).

# Resiliencia en AWS CloudTrail

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. 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 crea un registro de seguimiento de varias regiones, CloudTrail crea registros de seguimiento con configuraciones idénticas en todas las Regiones de AWS habilitadas en la cuenta.

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 la 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). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) 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.

Las siguientes prácticas recomendadas sobre seguridad también tratan la seguridad de la infraestructura en CloudTrail:

- [Considere 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 [Control del acceso desde puntos de enlace de la VPC con políticas de bucket.](#)
- 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 [Grupos de recursos de AWS.](#)

## Prevención de la sustitución confusa entre servicios

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. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. 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. Utiliza `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utiliza `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 de la sustitución confusa 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, utiliza 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](#).

## Prácticas recomendadas de seguridad de AWS CloudTrail

AWS CloudTrail proporciona un número 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 constituyen 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

- [Prácticas recomendadas de seguridad de CloudTrail Detective](#)
- [Prácticas recomendadas preventivas de seguridad de CloudTrail](#)

## Prácticas recomendadas de seguridad de CloudTrail Detective

### Crear un registro de seguimiento de

Para mantener un registro continuo de los eventos de la cuenta de AWS, debe crear un registro de seguimiento. Aunque CloudTrail proporciona 90 días de información del historial de eventos para los eventos de administración en la consola de CloudTrail sin crear un registro de seguimiento, 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 administrar los datos de CloudTrail con mayor facilidad, considere la posibilidad de crear un registro de traza para los eventos de administración de todas las Regiones de AWS y, a continuación, crear trazas adicionales para tipos de eventos específicos de los recursos, como, por ejemplo, la actividad de los buckets de Amazon S3 o las funciones de AWS Lambda.

Estas son algunas de las acciones que puede realizar:

- [Crear una traza para su cuenta de AWS.](#)
- [Crear una traza para una organización.](#)

### Crear un registro de seguimiento de varias regiones

Para obtener un registro completo de los eventos relacionados con una identidad de IAM o un servicio de su cuenta de AWS, cree un registro de seguimiento de varias regiones. Los registros de seguimiento de varias regiones registran los eventos en todas las Regiones de AWS que están [habilitadas](#) en su Cuenta de AWS. Al registrar los eventos en todas las Regiones de AWS habilitadas, se asegura de captar la actividad en todas las regiones habilitadas de su Cuenta de AWS. Esto incluye el registro de los [eventos de servicios globales](#), que se registran en una Región de AWS específica de dicho servicio. Todos los registros de seguimiento que se crearon mediante la consola de CloudTrail son registros de seguimiento de varias regiones.

Estas son algunas de las acciones que puede realizar:

- [Crear una traza para su cuenta de AWS.](#)
- [Convertir un registro de seguimiento de una sola región existente](#) en un registro de seguimiento de varias regiones.



- Implemente controles de supervisión continuos para ayudar a garantizar que todos los registros de seguimiento que se han creado registran los eventos de todas las Regiones de AWS mediante la regla [multi-region-cloud-trail-enabled](#) de AWS Config.

## Habilitar la integridad del archivo de registro de CloudTrail

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 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. La validación de la integridad de los archivos de registros de CloudTrail utiliza 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 modificar, eliminar o falsificar los archivos de registro de CloudTrail por medios informáticos sin que se sepa. Para obtener más información, consulte [Activación de la validación y los archivos de validación](#).

## Integración con Registros de Amazon CloudWatch

CloudWatch Logs le permite monitorear y recibir alertas para los eventos específicos capturados por CloudTrail. Los eventos que se envían a los Registros de CloudWatch son los que se configuraron para registrarlos con el registro de seguimiento, por lo que tiene que asegurarse de que ha configurado los registros de seguimiento para registrar los tipos de eventos (eventos de administración, de datos o de actividad de datos) que le interese monitorear.

Por ejemplo, puede monitorear los eventos de administración claves relacionados con la seguridad y la red, como [Eventos de error de inicio de sesión en la Consola de administración de AWS](#).

Estas son algunas de las acciones que puede realizar:

- Revisar el ejemplo [Integraciones de CloudWatch Logs con CloudTrail](#).
- Configurar el registro de seguimiento para [enviar eventos a CloudWatch Logs](#).
- Implemente controles de supervisión continuos para ayudar a garantizar que todos los registros de seguimiento estén enviando eventos a CloudWatch Logs para su monitoreo mediante la regla [cloud-trail-cloud-watch-logs-enabled](#) de AWS Config.

## Uso de Amazon GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas que lo ayuda a proteger las cuentas, los contenedores, las cargas de trabajo y los datos de su entorno de AWS. Mediante modelos de machine learning (ML) y capacidades de detección de anomalías y amenazas, GuardDuty supervisa continuamente los diferentes orígenes de registros para identificar y priorizar los posibles riesgos de seguridad y las actividades maliciosas en el entorno.

Por ejemplo, GuardDuty detectará posibles exfiltraciones de credenciales en caso de que detecte credenciales que se crearon exclusivamente para una instancia de Amazon EC2 a través de un rol de lanzamiento de instancias, pero que se utilizan desde otra cuenta dentro de AWS. Para obtener más información, consulte la [Guía del usuario de Amazon GuardDuty](#).

## Uso de AWS Security Hub CSPM

Supervise el uso de CloudTrail en relación con las prácticas recomendadas de seguridad con [AWS Security Hub CSPM](#). 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 los recursos de CloudTrail, consulte [controles de AWS CloudTrail](#) en la Guía del usuario de AWS Security Hub CSPM.

## Prácticas recomendadas preventivas de seguridad de CloudTrail

Las siguientes prácticas recomendadas para CloudTrail pueden ser de utilidad para evitar incidentes de seguridad.

### Efectuar el registro en un bucket de Amazon S3 dedicado y centralizado

Los archivos de registro de CloudTrail son un registro de auditoría de las acciones hechas por una identidad de IAM o un servicio de AWS. 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:

- Crear una cuenta de AWS independiente como cuenta de archivo de registros. Si utiliza AWS Organizations, inscriba esta cuenta en la organización y considere la posibilidad de [crear un registro de seguimiento de la organización](#) para registrar los datos de todas las cuentas de AWS de la organización.

- Si no utiliza Organizations, pero quiere registrar los datos de varias cuentas de AWS, [cree un registro de seguimiento](#) 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 un registro de seguimiento, tanto si se trata de un registro de seguimiento de la organización como si es para una única cuenta de AWS, cree un bucket de Amazon S3 dedicado para almacenar los archivos de registros de este registro de seguimiento.
- Si desea registrar la actividad de más de una cuenta de AWS, [modifique la política de bucket](#) para permitir el registro y el almacenamiento de los archivos de registro de todas las cuentas de AWS para las que desea registrar la actividad de la cuenta de AWS.
- 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.

Utilizar el cifrado del lado del servidor con claves administradas por AWS KMS

De forma predeterminada, los archivos de registro que envía CloudTrail a su bucket de S3 se cifran mediante [cifrado en el servidor con una clave de KMS \(SSE-KMS\)](#). Para utilizar SSE-KMS con CloudTrail, cree y administre una [AWS KMS key](#), también denominada clave de 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.](#)

- Considerar la posibilidad de implementar controles de supervisión continuos para ayudar a garantizar que todos los registros de seguimiento están cifrados los archivos de registro con SSE-KMS mediante la regla [cloud-trail-encryption-enabled](#) de AWS Config.

Agregar una clave de condición a la política de temas de Amazon SNS predeterminada

Cuando configura un registro de seguimiento para enviar notificaciones a Amazon SNS, CloudTrail agrega una instrucción a su política de acceso a temas de SNS que permite a CloudTrail enviar contenido a un tema de SNS. Como práctica de seguridad, recomendamos que agregue una clave de condición `aws:SourceArn` (u, opcionalmente, `aws:SourceAccount`) a la declaración de la política de temas de Amazon SNS. Esto ayuda a evitar el acceso no autorizado de la cuenta al tema de SNS. Para obtener más información, consulte [Política de temas 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 realiza un registro de seguimiento de los eventos de registro en un bucket de Amazon S3 que especifique. Estos archivos de registro contienen un registro de auditoría de las acciones hechas por las identidades de IAM y los servicios de AWS. La integridad y plenitud de estos archivos de registro son fundamentales para fines forenses y de auditoría. Con el fin de ayudar a garantizar esa integridad, debe cumplir el principio de privilegios mínimos al crear o modificar el acceso a cualquier bucket de Amazon S3 utilizado para almacenar los archivos de registros de CloudTrail.

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 de seguimiento mediante la consola de CloudTrail, pero también puede crearla y administrarla de forma manual.
- 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 bucket de Amazon S3 para almacenar los archivos de registros de varias cuentas de AWS, siga las instrucciones para [recibir los archivos de registros 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 [Creación de un registro de seguimiento para una organización con la AWS CLI](#).

- 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

De forma predeterminada, el registro de seguimiento de CloudTrail almacena los archivos de registros de forma indefinida en el bucket de Amazon S3 configurado para el registro de seguimiento. 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).

### Limitar el acceso a la política `AWSCloudTrail_FullAccess`

Los usuarios que tienen la política [AWSCloudTrail\\_FullAccess](#) tienen la capacidad de desactivar o reconfigurar las funciones de auditoría más importantes y confidenciales de sus cuentas de AWS. Esta política no se ha concebido para compartirla ni aplicarla ampliamente a las identidades de IAM de una cuenta de AWS. Limite la aplicación de esta política al menor número de personas posible, las que espera que actúen como administradores de la cuenta de AWS.

## Cifrado de archivos de registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS (SSE-KMS)

De forma predeterminada, los archivos de registro y de resumen que envía CloudTrail a su bucket se cifran mediante [cifrado en el servidor con una clave de KMS \(SSE-KMS\)](#). Si no habilita el cifrado SSE-KMS, los archivos de registro y de resumen se cifrarán mediante el [cifrado SSE-S3](#).

 Note

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 de AWS KMS `GenerateDataKey` y `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 utilizar SSE-KMS con CloudTrail, debe crear y administrar una [AWS KMS key](#). Adjunte una política a la clave que determine qué usuarios pueden utilizar la clave para cifrar y descifrar archivos de registros y de resumen de CloudTrail. El proceso de descifrado transcurre de manera fluida a través de S3. Cuando los usuarios autorizados de la clave leen archivos de registros y de resumen de CloudTrail, S3 administra el descifrado y los usuarios autorizados pueden leer los archivos ya sin cifrado.

Este enfoque tiene las siguientes ventajas:

- Puede crear y administrar la clave de KMS usted mismo.
- Puede utilizar una única clave de KMS para cifrar y descifrar los archivos de registros y de resumen de varias cuentas en todas las regiones.
- Puede controlar quién puede utilizar su clave para cifrar y descifrar archivos de registros y de resumen de CloudTrail. 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 y de resumen:
  - Un usuario debe tener permisos de lectura de S3 para el bucket que contiene los archivos de registro y de resumen.
  - También se debe aplicar a un usuario una política o un rol que la política de la clave de KMS conceda permisos de descifrado.
- Puesto que S3 descifra automáticamente los archivos de registros y de resumen de las solicitudes de los usuarios autorizados para utilizar la clave de KMS, el cifrado SSE-KMS de los archivos es compatible con versiones anteriores de las aplicaciones que leen datos de registros de CloudTrail.

 Note

La clave de KMS que elija debe crearse en la misma región de AWS que el bucket de Amazon S3 que recibe los archivos de registros y de resumen. Por ejemplo, si los archivos de registros y de registro se almacenarán en un bucket en la región Este de EE. UU. (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.

De forma predeterminada, CloudTrail cifra todos los almacenes de datos de eventos. Tiene la opción de usar su propia clave de KMS para el cifrado al crear o actualizar un almacén de datos de eventos.

## Activación del cifrado de los archivos de registro

### Note

Si crea una clave de KMS en la consola de CloudTrail, CloudTrail agrega las secciones de política de clave de KMS necesarias. Siga estos procedimientos si ha creado una clave en la consola de IAM o en la AWS CLI y necesita agregar manualmente las secciones necesarias de la política.

Para habilitar el cifrado SSE-KMS para los archivos de registros de CloudTrail, siga estos pasos de alto nivel:

#### 1. Creación de una clave de KMS.

- Para obtener información sobre cómo crear una clave de KMS con la Consola de administración de AWS, consulte [Creación de claves](#) en la Guía para desarrolladores AWS Key Management Service.
- Para obtener información sobre cómo crear una clave de KMS con la 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 y de resumen. Para verificar la región a la que pertenece un bucket de S3, inspeccione las propiedades del bucket en la consola de S3.

#### 2. Agregue secciones de política a la clave para que CloudTrail pueda cifrar los archivos de registros y de resumen y los usuarios puedan descifrarlos.

- 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 y de resumen. 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 asociar una política a una clave de KMS con la AWS CLI, consulte [put-key-policy](#).
3. Actualice su registro de seguimiento o almacén de datos de eventos para utilizar la clave de KMS cuya política ha modificado para CloudTrail.
- Para actualizar un registro de seguimiento o almacén de datos de eventos con la consola de CloudTrail, consulte [Actualización de un recurso para que utilice su clave de KMS con la consola](#).
  - Para actualizar un registro de seguimiento o almacén de datos de eventos con la AWS CLI, consulte [Habilitar y deshabilitar el cifrado de los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail con AWS CLI](#).

CloudTrail también admite claves de AWS KMS de varias regiones. 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 que requiere su política de clave de KMS para utilizarse con CloudTrail.

## 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 la pestaña Permisos.
4. En la lista Agregar permisos, seleccione Asociar políticas.

5. Busque `AWSKeyManagementServicePowerUser`, elija la política y después elija Asociar políticas.

El usuario ahora tiene permiso para crear una clave de KMS. Para obtener más información acerca de la creación de políticas, consulte [Creación de políticas de IAM](#) 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 Consola de administración de AWS o la AWS CLI, debe agregar las 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, de resumen y los almacenes de datos de eventos. También debe permitir que los usuarios especificados lean archivos de registro y de resumen 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, consulte [Edición de una política de claves](#) en la AWS Key Management Service Guía para desarrolladores.
- Si quiere obtener más información técnica sobre cómo CloudTrail utiliza AWS KMS, consulte [Cómo AWS CloudTrail usa AWS KMS](#).

## Temas

- [Secciones de política de clave de KMS necesarias para utilizar con CloudTrail](#)
- [Otorgar permisos de cifrado para los registros de seguimiento](#)
- [Otorgar permisos de cifrado para los almacenes de datos de eventos](#)
- [Otorgar permisos de descifrado para los registros de seguimiento](#)
- [Otorgar permisos de descifrado para los almacenes de datos de eventos](#)
- [Habilitar CloudTrail para describir las propiedades de la clave de KMS](#)
- [Política de claves de KMS predeterminada creada en la consola de CloudTrail](#)

## 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. Otorgue permisos para cifrar los archivos de registro y de resumen de CloudTrail. Para obtener más información, consulte [Otorgar permisos de cifrado para los registros de seguimiento](#).
2. Otorgue permisos para descifrar los archivos de registro y de resumen de CloudTrail. Para obtener más información, consulte [Otorgar permisos de descifrado para los registros de seguimiento](#). 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. Para obtener más información, 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. Otorgue permisos para cifrar un almacén de datos de eventos de CloudTrail Lake. Para obtener más información, consulte [Otorgar permisos de cifrado para los almacenes de datos de eventos](#).
2. Otorgue permisos para descifrar un almacén de datos de eventos de CloudTrail Lake. Para obtener más información, consulte [Otorgar permisos de descifrado para los almacenes de datos de eventos](#).

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.

3. Habilite CloudTrail para describir las propiedades de la clave de KMS. Para obtener más información, 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.

## Otorgar permisos de cifrado para los registros de seguimiento

Example Permita a CloudTrail cifrar archivos de registros y de resumen en nombre de cuentas específicas.

CloudTrail necesita permisos explícitos para utilizar la clave de KMS para cifrar archivos de registros y de resumen 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 y de resumen.

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": "AllowCloudTrailEncryptLogs",
  "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/*"
    }
  }
}

```

## Example

La siguiente instrucción de política de ejemplo ilustra cómo otra cuenta puede utilizar su clave de KMS para cifrar archivos de registros y de resumen 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 los archivos de registro y de resumen solo para las cuentas que especifique. Cuando concede permiso a la raíz de la cuenta *222222222222* para cifrar los archivos de registro y de resumen, 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": "EnableCloudTrailEncryptPermissions",
  "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.

## Otorgar permisos de cifrado para los almacenes de datos de eventos

La política de una clave de KMS utilizada para cifrar el almacén de datos de un evento 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": "AllowCloudTrailEncryptEds",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*"
}

```

## Otorgar permisos de descifrado para los registros de seguimiento

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": "EnableCloudTrailLogDecryptPermissions",
  "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": "AllowCloudTrailDecryptTrail",
  "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": "EnableCloudTrailLogDecryptPermissions",
  "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 del registro de seguimiento. 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": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:111111111111:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Instrucción de política de la usuaria de IAM Alice:

JSON

```
{
  "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": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111111111111: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:

## JSON

```
{
  "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.

## Otorgar permisos de descifrado para los almacenes de datos de eventos

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": "EnableUserKeyPermissionsEds"
  "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 el almacén de datos de eventos.

```
{
  "Sid": "AllowCloudTrailDecryptEds",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

## 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": "AllowCloudTrailAccess",
  "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 y de resumen con la clave de KMS y describir la clave de KMS.
- Permite que todos los usuarios de las cuentas especificadas descifren archivos de registro y de resumen.
- 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 registros de seguimiento](#)
- [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

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 y de resumen entre cuentas con la clave de KMS.

### JSON

```
{
  "Version": "2012-10-17",
  "Id": "Key policy created by CloudTrail",
  "Statement": [
    {
```

```

        "Sid": "Enable IAM user permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": [
                "arn:aws:iam::111111111111:root",
                "arn:aws:iam::111111111111: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:us-east-1:111111111111:trail/trail-name"
            },
            "StringLike": {
                "kms:EncryptionContext:aws:cloudtrail:arn":
                    "arn:aws:cloudtrail:*:111111111111: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": "111111111111"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:111111111111:trail/*"
        }
    }
},
{
    "Sid": "Enable cross account log decryption",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptFrom"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "111111111111"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:111111111111:trail/*"
        }
    }
}
]
}

```



## 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.

JSON

```
{
  "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::111111111111:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Enable user to have permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:sts::111111111111:assumed-role/example-role-name"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
    }
  ]
}
```

```
    "Resource": "*"
  }
]
}
```

## Actualización de un recurso para que utilice su clave de KMS con la consola

En la consola de CloudTrail, actualice un registro de seguimiento o un almacén de datos de eventos para que utilicen una clave de KMS. Tenga en cuenta que el uso de su propia clave de KMS implica costos de cifrado y descifrado de AWS KMS. Para 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

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 los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail con AWS CLI](#).

Para actualizar un registro de seguimiento a fin de utilizar su clave de KMS

1. Inicie sesión en la Consola de administración de AWS 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), elija Edit (Editar).
4. En Cifrado SSE-KMS de archivos de registro, elija Habilitado si desea cifrar sus archivos de registro y de resumen con cifrado SSE-KMS en vez de SSE-S3. El valor predeterminado es Enabled (Habilitado). Si no habilita el cifrado SSE-KMS, los archivos de registro y de resumen 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 con la consola](#). La política de claves debe permitir que CloudTrail utilice la clave para cifrar los archivos de registro y de resumen, y que los usuarios especificados lean archivos de registro y de resumen 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 con la consola](#).

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 de alias: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- ARN de 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 Consola de administración de AWS 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), elija Edit (Editar).
4. Si la opción Cifrado aún no está habilitada, seleccione Utilizar mi propia AWS KMS key para cifrar el almacén de datos de eventos 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/MyAlias`. Para obtener más información, consulte [Actualización de un recurso para que utilice su clave de KMS con la consola](#).

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 de alias: `arn:aws:kms:region:123456789012:alias/MyAliasName`
  - ARN de clave:  
`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
  - ID de la clave único global: `12345678-1234-1234-1234-123456789012`
5. Seleccione 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 desarrolladores AWS Key Management Service.

# Habilitar y deshabilitar el cifrado de los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail con AWS CLI

En este tema, se describe cómo habilitar y deshabilitar el cifrado SSE-KMS de archivos de registro, de resumen y los almacenes de datos de eventos para CloudTrail mediante la AWS CLI. Para obtener información general, consulte [Cifrado de archivos de registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS \(SSE-KMS\)](#).

## Temas

- [Habilitar el cifrado de los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail mediante AWS CLI](#)
- [Deshabilitar el cifrado de los archivos de registro y de resumen mediante el AWS CLI](#)

## Habilitar el cifrado de los archivos de registro, los archivos de resumen y los almacenes de datos de eventos de CloudTrail mediante AWS CLI

- [Habilite el cifrado de archivos de registro y de resumen para un registro de seguimiento](#)
- [Habilite el cifrado para un almacén de datos de eventos](#)

### Habilite el cifrado de archivos de registro y de resumen 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 de resumen 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 permite el cifrado de los archivos de registro y de resumen.

```
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 de 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": "amzn-s3-demo-bucket"
}
```

La presencia del elemento `KmsKeyId` indica que se habilitó el cifrado de los archivos de registro. Si se habilitó la validación de los archivos de registro (lo que se indica con el valor verdadero del elemento `LogFileValidationEnabled`), esto también indica que se habilitó el cifrado de los archivos de resumen. Los archivos de registros y de resumen cifrados deberían aparecer en el bucket de S3 configurado para el registro de seguimiento en un plazo de aproximadamente 5 minutos.

## Habilite el cifrado 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 el almacén de datos de eventos y los usuarios puedan descifrarlo. Asegúrese de que todos los usuarios que van a leer el almacén de datos de eventos 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 del almacén de datos de eventos.

```
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 de 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 habilitó el cifrado del almacén de datos de eventos.

## Deshabilitar el cifrado de los archivos de registro y de resumen mediante el AWS CLI

Para detener el cifrado de los archivos de registro y de resumen en un registro de seguimiento, ejecute `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": "amzn-s3-demo-bucket"
}

```

La ausencia del valor `KmsKeyId` indica que el cifrado de los archivos de registro y de resumen ya no está habilitado.

 Important

No se puede detener el cifrado de un almacén de datos de eventos.

## Cómo AWS CloudTrail usa AWS KMS

En esta sección se describe cómo AWS KMS se usa un registro de seguimiento de CloudTrail cifrado con una clave de SSE-KMS.

 Important

AWS CloudTrail y Amazon S3 solo admite CMK [AWS KMS keys simétricas](#). No puede usar una [clave KMS asimétrica](#) para cifrar sus registros de CloudTrail. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte [Identificación de distintos tipos de claves](#) en la Guía para desarrolladores de AWS Key Management Service.

No se paga un cargo por uso de claves cuando CloudTrail lee o escribe archivos de registro cifrados con una clave SSE-KMS. Sin embargo, se paga un cargo por uso de claves cuando se accede a los archivos de registro de CloudTrail cifrados con una clave SSE-KMS. Para obtener más información acerca de los precios de AWS KMS, consulte [Precios de AWS Key Management Service](#). Para obtener más información sobre los precios de CloudTrail, consulte [Precios de AWS CloudTrail](#).

### Conocer cuándo se usa su clave KMS en el registro de seguimiento

El cifrado de los archivos de registro de CloudTrail con AWS KMS se basa en la característica de Amazon S3 denominada cifrado del lado del servidor con AWS KMS key (SSE-KMS). Para obtener más información sobre SSE-KMS, consulte [Uso del cifrado del lado del servidor con claves AWS KMS \(SSE-KMS\)](#) en la Guía del usuario de Amazon Simple Storage Service.

Al configurar AWS CloudTrail para utilizar SSE-KMS para cifrar los archivos de registro, CloudTrail y Amazon S3 usan la AWS KMS keys al realizar determinadas acciones con esos servicios. En las secciones siguientes se explica cuándo y cómo dichos servicios pueden utilizar su clave KMS y se proporciona información adicional que puede utilizar para validar esta explicación.

Acciones que hacen que CloudTrail y Amazon S3 utilicen su clave KMS

- [Configure CloudTrail para cifrar los archivos de registro con AWS KMS key](#)
- [CloudTrail guarda un archivo de registro en su bucket de S3](#)

- [Obtenga un archivo de registro cifrado del bucket de S3](#)

Configure CloudTrail para cifrar los archivos de registro con AWS KMS key

Cuando [actualice su configuración de CloudTrail para utilizar su clave KMS](#), CloudTrail envía una solicitud [GenerateDataKey](#) a AWS KMS para comprobar que la clave KMS existe y que CloudTrail tiene permiso para utilizarla para el cifrado. CloudTrail no utiliza la clave de datos resultante.

La solicitud GenerateDataKey incluye la siguiente información para el [contexto de cifrado](#):

- El [nombre de recurso de Amazon \(ARN\)](#) del seguimiento de CloudTrail
- El ARN del bucket de S3 y la ruta donde se entregan los archivos de registro de CloudTrail

La solicitud GenerateDataKey genera una entrada en los registros de CloudTrail similar al ejemplo siguiente. Cuando aparece una entrada de registro como esta, se puede determinar que CloudTrail ha llamado a la operación de AWS KMS GenerateDataKey para un registro de seguimiento específico. AWS KMS creó la clave de datos con una clave KMS específica.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "cloudtrail.amazonaws.com"
  },
  "eventTime": "2024-12-06T20:14:46Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "cloudtrail.amazonaws.com",
  "userAgent": "cloudtrail.amazonaws.com",
  "requestParameters": {
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-exampleeeb770",
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/management-events",
      "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-bucket-123456789012-9af1fb49/AWSLogs/123456789012/CloudTrail/us-east-1/2024/12/06/123456789012_CloudTrail_us-east-1_20241206T2010Z_T0500LMG1hIQ1png.json.gz"
    }
  }
}
```

```

    }
  },
  "responseElements": null,
  "requestID": "a0555e85-7e8a-4765-bd8f-2222295558e1",
  "eventID": "e4f3557e-7dbd-4e37-a00a-d86c137d1111",
  "readOnly": true,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-exampleeeb770"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "sharedEventID": "ce71d6be-0846-498e-851f-111a1af9078f",
  "eventCategory": "Management"
}

```

CloudTrail guarda un archivo de registro en su bucket de S3

Cada vez que CloudTrail guarda un archivo de registro en un bucket de S3, Amazon S3 envía una solicitud [GenerateDataKey](#) a AWS KMS en nombre de CloudTrail. En respuesta a esta solicitud, AWS KMS genera una clave de datos única y, a continuación, envía a Amazon S3 dos copias de la clave de datos, una en texto no cifrado y otra cifrada con la clave KMS especificada. Amazon S3 utiliza la clave de datos de texto no cifrado para cifrar el archivo de registro de CloudTrail y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla. Amazon S3 almacena la clave de datos cifrada como metadatos cifrados con el archivo de registro de CloudTrail cifrado.

La solicitud GenerateDataKey incluye la siguiente información para el [contexto de cifrado](#):

- El [nombre de recurso de Amazon \(ARN\)](#) del seguimiento de CloudTrail
- El ARN del objeto de S3 (el archivo de registro de CloudTrail)

Cada solicitud GenerateDataKey genera una entrada en los registros de CloudTrail similar al ejemplo siguiente. Cuando aparece una entrada de registro como esta, se puede determinar que CloudTrail ha llamado a la operación de AWS KMS GenerateDataKey para un registro de

seguimiento específico para proteger un archivo de registro específico. AWS KMS creó la clave de datos con la clave KMS específica, que se muestra dos veces en la misma entrada de registro.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "cloudtrail.amazonaws.com"
  },
  "eventTime": "2024-12-06T21:49:28Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "cloudtrail.amazonaws.com",
  "userAgent": "cloudtrail.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1::trail/insights-trail",
      "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2150Z_hVXmrJzjZk2wAM2V.json.gz"
    },
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
  },
  "responseElements": null,
  "requestID": "11117d14-9232-414a-b3d1-01bab4dc9f99",
  "eventID": "999e9a50-512c-4e2a-84a3-111a5f511111",
  "readOnly": true,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "sharedEventID": "5e663acc-b7fd-4cdd-8328-0eff862952fa",
}
```

```
"eventCategory": "Management"
}
```

Obtenga un archivo de registro cifrado del bucket de S3

Cada vez que usted obtiene un archivo de registro de CloudTrail cifrado del bucket de S3, Amazon S3 envía una solicitud [Decrypt](#) a AWS KMS en su nombre para descifrar la clave de datos cifrada del archivo de registro. Como respuesta a esta solicitud, AWS KMS utiliza su clave KMS para descifrar la clave de datos y, a continuación, envía la clave de datos en texto no cifrado a Amazon S3. Amazon S3 utiliza la clave de datos de texto no cifrado para descifrar el archivo de registro de CloudTrail y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla.

La solicitud Decrypt incluye la siguiente información para el [contexto de cifrado](#):

- El [nombre de recurso de Amazon \(ARN\)](#) del seguimiento de CloudTrail
- El ARN del objeto de S3 (el archivo de registro de CloudTrail)

Cada solicitud Decrypt genera una entrada en los registros de CloudTrail similar al ejemplo siguiente. Cuando aparece una entrada de registro como esta, se puede determinar que un rol que se asumió ha llamado a la operación de AWS KMS Decrypt para un registro de seguimiento específico y un archivo de registro específico. AWS KMS descifró la clave de datos con una clave KMS específica.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      }
    }
  },
```

```

        "attributes": {
            "creationDate": "2024-12-06T22:04:04Z",
            "mfaAuthenticated": "false"
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-12-06T22:26:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T0000Z_aAAsHbGBdye3jp2R.json.gz"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "1ab2d2d2-111a-2222-a59b-11a2b3832b53",
    "eventID": "af4d4074-2849-4b3d-1a11-a1aaa111a111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}

```

# Historial de documentos

En la siguiente tabla se describen los cambios importantes que se han hecho en la documentación para AWS CloudTrail. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

- Versión de la API: 2013-11-01
- 

| Cambio                                 | Descripción                                                                                                                                                                                                            | Fecha                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de actividad de la red de CloudTrail adicionales. Para obtener más información, consulte <a href="#">Eventos de actividad de la red</a> .                                                | 15 de octubre de 2025    |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail adicionales para Amazon Bedrock, Amazon Elastic Container Service y Amazon Quick Suite. Para obtener más información, consulte <a href="#">Eventos de datos</a> . | 15 de octubre de 2025    |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de actividad de la red de CloudTrail adicionales. Para obtener más información, consulte <a href="#">Eventos de actividad de la red</a> .                                                | 15 de septiembre de 2025 |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail                                                                                                                                                                   | 12 de septiembre de 2025 |



adicionales para Amazon Q Business, Amazon Quick Suite, Amazon SageMaker AI, Amazon Bedrock, Amazon Elastic Compute Cloud y Amazon Kinesis Video Streams. Para obtener más información, consulte [Eventos de datos](#).

#### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail adicionales para Amazon Aurora DSQL, Amazon Bedrock, Amazon Elastic Kubernetes Service, Amazon S3 y Amazon Keyspaces (para Apache Cassandra). Para obtener más información, consulte [Eventos de datos](#).

1 de julio de 2025

#### Se agregó compatibilidad para los servicios

Esta versión admite el registro de llamadas a la API de aprobación de varias partes. Para obtener más información, consulte [Servicios e integraciones admitidos de CloudTrail](#).

17 de junio de 2025

|                                        |                                                                                                                                                                                                                                                                                                                                                                     |                    |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Funcionalidad agregada</a> | <p>El registro de las operaciones DeleteObject de eventos de datos de Amazon S3 ahora incluye información sobre todos los objetos individuales eliminados por la llamada. Puede elegir filtrar esta información adicional. Para obtener más información, consulte <a href="#">Ejemplos de la AWS CLI para filtrar eventos de datos</a>.</p>                         | 9 de junio de 2025 |
| <a href="#">Funcionalidad agregada</a> | <p>Ahora puede registrar eventos de actividad de la red de CloudTrail adicionales. Para obtener más información, consulte <a href="#">Eventos de actividad de la red</a>.</p>                                                                                                                                                                                       | 30 de mayo de 2025 |
| <a href="#">Nueva funcionalidad</a>    | <p>Ahora puede enriquecer los eventos de administración y de datos de CloudTrail para mejorar los resultados al categorizar, buscar y analizar los eventos de CloudTrail. Para obtener más información, consulte <a href="#">Enriquecer los eventos de CloudTrail mediante la adición de claves de etiqueta de recurso y claves de condición global de IAM</a>.</p> | 29 de mayo de 2025 |

|                                        |                                                                                                                                                                                                                                                                                                            |                     |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Nueva funcionalidad</a>    | Se agregó documentación e información sobre las políticas para el rol vinculado al servicio <code>AWSServiceRoleForCloudTrailEventContext</code> . Para obtener más información, consulte <a href="#">Utilizar los roles para crear y administrar el contexto de eventos de CloudTrail en CloudTrail</a> . | 29 de mayo de 2025  |
| <a href="#">Funcionalidad agregada</a> | Ahora puede cifrar tanto los archivos de registro como los archivos de resumen con AWS KMS keys (SSE-KMS) . Para obtener más información, consulte <a href="#">Cifrar los archivos de registros de CloudTrail con AWS KMS keys (SSE-KMS)</a> .                                                             | 22 de mayo de 2025  |
| <a href="#">Funcionalidad agregada</a> | Ahora puede utilizar selectores de eventos avanzados adicionales y plantillas predefinidas para registrar los eventos de datos en el registro de seguimiento. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                    | 10 de abril de 2025 |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar los eventos de actividad de la red para AWS Lambda y Amazon Comprehend. Para obtener más información, consulte <a href="#">Eventos de actividad de la red</a> .                                                                                                                      | 10 de abril de 2025 |

|                                        |                                                                                                                                                                                                                                                          |                     |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en los conjuntos de configuración, las identidades de correo electrónico y las plantillas de Amazon Simple Email Service. Para obtener más información, consulte <a href="#">Eventos de datos</a> . | 10 de abril de 2025 |
| <a href="#">Funcionalidad agregada</a> | AWS CloudTrail ahora admite políticas de punto de conexión de VPC. Para obtener más información, consulte <a href="#">Uso de AWS CloudTrail con puntos de conexión de VPC de Amazon</a> .                                                                | 9 de abril de 2025  |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de actividad de la red de CloudTrail para AWS IoT FleetWise.                                                                                                                                                               | 8 de abril de 2025  |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en las sesiones de Amazon Bedrock mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                               | 19 de marzo de 2025 |

### Documentación actualizada

Se actualizó el esquema de SQL para los eventos de CloudTrail Lake Insights. Se agregaron nuevos temas para describir los campos de registro de eventos de Insights para los [registros de seguimiento](#) y los [almacenes de datos de eventos](#). Para obtener más información sobre el esquema de SQL compatible para los eventos de CloudTrail Lake Insights, consulte [Esquema compatible para los campos de registro de eventos de CloudTrail Insights](#).

13 de marzo de 2025

### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail en las aplicaciones y grupos de transmisión de Amazon GameLift Streams mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

7 de marzo de 2025

### Se agregó compatibilidad para los servicios

Esta versión es compatible con las integraciones administradas para AWS IoT Device Management. Para obtener más información, consulte [Servicio de AWS topics for CloudTrail](#).

3 de marzo de 2025

|                                                                              |                                                                                                                                                                                                                                      |                       |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Funcionalidad agregada</a>                                       | Ahora puede registrar eventos de datos de CloudTrail en las aplicaciones de seguimiento móvil de Amazon Pinpoint mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> . | 24 de febrero de 2025 |
| <a href="#">Disponibilidad general de los eventos de actividad de la red</a> | Los eventos de actividad de la red ya están disponibles de manera general. Para obtener más información, consulte <a href="#">Logging network activity events</a> .                                                                  | 13 de febrero de 2025 |
| <a href="#">Documentación actualizada</a>                                    | Se agregó el tema <a href="#">Cómo entender los registros de seguimiento de varias regiones y las regiones optativas</a> para describir los registros de seguimiento de varias regiones y las regiones optativas.                    | 10 de febrero de 2025 |
| <a href="#">Funcionalidad agregada</a>                                       | Ahora puede registrar eventos de datos de CloudTrail en los puntos de conexión regionales de Amazon Timestream mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .   | 31 de enero de 2025   |

|                                                    |                                                                                                                                                                                                                                                                                                                                                |                     |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Funcionalidad agregada</a>             | Ahora puede registrar eventos de datos de CloudTrail en peticiones de Amazon Bedrock y actividades de AWS Step Functions mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                                   | 24 de enero de 2025 |
| <a href="#">Documentación actualizada</a>          | Se agregó el tema <a href="#">Optimizar las consultas de CloudTrail Lake</a> para ofrecer orientación sobre cómo optimizar las consultas de CloudTrail Lake para mejorar el rendimiento y la fiabilidad. Este tema abarca las técnicas de optimización específicas, así como soluciones alternativas para los errores de consulta más comunes. | 22 de enero de 2025 |
| <a href="#">Compatibilidad con nuevas regiones</a> | CloudTrail amplió la compatibilidad con una nueva región: la región México (centro). Para más información, consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                                      | 13 de enero de 2025 |
| <a href="#">Compatibilidad con nuevas regiones</a> | CloudTrail amplió la compatibilidad con una nueva región: la región Asia-Pacífico (Tailandia). Para más información, consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                            | 7 de enero de 2025  |

|                                           |                                                                                                                                                                                                                                                                                                                                                  |                         |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en trabajos de búsqueda de AWS Backup mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                                                                   | 30 de diciembre de 2024 |
| <a href="#">Documentación actualizada</a> | Convirtió el tema de Eventos de registro de Insights en un capítulo denominado <a href="#">Trabajar con CloudTrail Insights</a> . En el capítulo se incluyen nuevas secciones sobre los <a href="#">costos de los eventos de Insights</a> y la <a href="#">visualización de los eventos de Insights para los almacenes de datos de eventos</a> . | 23 de diciembre de 2024 |
| <a href="#">Compatibilidad con IPv6</a>   | CloudTrail agrega compatibilidad con IPv6.                                                                                                                                                                                                                                                                                                       | 20 de diciembre de 2024 |
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en trabajos de firma y perfiles de AWS Signer mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                                                           | 20 de diciembre de 2024 |



Documentación actualizada

Se actualizó la sección de [Servicios e integraciones compatibles con CloudTrail](#) para incluir descripciones de las integraciones de AWS Config, AWS Audit Manager y Amazon Athena con CloudTrail Lake.

18 de diciembre de 2024

Se agregó compatibilidad para los servicios

Esta versión es compatible con AWS Migration Hub Journeys. Para obtener más información, consulte [Temas de Servicio de AWS para CloudTrail](#) y [Registro de llamadas a la API de AWS Migration Hub Journeys con AWS CloudTrail](#).

3 de diciembre de 2024

Se agregó compatibilidad para los servicios

Esta versión es compatible con Oracle Database@AWS. Para obtener más información, consulte [Temas de Servicio de AWS para CloudTrail](#) y [Registro de llamadas a la API de Oracle Database@AWS con AWS CloudTrail](#).

1 de diciembre de 2024

### Se agregó compatibilidad para los servicios

Esta versión admite la respuesta a incidentes de seguridad de AWS. Para obtener más información, consulte [Temas de Servicio de AWS para CloudTrail](#) y [Registro de llamadas a la API de respuesta a incidentes de seguridad de AWS con AWS CloudTrail](#).

1 de diciembre de 2024

### Funcionalidad agregada

CloudTrail Lake agrega compatibilidad con paneles personalizados, el panel de aspectos destacados y paneles administrados nuevos. Puede crear paneles personalizados y agregar hasta 10 widgets a cada uno. Puede habilitar el panel de aspectos destacados para ver un resumen rápido de la actividad de AWS recopilada por los almacenes de datos de eventos de la cuenta. Para obtener más información, consulte los [Paneles de CloudTrail Lake](#).

21 de noviembre de 2024

### Funcionalidad agregada

CloudTrail Lake agrega compatibilidad para las políticas basadas en recursos en los almacenes de datos de eventos. Puede utilizar políticas basadas en recursos para ofrecer acceso entre cuentas y permitir que las entidades principales seleccionadas consulten al almacén de datos de eventos, enumeren y cancelen consultas y vean los resultados de las consultas. Para obtener más información, consulte [Ejemplos de políticas basadas en recursos para almacenes de datos de eventos](#).

21 de noviembre de 2024

### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail para las API de GraphQL AWS AppSync mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

19 de noviembre de 2024

### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail en las conversaciones con asistentes de AWS IoT SiteWise mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

18 de noviembre de 2024

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                    |                         |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>                                               | Ahora puede registrar eventos de datos de CloudTrail en los mensajes SMS para usuarios finales de AWS mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                                                                          | 15 de noviembre de 2024 |
| <a href="#">Funcionalidad agregada</a>                                               | Se agregó compatibilidad para el campo <code>assumedRole</code> para el <code>sessionContext</code> del elemento <code>userIdentity</code> . Para obtener más información, consulte <a href="#">Elemento de identidad de usuario de CloudTrail</a> en esta guía y <a href="#">Seguimiento de tareas privilegiadas en CloudTrail</a> en la Guía del usuario de IAM. | 14 de noviembre de 2024 |
| <a href="#">Disponibilidad general del asistente de consultas de CloudTrail Lake</a> | El asistente de consultas de CloudTrail Lake ya está disponible de manera general. El asistente de consultas le permite crear consultas SQL a partir de solicitudes en lenguaje natural en inglés. Para obtener más información, consulte <a href="#">Creación de consultas de CloudTrail Lake a partir de peticiones de lenguaje natural</a> .                    | 12 de noviembre de 2024 |

## Funcionalidad agregada

Presentamos una característica en versión preliminar para consultas de CloudTrail Lake que utiliza las capacidades de la inteligencia artificial generativa (IA generativa) para resumir los resultados. Para obtener más información, consulte [Resumir los resultados de las consultas en lenguaje natural](#).

12 de noviembre de 2024

## Funcionalidad agregada

11 de noviembre de 2024

Ahora puede configurar campos selectores de eventos avanzados adicionales para los almacenes de datos de eventos de CloudTrail Lake, lo que le ofrece un mayor control sobre qué eventos de CloudTrail se incorporan a los almacenes de datos de eventos. Puede filtrar los eventos administrados en los siguientes campos del selector de eventos avanzados: `eventName` (nuevo), `eventSource`, `eventType`, `readOnly`, `sessionCredentialFromConsole` (nuevo) y `userIdentity.arn` (nuevo). Puede filtrar los eventos de datos en los siguientes campos del selector de eventos avanzados: `eventName`, `eventSource` (nuevo), `eventType` (nuevo), `resources.type`, `resources.ARN`, `readOnly`, `sessionCredentialFromConsole` (nuevo) y `userIdentity.arn` (nuevo). Para obtener más información, consulte [Creación de un almacén de datos de eventos para eventos de CloudTrail](#)

[I con la consola](#) (pasos 16 y 17).

#### Versión del evento actualizada

Se actualizó eventVersion a 1.11 y se agregó un campo inScopeOf para el elemento userIdentity . Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).

29 de octubre de 2024

#### Se agregó compatibilidad para los servicios

Esta versión es compatible con los mensajes SMS para usuarios finales de AWS. Para obtener más información, consulte [Servicio de AWS topics for CloudTrail](#) y [Logging AWS End User Messaging SMS API calls using AWS CloudTrail](#).

22 de octubre de 2024

#### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail en las identidades de origen de mensajes SMS para usuarios finales de AWS mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

22 de octubre de 2024

### Se agregó compatibilidad para los servicios

Esta versión es compatible con los mensajes de redes sociales para usuarios finales de AWS. Para obtener más información, consulte [Servicio de AWS topics for CloudTrail](#) y [Logging AWS End User Messaging Social API calls using AWS CloudTrail](#).

10 de octubre de 2024

### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail en los ID de números de teléfono de mensajes de redes sociales para usuarios finales de AWS mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

10 de octubre de 2024

### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail en modelos de Amazon Bedrock y activos de AWS Data Exchange mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

27 de septiembre de 2024



## Funcionalidad agregada

Ahora puede configurar registros de seguimiento y almacenes de datos de eventos para registrar eventos de actividad de la red de CloudTrail (en versión preliminar). Los eventos de actividad de la red permiten a los propietarios de los puntos de conexión de VPC grabar las llamadas a la API de AWS realizadas con sus puntos de conexión de VPC desde una VPC privada al Servicio de AWS. Esta versión es compatible con el registro de eventos de actividad de la red para los siguientes orígenes de eventos: `cloudtrail.amazonaws.com`, `ec2.amazonaws.com`, `kms.amazonaws.com` y `secretsmanager.amazonaws.com`. Para obtener más información, consulte [Logging network activity events](#).

24 de septiembre de 2024

## Se agregó compatibilidad para los servicios

Esta versión es compatible con los datos de Directory Service. Para obtener más información, consulte [Servicio de AWS topics for CloudTrail](#) y [Logging Directory Service Data API calls using AWS CloudTrail](#).

18 de septiembre de 2024

### [Compatibilidad con nuevas regiones](#)

CloudTrail amplió la compatibilidad con una nueva región: la región Asia-Pacífico (Malasia). Para más información, consulte [Regiones compatibles con CloudTrail](#).

22 de agosto de 2024

### [Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en los monitores de aplicaciones de Amazon CloudWatch RUM mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

25 de julio de 2024

### [Funcionalidad agregada](#)

Ahora puede controlar el acceso a los registros de seguimiento mediante las etiquetas. Para obtener más información, consulte [ABAC with CloudTrail](#).

23 de julio de 2024

### [Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en usuarios y claves de usuarios de Amazon One Enterprise mediante selectores de eventos avanzados. Para obtener más información, consulte [Eventos de datos](#).

23 de julio de 2024

|                                        |                                                                                                                                                                                                                                                                                                                                                                               |                     |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en las barreras de protección y los alias de flujo de Amazon Bedrock, y la actividad de la API de Amazon S3 en el nivel de objeto en los buckets de directorio mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                       | 9 de julio de 2024  |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en las claves y alias de AWS Payment Cryptography mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                                                                                    | 5 de julio de 2024  |
| <a href="#">Funcionalidad agregada</a> | Presentamos una característica en versión preliminar para consultas de CloudTrail Lake que utiliza las capacidades de la inteligencia artificial generativa (IA generativa) para generar una consulta SQL a partir de una petición redactada en inglés. Para obtener más información, consulte <a href="#">Create CloudTrail Lake queries from English language prompts</a> . | 11 de junio de 2024 |

|                                           |                                                                                                                                                                                                                                                                              |                    |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en las métricas de Amazon CloudWatch, los modelos de ML de Amazon Machine Learning y AWS Private CA mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> . | 5 de junio de 2024 |
| <a href="#">Documentación actualizada</a> | Se agregó una sección para describir cómo filtrar los eventos de datos mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Filtering data events by using advanced event selectors</a> .                                            | 29 de mayo de 2024 |
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en los flujos y consumidores de flujos de Amazon Kinesis Data Streams mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                               | 21 de mayo de 2024 |
| <a href="#">Documentación actualizada</a> | Se actualizó la página <a href="#">Regiones en las que se admite CloudTrail Lake</a> para agregar la región de Asia Pacífico (Hyderabad) (ap-south-2), la región de Europa (Zúrich) (eu-central-2) y la región de Israel (Tel Aviv) (il-central-1).                          | 16 de mayo de 2024 |

|                                           |                                                                                                                                                                                                                          |                    |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en las máquinas de estado de AWS Step Functions mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> . | 16 de mayo de 2024 |
| <a href="#">Documentación actualizada</a> | Se agregó una sección sobre cómo ver el uso y el costo de CloudTrail mediante AWS Cost Explorer. Para obtener más información, consulte <a href="#">Viewing your CloudTrail cost and usage with AWS Cost Explorer</a> .  | 14 de mayo de 2024 |
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en Amazon Q Apps mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                | 1 de mayo de 2024  |

## Documentación actualizada

10 de abril de 2024

Mejoras generales en la organización de los títulos de las páginas y secciones de la guía del usuario, que incluyen lo siguiente: cambio del título de la página de referencia sobre eventos de registro de CloudTrail por [Descripción de los eventos de CloudTrail](#) y adición de descripciones de los eventos de administración, eventos de datos y eventos de Insights. Se cambió el título de la página de configuración a [Configuración de los ajustes de CloudTrail](#). Se movieron las páginas [Registro de eventos de datos](#), [Registro de eventos de administración](#) y [Registro de eventos de Insights](#) a la sección Descripción de los eventos de CloudTrail. Se movió la página [Ejemplos de archivos de registros de CloudTrail](#) a la sección [Archivos de registros de CloudTrail](#). Se agregaron páginas independientes para enumerar los comandos de la AWS CLI para los almacenes de datos de eventos, consultas e integraciones de CloudTrail Lake.

|                                                             |                                                                                                                                                                                                                                                 |                     |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Documentación actualizada</a>                   | Se actualizó la página de <a href="#">Regiones en las que se admite CloudTrail Lake</a> para agregar la región Europa (España) (eu-south-2).                                                                                                    | 10 de abril de 2024 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Control Catalog. Para obtener más información, consulte <a href="#">Temas de Servicio de AWS para CloudTrail</a> y <a href="#">Registro de llamadas a la API de AWS Control Catalog con AWS CloudTrail</a> . | 8 de abril de 2024  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Deadline Cloud. Para obtener más información, consulte <a href="#">Servicio de AWS topics for CloudTrail</a> .                                                                                               | 2 de abril de 2024  |
| <a href="#">Versión del evento actualizada</a>              | La versión del evento AWS CloudTrail ahora es 1.10. Para obtener más información, consulte <a href="#">Contenido de registros de CloudTrail</a> .                                                                                               | 26 de marzo de 2024 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Billing Conductor. Para obtener más información, consulte <a href="#">Temas de Servicio de AWS para CloudTrail</a> y <a href="#">Registro de llamadas a la API de AWS Billing Conductor con AWS CloudTrail</a> .        | 12 de marzo de 2024 |

|                                        |                                                                                                                                                                                                                                                                                                                                                    |                       |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en registros de seguimiento de AWS X-Ray y nodos administrados de AWS Systems Manager mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                     | 7 de marzo de 2024    |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en los dominios de Amazon Simple Workflow Service (Amazon SWF) mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                                                            | 14 de febrero de 2024 |
| <a href="#">Funcionalidad agregada</a> | CloudTrail agregó la API <code>ListInsightsMetricData</code> . La API <code>ListInsightsMetricData</code> devuelve los datos de las métricas de Insights de los registros de seguimiento que tienen Insights activado. Para obtener más información, consulte <a href="#">ListInsightsMetricData</a> en la Referencia de la API de AWS CloudTrail. | 6 de febrero de 2024  |



|                                                    |                                                                                                                                                                                                                                                                          |                         |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>             | Ahora puede registrar eventos de datos de CloudTrail para AWS IoT, AWS IoT SiteWise y AWS AppConfig mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                  | 4 de enero de 2024      |
| <a href="#">Funcionalidad agregada</a>             | Ahora puede registrar eventos de datos de CloudTrail para AWS IoT Greengrass mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Eventos de datos</a> .                                                                         | 22 de diciembre de 2023 |
| <a href="#">Compatibilidad con nuevas regiones</a> | CloudTrail amplió la compatibilidad con una nueva región: la región Oeste de Canadá (Calgary). Para más información, consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                      | 20 de diciembre de 2023 |
| <a href="#">Funcionalidad agregada</a>             | Ahora puede registrar eventos de datos de CloudTrail 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 <a href="#">Eventos de datos</a> . | 20 de diciembre de 2023 |

### Actualización de la política administrada de AWS

Se actualizó la política administrada [CloudTrailServiceRolePolicy](#) para permitir las siguientes acciones en el almacén de datos de eventos de una organización cuando la federación está deshabilitada: `glue:DeleteTable` y `lakeformation:DeleteResource` .

26 de noviembre de 2023

### Funcionalidad agregada

Ahora puede federar un almacén de datos de eventos de CloudTrail Lake 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 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. Para obtener más información, consulte [Federación de un almacén de datos de eventos](#).

26 de noviembre de 2023

Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail para AWS Cloud Map mediante selectores 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 datos de CloudTrail 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: precios de retención ampliables por un año y precios 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 precios de retención de siete años a usar el precio de retención ampliable por un año con la [consola de CloudTrail](#), la [AWS CLI](#) o la operación [UpdateEventDataStore](#) de la API. 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 eventos de Insights en CloudTrail Lake. AWS CloudTrail Insights ayuda a los usuarios de AWS a identificar y responder a la actividad inusual asociada a las tasas de llamada a la API y las tasas de error de la API mediante el análisis continuo de los eventos de administración de CloudTrail. Para recopilar 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 almacén de datos de eventos de destino que recopile 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 [Creación de un almacén de datos de eventos para los eventos de CloudTrail Insights](#) y [Registre 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 [Temas de Servicio de AWS para CloudTrail](#) y [Registro de llamadas a la API de AWS Launch Wizard con 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 [Temas de Servicio de AWS para CloudTrail](#) y [Registrar las llamadas a la API de Amazon Bedrock con AWS CloudTrail](#).

23 de octubre de 2023

[Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en las personalizaciones de Amazon CodeWhisperer 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 datos de CloudTrail en las bases de datos y las tablas de Amazon Timestream mediante selectores de eventos avanzados. Para obtener más información, consulte [Registro de eventos de datos](#).

28 de septiembre de 2023

|                                                             |                                                                                                                                                                                                                                                                                                                                                            |                          |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">Funcionalidad agregada</a>                      | Ahora puede registrar eventos de datos de CloudTrail en los temas de Amazon SNS y los puntos de conexión de la plataforma mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                                                                                  | 28 de septiembre de 2023 |
| <a href="#">Documentación actualizada</a>                   | Se agregó una tabla para mostrar las tareas que la cuenta de administración, las cuentas de administrador delegado y las cuentas de miembros de una organización de AWS Organizations pueden hacer en CloudTrail. Para obtener más información, consulte <a href="#">Organization delegated administrator</a> (Administrador delegado de la organización). | 25 de septiembre de 2023 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con los acuerdos de AWS Marketplace. Para obtener más información, consulte <a href="#">Temas de Servicio de AWS para CloudTrail</a> y <a href="#">Registro de llamadas a la API de acuerdos con AWS CloudTrail</a> .                                                                                                           | 1 de septiembre de 2023  |

|                                                             |                                                                                                                                                                                                                                                                                                                       |                      |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">Funcionalidad agregada</a>                      | Ahora puede registrar eventos de datos de CloudTrail en los puntos de conexión de Amazon Kinesis Video Streams y Amazon SageMaker AI mediante el uso de selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                        | 31 de agosto de 2023 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | 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 <a href="#">Servicios e integraciones admitidos de CloudTrail</a> . | 26 de agosto de 2023 |
| <a href="#">Funcionalidad agregada</a>                      | Ahora puede registrar eventos de datos de CloudTrail en el conector de AWS Private CA para Active Directory mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                                                           | 24 de agosto de 2023 |



### [Documentación actualizada](#)

Se agregaron nuevos escenarios de CloudTrail Lake en los que se muestra cómo crear almacenes de datos de eventos, ver los paneles de CloudTrail Lake, copiar eventos de registros de seguimiento en un almacén de datos de eventos, ver y ejecutar consultas de ejemplo y guardar los resultados de las consultas en un bucket de Amazon S3 mediante la Consola de administración de AWS. Para obtener más información, consulte [Scenarios for CloudTrail Lake](#).

16 de agosto de 2023

### [Compatibilidad con nuevas regiones](#)

CloudTrail amplió la compatibilidad con una nueva región: la región Israel (Tel Aviv). Para más información, consulte [Regiones compatibles con CloudTrail](#).

1 de agosto de 2023

### [Se agregó compatibilidad para los servicios](#)

Esta versión es compatible con AWS HealthImaging. Para obtener más información, consulte [Servicios e integraciones compatibles con CloudTrail](#) y [Registro de llamadas a la API de AWS HealthImaging mediante AWS CloudTrail](#).

26 de julio de 2023

|                                        |                                                                                                                                                                                                                                                                                          |                     |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en los almacenes de datos de AWS HealthImaging mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                                      | 26 de julio de 2023 |
| <a href="#">Funcionalidad agregada</a> | Ahora puede registrar eventos de datos de CloudTrail en los canales de control de AWS Systems Manager y las redes de Amazon Managed Blockchain mediante el uso de selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> . | 21 de junio de 2023 |
| <a href="#">Funcionalidad agregada</a> | Ahora puede verificar los resultados de consultas guardados en CloudTrail Lake mediante el comando <code>aws cloudtrail verify-query-results</code> . Para obtener más información, consulte <a href="#">Validar los resultados de consultas guardados con la AWS CLI</a> .              | 21 de junio de 2023 |

### [Se agregó compatibilidad para los servicios](#)

Esta versión es compatible con Amazon Verified Permissions. Para obtener más información, consulte [Servicios e integraciones compatibles con CloudTrail y Registro de llamadas a la API de Amazon Verified Permissions mediante la AWS CloudTrail](#).

13 de junio de 2023

### [Funcionalidad agregada](#)

Ahora puede utilizar los paneles de CloudTrail Lake para ver los eventos de un almacén de datos de eventos. Para obtener más información, consulte [Ver los paneles de Lake](#).

13 de junio de 2023

### [Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en los almacenes de políticas de Amazon Verified Permissions mediante el uso de selectores de eventos avanzados. Para obtener más información, consulte [Registro de eventos de datos](#).

13 de junio de 2023

### [Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en un perfil de Amazon CodeWhisperer mediante selectores de eventos avanzados. Para obtener más información, consulte [Registro de eventos de datos](#).

6 de junio de 2023

### Funcionalidad agregada

Ahora puede iniciar y detener la ingesta de eventos en los almacenes de datos de eventos de CloudTrail. 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 la AWS CLI, consulte [Detener la ingesta de eventos en un almacén de datos de eventos](#).

2 de junio de 2023

### Funcionalidad agregada

Ahora puede registrar eventos de datos de CloudTrail en un espacio de trabajo de registros 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 información, consulte [Servicios e integraciones compatibles con CloudTrail](#) y [Registro de llamadas a la API de Amazon Security Lake mediante la AWS CloudTrail](#).

30 de mayo de 2023

|                                                |                                                                                                                                                                                                                                                                                                                                            |                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Versión del evento actualizada</a> | El eventVersion ahora es 1,09.                                                                                                                                                                                                                                                                                                             | 23 de mayo de 2023 |
| <a href="#">Documentación actualizada</a>      | Se actualizó el tema del elemento userIdentity de CloudTrail para incluir un ejemplo y descripciones de campo para una solicitud hecha en nombre de un usuario de IAM Identity Center. Para obtener más información, consulte <a href="#">Elemento userIdentity de CloudTrail</a> .                                                        | 23 de mayo de 2023 |
| <a href="#">Documentación actualizada</a>      | Esta actualización admite la siguiente versión de parche para la biblioteca de procesamiento de CloudTrail: aws-cloudtrail-processing-library-1.6.1.jar. Para obtener más información, consulte <a href="#">Uso de la Biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub. | 23 de mayo de 2023 |
| <a href="#">Funcionalidad agregada</a>         | Ahora CloudTrail Lake admite todas las funciones y operadores de Presto. Para obtener más información, consulte <a href="#">Restricciones SQL de CloudTrail Lake</a> .                                                                                                                                                                     | 9 de mayo de 2023  |

|                                                             |                                                                                                                                                                                                                                                                                                                                                |                       |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Funcionalidad agregada</a>                      | Ahora puede registrar eventos de datos de CloudTrail en un detector de Amazon GuardDuty mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> y <a href="#">Registro de llamadas a la API de Amazon GuardDuty con la AWS CloudTrail</a> .                              | 30 de marzo de 2023   |
| <a href="#">Documentación actualizada</a>                   | 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 <a href="#">Creación de etiquetas de asignación de costos definidas por el usuario para almacenes de datos de eventos de CloudTrail Lake</a> . | 24 de marzo de 2023   |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con el Creador de redes de telecomunicaciones de AWS (AWS TNB). Para obtener más información, consulte <a href="#">Servicios e integraciones compatibles con CloudTrail y Llamadas a la API del Creador de redes de telecomunicaciones de AWS mediante la AWS CloudTrail</a> .                                      | 21 de febrero de 2023 |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                       |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Funcionalidad agregada</a>    | Ahora puede registrar eventos de datos de CloudTrail en los grupos de identidades de Amazon Cognito mediante selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                                                                                                                                                                                                  | 15 de febrero de 2023 |
| <a href="#">Documentación actualizada</a> | Se agregó una nueva sección sobre los recursos de aprendizaje disponibles para CloudTrail Lake. Para obtener más información, consulte <a href="#">Learning resources</a> (Recursos de aprendizaje).                                                                                                                                                                                                                                                 | 9 de febrero de 2023  |
| <a href="#">Funcionalidad agregada</a>    | Ahora puede crear integraciones de CloudTrail Lake con orígenes de eventos externos a AWS. 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 <a href="#">Crear una integración con un origen de eventos externo a AWS</a> . | 31 de enero de 2023   |

|                                                    |                                                                                                                                                                                                                                                                               |                         |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>             | Ahora puede registrar eventos de datos de CloudTrail en la actividad de PutAuditEvents de CloudTrail en un canal de CloudTrail Lake mediante el uso de selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> . | 31 de enero de 2023     |
| <a href="#">Compatibilidad con nuevas regiones</a> | CloudTrail amplió la compatibilidad con una nueva región: la región Asia-Pacífico (Melbourne). Para más información, consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                           | 24 de enero de 2023     |
| <a href="#">Documentación actualizada</a>          | Se agregó una nueva sección sobre la administración de la coherencia de datos en CloudTrail, consulte <a href="#">Managing data consistency in CloudTrail</a> (Administración de la coherencia de datos en CloudTrail).                                                       | 18 de enero de 2023     |
| <a href="#">Funcionalidad agregada</a>             | Ahora puede registrar eventos de datos de CloudTrail en los almacenes de características de Amazon SageMaker AI mediante el uso de selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                     | 27 de diciembre de 2022 |



### [Se agregó compatibilidad para los servicios](#)

Esta versión es compatible con AWS Marketplace Discovery. Consulte [Servicios e integraciones admitidos con AWS CloudTrail](#).

15 de diciembre de 2022

### [Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en los componentes de prueba experimental de las métricas de Amazon SageMaker AI mediante el uso de 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 en él elementos de configuración de AWS Config y utilizarlo para investigar los cambios en los entornos de producción que no cumplen con los requisitos. Para obtener más información, consulte [Creación de un almacén de datos de eventos para los elementos de configuración de AWS Config](#).

28 de noviembre de 2022

### [Compatibilidad con nuevas regiones](#)

CloudTrail amplió la compatibilidad con una nueva región: la región Asia-Pacífico (Hyderabad). Para más información, consulte [Regiones compatibles con CloudTrail](#).

22 de noviembre de 2022

### [Funcionalidad agregada](#)

Ahora puede registrar eventos de datos de CloudTrail en los entornos de Amazon FinSpace mediante el uso de 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 la compatibilidad con una nueva región: la región Europa (España). Para más información, consulte [Regiones compatibles con CloudTrail](#).

16 de noviembre de 2022

### [Compatibilidad con nuevas regiones](#)

CloudTrail amplió la compatibilidad con una nueva región: la región Europa (Zúrich). Para más información, consulte [Regiones compatibles con CloudTrail](#).

9 de noviembre de 2022

### Funcionalidad agregada

La cuenta de administración de una organización de AWS Organizations ahora puede agregar un administrador delegado para que se encargue de los registros de seguimiento y los almacenes de datos de eventos de CloudTrail 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 cifrado de AWS Key Management Service para los almacenes 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 registro de seguimiento de CloudTrail en un almacén de datos de eventos de CloudTrail Lake. Para obtener más información, consulte [Copia de eventos de registro de seguimiento en CloudTrail Lake](#).

19 de septiembre de 2022

### Documentación actualizada

Se agregó una lista de métricas de Amazon CloudWatch admitidas para CloudTrail Lake. Para obtener más información, consulte [Métricas de CloudWatch admitidas](#).

16 de septiembre de 2022

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>             | Ahora puede ver los canales vinculados a servicios de CloudTrail con la AWS CLI. Para obtener más información, consulte <a href="#">Visualización de canales vinculados a servicios para CloudTrail con la AWS CLI</a> .                                                                                                                                                                                                | 9 de septiembre de 2022 |
| <a href="#">Compatibilidad con nuevas regiones</a> | CloudTrail amplió la compatibilidad con una nueva región: la región Medio Oriente (EAU). Para más información, consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                                                                                                           | 30 de agosto de 2022    |
| <a href="#">Funcionalidad modificada</a>           | CloudTrail ha cambiado el nombre de la política administrada AWSCloudTrailReadOnlyAccess por AWSCloudTrail_ReadOnlyAccess. Se han reducido los permisos de esta política. De manera predeterminada, la política ya no concede permiso para ver una lista de todos los buckets de Amazon S3, funciones de AWS Lambda o alias de AWS KMS. Para obtener más información, consulte <a href="#">Acceso de solo lectura</a> . | 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 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 comenzó a cambiar los valores de los campos `userAgent` y `sourceIPAddress` en cualquier evento que se haya originado a partir de una sesión de Consola de administración de AWS en la que se hubiera utilizado un cliente proxy. Para estos eventos, CloudTrail sustituye los valores de los campos `userAgent` y `sourceIPAddress` con `AWS Internal`. CloudTrail realizó este cambio para estandarizar la forma en que registra la información de las acciones de servicio en todos los servicios de AWS. Para obtener más información, consulte [Contenido de registros de CloudTrail](#).

12 de abril de 2022

### Se agregó compatibilidad para los servicios

Esta versión es compatible con Amazon GameParks. Consulte [Servicios e integraciones admitidos con AWS CloudTrail](#).

24 de marzo de 2022

### [Se agregó compatibilidad para los servicios](#)

Esta versión es compatible con Servicio de administración de envíos AWS App Mesh. 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 característica que permite ejecutar consultas SQL detalladas y sobre múltiples campos en los 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, consulta [Trabajar con CloudTrail](#).

4 de marzo de 2022



## Funcionalidad modificada

Ahora, CloudTrail elimina el ID de la cuenta del propietario del bucket de Amazon S3 del bloque `resources` de un evento de datos si se cumplen las dos condiciones siguientes: la llamada a la API de eventos de datos proviene de una cuenta de AWS distinta a la del propietario del bucket de Amazon S3 y el llamante de la API recibió un error `AccessDenied` que era solo para la cuenta del llamante. 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](#)

28 de enero de 2022

Esta actualización es compatible con la siguiente versión de la biblioteca de procesamiento de CloudTrail: soporte adicional para implementar un administrador de S3 personalizado, registro de eventos para registrar las excepciones relacionadas con archivos de registro, soporte para analizar un campo `errorCode` opcional en `insightDetails`, y se ha actualizado la regex de análisis del ID de la cuenta para aceptar valores no numéricos. Para obtener más información, consulte [Uso de la Biblioteca de procesamiento de CloudTrail](#) y [Biblioteca de procesamiento de CloudTrail](#) en GitHub.

### Funcionalidad agregada

CloudTrail presenta CloudTrail Lake, una nueva característica que le permite ejecutar consultas SQL detalladas de múltiples 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 CloudTrail](#).

5 de enero de 2022

### Compatibilidad con nuevas regiones

CloudTrail amplió la compatibilidad con una nueva región: la región Asia-Pacífico (Yakarta). Para más información, consulte [Regiones compatibles con CloudTrail](#).

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

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                  |                         |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>                      | Ahora puede registrar eventos de datos de CloudTrail en las tablas de AWS Glue creadas por Lake Formation mediante el uso de selectores de eventos avanzados. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                                                                                                                                                              | 30 de noviembre de 2021 |
| <a href="#">Funcionalidad modificada</a>                    | Como práctica recomendada de seguridad, ahora puede agregar una clave de condición <code>aws:SourceArn</code> o <code>aws:SourceAccount</code> para las políticas de claves AWS KMS y las políticas de bucket de Amazon S3. Para obtener más información, consulte <a href="#">Configurar las políticas de claves de AWS KMS para CloudTrail</a> y <a href="#">Configurar políticas de bucket de Amazon S3 para CloudTrail</a> . | 15 de noviembre de 2021 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con el centro de resiliencia de AWS. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                | 10 de noviembre de 2021 |

Funcionalidad agregada

Hay disponible un nuevo tipo de evento CloudTrail Insights: eventos de Insights de tasa de errores. 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 datos de CloudTrail en DynamoDB streams 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 un registro de seguimiento para enviar notificaciones a Amazon SNS, CloudTrail agrega una instrucción a su política de acceso a temas de SNS que permite a CloudTrail enviar contenido a un tema de SNS. Por seguridad, recomendamos que agregue una clave de condición `aws:SourceArn` o `aws:SourceAccount` a la instrucción de la política de CloudTrail. Para obtener más información, consulte [Política de temas 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 eventos que tienen enteros en los campos de un evento de datos, CloudTrail ha procesado históricamente estos números como flotantes. Ahora, CloudTrail mantiene el formato original de enteros en eventos de datos. Para obtener más información, consulte [Uso de la biblioteca de procesamiento de CloudTrail](#).

13 de julio de 2021

|                                                             |                                                                                                                                                                                                                                                  |                     |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Funcionalidad agregada</a>                      | 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 <a href="#">Registro de eventos de administración para registros de seguimiento</a> . | 1 de julio de 2021  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS BugBust Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                     | 24 de junio de 2021 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Managed Grafana y Amazon Managed Service for Prometheus. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                 | 2 de junio de 2021  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS App Runner. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                 | 18 de mayo de 2021  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Systems Manager Incident Manager. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                           | 10 de mayo de 2021  |



### Documentación actualizada

Esta actualización describe los requisitos de registro de eventos de datos para los paquetes de conformidad de AWS Config, especialmente para marcos de conformidad 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

Después de que un administrador de IAM configura [AWS STS](#), CloudTrail registra sourceIdentity información en eventos cuando los usuarios adoptan un rol de IAM o realizan acciones con dicho rol. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).

13 de abril de 2021

Documentación actualizada

Esta actualización documenta límites, en kilobytes (KB), de contenido en algunos campos de registro de eventos de CloudTrail. Para obtener más información, consulte [Contenido de registros de CloudTrail](#).

8 de abril de 2021

Funcionalidad agregada

Después de que un administrador de IAM configura [AWS STS](#), CloudTrail registra sourceIdentity información en eventos cuando los usuarios adoptan un rol de IAM o realizan acciones con dicho rol. 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

|                                                             |                                                                                                                                                                                                                                     |                     |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite Amazon Managed Workflows for Apache Airflow Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                   | 22 de marzo de 2021 |
| <a href="#">Funcionalidad agregada</a>                      | 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 <a href="#">Registro de eventos de datos</a> .           | 18 de marzo de 2021 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Fault Injection Simulator Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                      | 15 de marzo de 2021 |
| <a href="#">Funcionalidad agregada</a>                      | 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 <a href="#">Registro de eventos de datos</a> . | 1 de marzo de 2021  |

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                |                      |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Managed Blockchain y la versión preliminar de Ethereum for Managed Blockchain. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                         | 4 de febrero de 2021 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Amplify. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                                             | 3 de febrero de 2021 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Lookout for Metrics. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                   | 1 de febrero de 2021 |
| <a href="#">Documentación actualizada</a>                   | Esta actualización admite la siguiente versión de parche para la biblioteca de procesamiento de CloudTrail. Actualice las referencias del archivo .jar en la guía del usuario para utilizar la última versión, aws-cloud-trail-processing-library-1.4.0.jar. Para obtener más información, consulte <a href="#">Uso de la Biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub. | 12 de enero de 2021  |

|                                                             |                                                                                                                                                                                                     |                         |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Funcionalidad agregada</a>                      | Ahora puede registrar eventos de datos en Amazon S3 en AWS Outposts. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                          | 21 de diciembre de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Lookout for Equipment, AWS Well-Architected Tool y Amazon Location Service. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> . | 16 de diciembre de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS IoT Greengrass V2. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                             | 15 de diciembre de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon EMR en EKS. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                 | 10 de diciembre de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Audit Manager y Amazon HealthLake. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                             | 8 de diciembre de 2020  |

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                         |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Lookout for Vision. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                  | 1 de diciembre de 2020  |
| <a href="#">Versión del evento actualizada</a>              | La versión del evento AWS CloudTrail ahora es 1.08. La versión 1.08 introduce nuevos campos para CloudTrail. Para obtener más información, consulte <a href="#">Contenido de registros de CloudTrail</a> .                                                                                                                                                                                                                                                                                   | 24 de noviembre de 2020 |
| <a href="#">Funcionalidad agregada</a>                      | AWS CloudTrail introduce 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 recursos específicos de AWS y seleccionar las API específicas en esos recursos para registrar en su registro de seguimiento. Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> . | 24 de noviembre de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Network Firewall. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                       | 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 [Concesión de permisos personalizados a usuarios de CloudTrail](#).

29 de septiembre de 2020

### Documentación actualizada

Esta actualización es compatible con la siguiente versión de parche para la biblioteca de procesamiento de CloudTrail. Actualice las referencias del archivo .jar en la guía del usuario para utilizar la última versión, aws-cloudtrail-processing-library-1.3.0.jar. Para obtener más información, consulte [Uso de la Biblioteca de procesamiento de CloudTrail](#) y [Biblioteca de procesamiento de CloudTrail](#) 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 introduce campos de atribuciones para eventos de información de CloudTrail. 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 comparación, los campos de atribuciones 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 Insights](#).

13 de agosto de 2020

### Funcionalidad agregada

La consola de AWS CloudTrail tiene un nuevo aspecto diseñado para facilitar el uso. La Guía del usuario de AWS CloudTrail se ha actualizado con cambios en los procedimientos para realizar tareas en la consola, como la creación de registros de seguimiento, la actualización de estos y la descarga del historial de eventos.

13 de agosto de 2020

|                                                             |                                                                                                                                         |                     |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite Amazon Interactive Video Service. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> . | 15 de julio de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Honeycode. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .      | 24 de junio de 2020 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Macie. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .          | 19 de mayo de 2020  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Kendra. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .         | 13 de mayo de 2020  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS IoT SiteWise. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                 | 29 de abril de 2020 |
| <a href="#">Se agregó compatibilidad con regiones</a>       | Esta versión es compatible con una región más: Europa (Milán). Consulte <a href="#">Regiones compatibles de AWS CloudTrail</a> .        | 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

Las acciones de gran volumen de AWS KMS como Encrypt, Decrypt y GenerateDataKey ahora se registran como eventos Read (de lectura). Si decide registrar todos los eventos de AWS KMS en su seguimiento, así como los eventos de administración de escritura, el seguimiento registrará las acciones relevantes de AWS KMS como Disable, 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 de la Biblioteca de procesamiento de CloudTrail: actualice las referencias del archivo .jar en la guía del usuario para utilizar la última versión, aws-cloudtrail-processing-library-1.2.0.jar. Para obtener más información, consulte [Uso de la Biblioteca de procesamiento de CloudTrail](#) y [Biblioteca de procesamiento de CloudTrail](#) en GitHub.

21 de noviembre de 2019

### [Funcionalidad agregada](#)

Esta versión es compatible con CloudTrail de AWS y lo ayuda a detectar actividad es inusuales en su cuenta. Consulte [Registro de eventos de información para registros de seguimiento](#).

20 de noviembre de 2019

### [Funcionalidad agregada](#)

Esta versión agrega una opción para filtrar eventos de AWS Key Management Service en un registro de seguimiento. Consulte [Creación de un registro de seguimiento](#).

20 de noviembre de 2019

|                                                             |                                                                                                                                                                                                                                                        |                        |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Notificaciones de AWS CodeStar. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                       | 7 de noviembre de 2019 |
| <a href="#">Funcionalidad agregada</a>                      | Esta versión admite la adición de etiquetas al crear un registro de seguimiento en CloudTrail, ya sea a través de la consola de CloudTrail o la API. Esta versión agrega dos nuevas API, <code>GetTrail</code> y <code>ListTrails</code> .             | 1 de noviembre de 2019 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS App Mesh. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                    | 17 de octubre de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Translate. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                     | 17 de octubre de 2019  |
| <a href="#">Actualización de la documentación</a>           | El tema Unsupported Services (Servicios no compatibles) se ha restaurado y actualizado para incluir únicamente los servicios de AWS que actualmente no registran eventos en CloudTrail. Consulte <a href="#">Servicios CloudTrail no compatibles</a> . | 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, [Administración de los costos de CloudTrail](#), para ayudarlo a obtener los datos de registro que necesita de CloudTrail sin tener que superar su 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

|                                                             |                                                                                                                                             |                     |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Se agregó compatibilidad con regiones</a>       | Esta versión es compatible con una región más: Medio Oriente (Baréin). Consulte <a href="#">Regiones compatibles de AWS CloudTrail</a> .    | 29 de julio de 2019 |
| <a href="#">Actualización de la documentación</a>           | La documentación se ha actualizado con información sobre seguridad de CloudTrail. Consulte <a href="#">Seguridad en AWS CloudTrail</a> .    | 3 de julio de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Ground Station. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                   | 6 de junio de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS IoT Things Graph. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                 | 4 de junio de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite Amazon WorkSpaces Applications. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .       | 25 de abril de 2019 |
| <a href="#">Se agregó compatibilidad con regiones</a>       | Esta versión es compatible con una región más: Asia Pacífico (Hong Kong). Consulte <a href="#">Regiones compatibles de AWS CloudTrail</a> . | 24 de abril de 2019 |

|                                                             |                                                                                                                                                               |                      |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con el Amazon Managed Service para Apache Flink. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> . | 22 de marzo de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Backup. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                             | 4 de febrero de 2019 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon WorkLink. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                             | 23 de enero de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Cloud9. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                             | 21 de enero de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Elemental MediaLive. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                | 19 de enero de 2019  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con Amazon Comprehend. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                           | 18 de enero de 2019  |



|                                                             |                                                                                                                                                                                                                                                                    |                         |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS Elemental MediaPackage. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                  | 21 de diciembre de 2018 |
| <a href="#">Se agregó compatibilidad con regiones</a>       | Esta versión es compatible con una región más: UE (Estocolmo). Consulte <a href="#">Regiones compatibles de AWS CloudTrail</a> .                                                                                                                                   | 11 de diciembre de 2018 |
| <a href="#">Actualización de la documentación</a>           | La documentación se ha actualizado con información sobre los servicios admitidos y no admitidos. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                 | 3 de diciembre de 2018  |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con AWS Resource Access Manager (AWS RAM). Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                            | 20 de noviembre de 2018 |
| <a href="#">Funcionalidad actualizada</a>                   | Esta versión admite la creación de un registro de seguimiento en CloudTrail que registra los eventos de todas las cuentas de AWS en una organización en AWS Organizations. Consulte <a href="#">Creación de un registro de seguimiento para una organización</a> . | 19 de noviembre de 2018 |

|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                         |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión es compatible con la API de SMS y voz de Amazon Pinpoint. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                 | 16 de noviembre de 2018 |
| <a href="#">Se agregó compatibilidad para los servicios</a> | Esta versión admite AWS IoT Greengrass. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                | 29 de octubre de 2018   |
| <a href="#">Documentación actualizada</a>                   | Esta actualización es compatible con la siguiente versión de parche para la biblioteca de procesamiento de CloudTrail. Actualice las referencias del archivo .jar en la guía del usuario para utilizar la última versión, aws-cloudtrail-processing-library-1.1.3.jar. Para obtener más información, consulte <a href="#">Uso de la Biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub. | 18 de octubre de 2018   |
| <a href="#">Funcionalidad agregada</a>                      | Esta versión admite el uso de filtros adicionales en Event history. Consulte <a href="#">Ver eventos de CloudTrail en la consola de CloudTrail</a> .                                                                                                                                                                                                                                                                                                     | 18 de octubre de 2018   |

|                                                                                                                        |                                                                                                                                                                                                                                                   |                     |
|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Funcionalidad agregada</a>                                                                                 | Esta versión es compatible con Amazon Virtual Private Cloud (Amazon VPC) para establecer una conexión privada entre su VPC y AWS CloudTrail. Consulte <a href="#">Uso de AWS CloudTrail con los puntos de enlace de la VPC de tipo interfaz</a> . | 9 de agosto de 2018 |
| <a href="#">Se agregó compatibilidad para los servicios</a>                                                            | Esta versión es compatible con Amazon Data Lifecycle Manager. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                   | 24 de julio de 2018 |
| <a href="#">Se agregó compatibilidad para los servicios</a>                                                            | Esta versión es compatible con Amazon MQ. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                                       | 19 de julio de 2018 |
| <a href="#">Se agregó compatibilidad para los servicios</a>                                                            | Esta versión es compatible con la CLI de AWS Mobile. Consulte <a href="#">Servicios e integraciones admitidos con AWS CloudTrail</a> .                                                                                                            | 29 de junio de 2018 |
| <a href="#">AWS CloudTrail Notificación del historial de la documentación de disponible a través de una fuente RSS</a> | Ahora puede recibir notificaciones sobre las actualizaciones de la documentación de AWS CloudTrail suscribiéndose a una fuente RSS.                                                                                                               | 29 de junio de 2018 |

## Actualizaciones anteriores

En la siguiente tabla se describe el historial de versiones de la documentación de AWS CloudTrail anteriores 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 <a href="#">Servicios e integraciones admitidos de CloudTrail</a> .                                                                                                                                                    | 21 de junio de 2018  |
| Funcionalidad agregada                      | Esta versión permite registrar todos los eventos de administración de CloudTrail en el historial de eventos. Para obtener más información, consulte <a href="#">Trabajar con el historial de eventos de CloudTrail</a> .                                                                                                                  | 14 de junio de 2018  |
| Se agregó compatibilidad para los servicios | Esta versión admite Administración de facturación y costos de AWS. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                           | 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 <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                 | 5 de junio de 2018   |
| Documentación actualizada                   | <p>Esta actualización es compatible con la siguiente versión del parche de la biblioteca de procesamiento de CloudTrail:</p> <ul style="list-style-type: none"><li>• Actualice las referencias al archivo .jar en la guía del usuario para poder utilizar la versión más reciente: aws-cloudtrail-processing-library-1.1.2.jar.</li></ul> | 16 de mayo de 2018   |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Fecha de lanzamiento |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
|                                             | Para obtener más información, consulte <a href="#">Uso de la biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub.                                                                                                                                                                                                                                                                                                                                                    |                      |
| Se agregó compatibilidad para los servicios | Esta versión admite Administración de facturación y costos de AWS. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                      | 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 <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                            | 5 de junio de 2018   |
| Documentación actualizada                   | <p>Esta actualización es compatible con la siguiente versión del parche de la biblioteca de procesamiento de CloudTrail:</p> <ul style="list-style-type: none"> <li>• Actualice las referencias al archivo .jar en la guía del usuario para poder utilizar la versión más reciente: aws-cloudtrail-processing-library-1.1.2.jar.</li> </ul> <p>Para obtener más información, consulte <a href="#">Uso de la biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub.</p> | 16 de mayo de 2018   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS X-Ray. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                                          | 25 de abril de 2018  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con AWS IoT Analytics. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                       | 23 de abril de 2018  |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Fecha de lanzamiento  |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Secrets Manager. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                   | 10 de abril de 2018   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Rekognition. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                | 6 de abril de 2018    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con AWS Private Certificate Authority (PCA). Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                           | 4 de abril de 2018    |
| Funcionalidad agregada                      | Esta versión facilita la búsqueda en archivos de registros de CloudTrail con Amazon Athena. Puede crear tablas de forma automática para consultar los registros directamente en la consola de CloudTrail y utilizar esas tablas para ejecutar consultas en Athena. Para obtener más información, consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> y <a href="#">Creación de una tabla para registros de CloudTrail en la consola de CloudTrail</a> . | 15 de marzo de 2018   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS AppSync. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                  | 13 de febrero de 2018 |
| Se añadió compatibilidad con regiones       | Esta versión es compatible con una región más: Asia-Pacífico (Osaka) (ap-northeast-3). Consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                                                                                                                                                                                          | 12 de febrero de 2018 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Shield. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                   | 12 de febrero de 2018 |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                  | Fecha de lanzamiento    |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon SageMaker AI. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                             | 11 de enero de 2018     |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Batch. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                  | 10 de enero de 2018     |
| Funcionalidad agregada                      | Esta versión permite ampliar a 90 días la cantidad de actividad de la cuenta que está disponible en el historial de eventos de CloudTrail. También puede personalizar la visualización de las columnas para ver mejor los eventos de CloudTrail. Para obtener más información, consulte <a href="#">Trabajar con el historial de eventos de CloudTrail</a> . | 12 de diciembre de 2017 |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon WorkMail. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                 | 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 <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                       | 1 de diciembre de 2017  |
| Se agregó funcionalidad y documentación     | Esta versión soporta registrar eventos de datos para funciones de AWS Lambda.<br><br>Para obtener más información, consulte <a href="#">Registro de eventos de datos</a> .                                                                                                                                                                                   | 30 de noviembre de 2017 |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Fecha de lanzamiento    |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Se agregó funcionalidad y documentación     | <p>Esta versión soporta registrar eventos de datos para funciones de AWS Lambda.</p> <p>Para obtener más información, consulte <a href="#">Registro de eventos de datos</a>.</p>                                                                                                                                                                                                                                                                                                                                               | 30 de noviembre de 2017 |
| Se agregó funcionalidad y documentación     | <p>Esta versión admite las siguientes actualizaciones de la biblioteca de procesamiento de CloudTrail:</p> <ul style="list-style-type: none"> <li>• Agregue compatibilidad con la identificación mediante valores booleanos de eventos de administración.</li> <li>• Actualice la versión de eventos de CloudTrail a 1.06.</li> </ul> <p>Para obtener más información, consulte <a href="#">Uso de la biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub.</p> | 30 de noviembre de 2017 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Glue. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                                     | 7 de noviembre de 2017  |
| Nueva documentación                         | Esta versión agrega un nuevo tema, <a href="#">Cuotas en AWS CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 19 de octubre de 2017   |
| Documentación actualizada                   | Esta versión es una actualización de la documentación sobre las API compatibles con el historial de eventos de CloudTrail para Amazon Athena, AWS CodeBuild, Amazon Elastic Container Registry y AWS Migration Hub.                                                                                                                                                                                                                                                                                                            | 13 de octubre de 2017   |



| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                             | Fecha de lanzamiento     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Chime. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                               | 27 de septiembre de 2017 |
| Se agregó funcionalidad y documentación     | Esta versión permite configurar el registro de eventos de datos para todos los buckets de Amazon S3 incluidos en su cuenta de AWS. Consulte <a href="#">Registro de eventos de datos</a> .                                                                                                                                                                                                                                                              | 20 de septiembre de 2017 |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Lex. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                 | 15 de agosto de 2017     |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Migration Hub. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                     | 14 de agosto de 2017     |
| Se agregó funcionalidad y documentación     | Esta versión admite que se active CloudTrail de forma predeterminada para todas las cuentas de AWS. Los últimos siete días de actividad de la cuenta están disponibles en el historial de eventos de CloudTrail y los eventos más recientes aparecen en el panel 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). | 14 de agosto de 2017     |
| Se agregó funcionalidad y documentación     | Esta versión admite la descarga de eventos en la consola de CloudTrail en la página de historial de actividades de la API. Puede descargar eventos en formato JSON o CSV.<br><br>Para obtener más información, consulte <a href="#">Descarga de eventos</a> .                                                                                                                                                                                           | 27 de julio de 2017      |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                              | Fecha de lanzamiento |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Funcionalidad agregada                      | <p>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).</p> <p>Para obtener más información, consulte <a href="#">Trabajar con archivos de registros de CloudTrail</a>.</p>                                                                  | 19 de julio de 2017  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con las búsquedas de las API para Amazon CloudWatch Events en la característica de historial de actividades de la API de CloudTrail.                                                                                                                                                                                          | 27 de junio de 2017  |
| Se agregó funcionalidad y documentación     | <p>Esta versión es compatible con las API adicionales de la característica de historial de actividades de la API de CloudTrail para los siguientes servicios:</p> <ul style="list-style-type: none"><li>• AWS CloudHSM</li><li>• Amazon Cognito</li><li>• Amazon DynamoDB</li><li>• Amazon EC2</li><li>• Kinesis</li><li>• AWS Storage Gateway</li></ul> | 27 de junio de 2017  |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS CodeStar. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                           | 14 de junio de 2017  |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Fecha de lanzamiento |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Se agregó funcionalidad y documentación     | <p>Esta versión admite las siguientes actualizaciones de la biblioteca de procesamiento de CloudTrail:</p> <ul style="list-style-type: none"><li>• Admite diferentes formatos de mensajes SQS de la misma cola SQS para identificar los archivos de registros de CloudTrail. Se admiten los siguientes formatos:</li><li>• Notificaciones que CloudTrail envía a un tema de SNS</li><li>• Notificaciones que Amazon S3 envía a un tema SNS</li><li>• Notificaciones que Amazon S3 envía directamente a una cola SQS</li><li>• Agrega compatibilidad para la propiedad <code>deleteMessageUponFailure</code> , que se puede utilizar para eliminar mensajes que no se pueden procesar.</li></ul> <p>Para obtener más información, consulte <a href="#">Uso de la biblioteca de procesamiento de CloudTrail</a> y <a href="#">Biblioteca de procesamiento de CloudTrail</a> en GitHub.</p> | 1 de junio de 2017   |
| Se agregó compatibilidad para los servicios | <p>Esta versión es compatible con Amazon Athena. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 19 de mayo de 2017   |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                       | Fecha de lanzamiento |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Funcionalidad agregada                      | <p>Esta versión es compatible con el envío de eventos de datos a Amazon CloudWatch Logs.</p> <p>Para obtener más información sobre cómo configurar el registro de seguimiento para registrar eventos de datos, consulte <a href="#">Eventos de datos</a>.</p> <p>Para obtener más información, consulte Envío de eventos a CloudWatch Logs en la <a href="#">Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs</a>.</p> | 9 de mayo de 2017    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con el servicio de medición de AWS Marketplace. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                           | 2 de mayo de 2017    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Quick Suite. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                   | 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 <a href="#">Creación de un registro de seguimiento con la consola de CloudTrail</a> .                                                                                                 | 11 de abril de 2017  |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Fecha de lanzamiento  |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Se agregar documentación                    | <p>Si CloudTrail no envía registros al bucket de S3 ni notificaciones de SNS desde algunas regiones en su cuenta, es posible que deba actualizar las políticas.</p> <p>Para obtener más información sobre cómo actualizar la política del bucket de S3, consulte <a href="#">Errores comunes en la configuración de la política de Amazon S3</a>.</p> <p>Para obtener más información sobre cómo actualizar la política de temas de SNS, consulte <a href="#">CloudTrail no envía notificaciones a una región</a>.</p> | 31 de marzo de 2017   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Organizations. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                    | 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 <a href="#">Trabajar con archivos de registros de CloudTrail</a> .                                                                                                                                                                                                                                                               | 10 de febrero de 2017 |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Cloud Directory. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                    | 26 de enero de 2017   |
| Se agregó funcionalidad y documentación     | Esta versión es compatible con la búsqueda de las API para AWS CodeCommit, Amazon GameLift Servers y AWS Managed Services en el historial de actividades de la API de CloudTrail.                                                                                                                                                                                                                                                                                                                                      | 26 de enero de 2017   |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Fecha de lanzamiento    |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Funcionalidad agregada                      | <p>Esta versión admite la integración con AWS Health Dashboard.</p> <p>Puede utilizar AWS Health Dashboard para identificar si los registros de seguimiento no pueden enviar registros a temas de SNS o buckets de S3. Esto podría ocurrir si hay problemas con la política para el bucket de S3 o el tema de SNS. AWS Health Dashboard informa sobre los registros de seguimiento afectados y sugiere métodos para corregir la política.</p> <p>Para obtener más información, consulte la <a href="#">Guía del usuario de AWS Health</a>.</p> | 24 de enero de 2017     |
| Se agregó funcionalidad y documentación     | <p>Esta versión permite filtrar por fuente de evento en la consola de CloudTrail. El origen del evento muestra el servicio AWS al que se emitió la solicitud.</p> <p>Para obtener más información, consulte <a href="#">Visualización de eventos de administración recientes con la consola</a>.</p>                                                                                                                                                                                                                                           | 12 de enero de 2017     |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS CodeCommit. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                                               | 11 de enero de 2017     |
| Se agregó compatibilidad para los servicios | Esta versión admite Amazon Lightsail. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                                             | 23 de diciembre de 2016 |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con AWS Managed Services. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                                              | 21 de diciembre de 2016 |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                    | Fecha de lanzamiento    |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Se añadió compatibilidad con regiones       | Esta versión es compatible con la región Europa (Londres). Consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                                                                                                                      | 13 de diciembre de 2016 |
| Se añadió compatibilidad con regiones       | Esta versión es compatible con la región Canadá (Central). Consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                                                                                                                      | 8 de diciembre de 2016  |
| Se agregó compatibilidad para los servicios | <p>Esta versión es compatible con AWS CodeBuild. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a>.</p> <p>Esta versión admite AWS Health. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a>.</p> <p>Esta versión admite AWS Step Functions. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a>.</p> | 1 de diciembre de 2016  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Polly. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                      | 30 de noviembre de 2016 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS OpsWorks for Chef Automate. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                               | 23 de noviembre de 2016 |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Fecha de lanzamiento     |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Se agregó funcionalidad y documentación     | <p>Esta versión permite configurar el registro de seguimiento para registrar eventos de solo lectura, solo escritura o todos los eventos.</p> <p>CloudTrail permite que se registren operaciones de API en el nivel de objetos de Amazon S3 como, por ejemplo, <code>GetObject</code> , <code>PutObject</code> y <code>DeleteObject</code> . Puede configurar los registros de seguimiento para registrar operaciones de API de nivel de objeto.</p> <p>Para obtener más información, consulte <a href="#">Trabajar con archivos de registros de CloudTrail</a>.</p> | 21 de noviembre de 2016  |
| Se agregó funcionalidad y documentación     | <p>Esta versión admite más valores para el campo <code>userIdentity</code> : <code>AWSAccount</code> y <code>AWSService</code> . Para obtener más información, consulte <a href="#">Campos</a> para <code>userIdentity</code> .</p>                                                                                                                                                                                                                                                                                                                                  | 16 de noviembre de 2016  |
| Se agregó compatibilidad para los servicios | <p>Esta versión es compatible con Application Auto Scaling. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                          | 31 de octubre de 2016    |
| Se añadió compatibilidad con regiones       | <p>Esta versión es compatible con la región EE. UU. Este (Ohio). Consulte <a href="#">Regiones compatibles con CloudTrail</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                   | 17 de octubre de 2016    |
| Se agregó funcionalidad y documentación     | <p>Esta versión permite registrar eventos de servicios de AWS no generados por la API. Para obtener más información, consulte <a href="#">Servicio de AWSEventos de</a> .</p>                                                                                                                                                                                                                                                                                                                                                                                        | 23 de septiembre de 2016 |



| Cambio                                      | Descripción                                                                                                                                                                                                                        | Fecha de lanzamiento |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Se agregó funcionalidad y documentación     | Esta versión admite el uso de la consola de CloudTrail para ver los tipos de recursos que admite AWS Config. Para obtener más información, consulte <a href="#">Ver los recursos a los que se hace referencia con AWS Config</a> . | 7 de julio de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Service Catalog. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                              | 6 de julio de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Elastic File System (Amazon EFS). Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                               | 28 de junio de 2016  |
| Se añadió compatibilidad con regiones       | Esta versión admite una región más: ap-south-1 (Asia-Pacífico [Bombay]). Consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                            | 27 de junio de 2016  |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Application Discovery Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                | 12 de mayo de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con CloudWatch Logs en la región América del Sur (São Paulo). Para obtener más información, consulte <a href="#">Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs</a> .      | 6 de mayo de 2016    |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS WAF. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                          | 28 de abril de 2016  |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Support. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                      | 21 de abril de 2016  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Inspector. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                      | 20 de abril de 2016  |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                                                                               | Fecha de lanzamiento  |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Se agregó compatibilidad para los servicios | Esta versión admite AWS IoT. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                 | 11 de abril de 2016   |
| Se agregó funcionalidad y documentación     | Esta versión permite registrar llamadas a la API de AWS Security Token Service (AWS STS) realizadas con el lenguaje de marcado para confirmaciones de seguridad (SAML) e identidad federada web. Para obtener más información, consulte <a href="#">Valores de las API de AWS STS con SAML e identidad federada web</a> . | 28 de marzo de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Certificate Manager. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                 | 25 de marzo de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Data Firehose. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                         | 17 de marzo de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon CloudWatch Logs. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                       | 10 de marzo de 2016   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Cognito. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                               | 18 de febrero de 2016 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Database Migration Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                          | 4 de febrero de 2016  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon GameLift Servers (Amazon GameLift Servers). Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                            | 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 <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                             | 16 de enero de 2016     |
| Se añadió compatibilidad con regiones       | Esta versión es compatible con una región más: ap-northeast-2 (Asia-Pacífico [Seúl]). Consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                              | 6 de enero de 2016      |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Elastic Container Registry (Amazon ECR). Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                       | 21 de diciembre de 2015 |
| Se agregó funcionalidad y documentación     | Esta versión permite activar CloudTrail en todas las regiones y admite múltiples registros de seguimiento por región. Para obtener más información, consulte <a href="#">Trabajar con registros de seguimiento de CloudTrail</a> .                                                                                                                                                                                                                                                                                                | 17 de diciembre de 2015 |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Machine Learning. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                              | 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 <a href="#">Cifrado de archivos de registros, archivos de resumen y los almacenes de datos de eventos de CloudTrail con claves de AWS KMS (SSE-KMS)</a> , <a href="#">Validar la integridad de los archivos de registros de CloudTrail</a> y <a href="#">Actualización de un registro de seguimiento con la consola de CloudTrail</a> . | 1 de octubre de 2015    |
| Se agregó support para los servicios        | Esta versión es compatible con Amazon OpenSearch Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                                                            | 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 <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                            | 1 de septiembre de 2015 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Device Farm. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                    | 13 de julio de 2015     |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon API Gateway. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                      | 9 de julio de 2015      |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con CodePipeline. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                            | 9 de julio de 2015      |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon DynamoDB. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                         | 28 de mayo de 2015      |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Registros de CloudWatch en la región Oeste de EE. UU. (Norte de California). Para obtener más información sobre el soporte de CloudTrail para el monitoreo de CloudWatch Logs, consulte <a href="#">Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs</a> . | 19 de mayo de 2015      |
| Se agregó compatibilidad para los servicios | Esta versión admite Directory Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                  | 14 de mayo de 2015      |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Simple Email Service (Amazon SES). Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                | 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. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                     | 9 de abril de 2015    |
| Se agregó compatibilidad para los servicios                  | Esta versión admite AWS Lambda. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                                      | 9 de abril de 2015    |
| Se agregó compatibilidad para los servicios                  | Esta versión es compatible con Amazon WorkSpaces. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                                                                                                                                                                                                                    | 9 de abril de 2015    |
|                                                              | Esta versión permite buscar actividades de AWS que CloudTrail (eventos de CloudTrail) haya detectado. Puede buscar y filtrar eventos en su cuenta relacionados con actividades de creación, modificación o eliminación. Para buscar estos eventos, puede utilizar la consola de CloudTrail, la AWS Command Line Interface, (AWS CLI) o el SDK de AWS. Para obtener más información, consulte <a href="#">Trabajar con el historial de eventos de CloudTrail</a> . | 12 de marzo de 2015   |
| Se agregó compatibilidad con servicios y documentación nueva | Esta versión es compatible con Registros de Amazon CloudWatch en las regiones Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio) y Europa (Fráncfort). Para obtener más información, consulte <a href="#">Envío de eventos a Registros de CloudWatch</a> .                                                                                                                                                                                   | 5 de marzo de 2015    |
| Nueva documentación                                          | En la página <a href="#">Conceptos de CloudTrail</a> se agregó una nueva sección que describe la compatibilidad de CloudTrail con los puntos de enlace regionales de AWS Security Token Service (AWS STS).                                                                                                                                                                                                                                                        | 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 <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                   | 11 de febrero de 2015   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Config. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                   | 10 de febrero de 2015   |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS CloudHSM. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                 | 8 de enero de 2015      |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS CodeDeploy. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                               | 17 de diciembre de 2014 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Storage Gateway. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                          | 16 de diciembre de 2014 |
| Se añadió compatibilidad con regiones       | Esta versión es compatible con una región más: us-gov-west-1 (AWS GovCloud [Oeste de EE. UU.]). Consulte <a href="#">Regiones compatibles con CloudTrail</a> . | 16 de diciembre de 2014 |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Glacier. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                    | 11 de diciembre de 2014 |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Data Pipeline. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                            | 2 de diciembre de 2014  |
| Se agregó compatibilidad para los servicios | Esta versión admite AWS Key Management Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                   | 12 de noviembre de 2014 |

| Cambio                                      | Descripción                                                                                                                                                                                                                                                          | Fecha de lanzamiento     |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Nueva documentación                         | Se agregó la sección nueva, <a href="#">Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs</a> , a la guía. Describe cómo utilizar Amazon CloudWatch Logs para monitorear los eventos de registro de CloudTrail.                            | 10 de noviembre de 2014  |
| Nueva documentación                         | Se agregó la sección nueva <a href="#">Uso de la biblioteca de procesamiento de CloudTrail</a> a la guía. Proporciona información sobre cómo escribir un procesador de registros de CloudTrail en Java a través de la biblioteca de procesamiento de AWS CloudTrail. | 5 de noviembre de 2014   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Elastic Transcoder. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                               | 27 de octubre de 2014    |
| Se añadió compatibilidad con regiones       | Esta versión es compatible con una región más: eu-central-1 (Europa [Fráncfort]). Consulte <a href="#">Regiones compatibles con CloudTrail</a> .                                                                                                                     | 23 de octubre de 2014    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon CloudSearch. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                      | 16 de octubre de 2014    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Simple Notification Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                      | 09 de octubre de 2014    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon ElastiCache. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                      | 15 de septiembre de 2014 |

| Cambio                                      | Descripción                                                                                                                                                                                                                                        | Fecha de lanzamiento |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon WorkDocs. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                       | 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 <a href="#">Consola de administración de AWSEventos de inicio de sesión en la</a> .                                                              | 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 <a href="#">CloudTrail registra el contenido de los eventos de administración, de datos y de actividad de la red</a> . | 18 de julio de 2014  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Auto Scaling (consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> ).                                                                                                                         | 17 de julio de 2014  |
| Se añadió compatibilidad con regiones       | 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 <a href="#">Regiones compatibles con CloudTrail</a> .      | 30 de junio de 2014  |
| Compatibilidad adicional con servicio       | Esta versión es compatible con Amazon Redshift. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                       | 10 de junio de 2014  |
| Se agregó compatibilidad para los servicios | Esta versión admite OpsWorks. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                                         | 5 de junio de 2014   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon CloudFront. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                     | 28 de mayo de 2014   |



| Cambio                                      | Descripción                                                                                                                                                                                                                                 | Fecha de lanzamiento |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Se añadió compatibilidad con regiones       | 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 <a href="#">Regiones compatibles con CloudTrail</a> . | 13 de mayo de 2014   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Simple Workflow Service. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                 | 9 de mayo de 2014    |
| Se agregó contenido nuevo                   | Esta versión incluye temas sobre el uso compartido de archivos de registro entre cuentas. Consulte <a href="#">Compartir archivos de registro de CloudTrail entre cuentas de AWS</a> .                                                      | 2 de mayo de 2014    |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon CloudWatch. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                              | 28 de abril de 2014  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon Kinesis. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                 | 22 de abril de 2014  |
| Se agregó compatibilidad para los servicios | Esta versión admite Direct Connect. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                            | 11 de abril de 2014  |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Amazon EMR. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                                     | 4 de abril de 2014   |
| Se agregó compatibilidad para los servicios | Esta versión es compatible con Elastic Beanstalk. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> .                                                                                                              | 2 de abril de 2014   |

| Cambio                                | Descripción                                                                                                      | Fecha de lanzamiento    |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------|-------------------------|
| Compatibilidad adicional con servicio | Esta versión admite CloudFormation. Consulte <a href="#">Integraciones y servicios admitidos de CloudTrail</a> . | 7 de marzo de 2014      |
| Nueva guía                            | Esta versión introduce AWS CloudTrail.                                                                           | 13 de noviembre de 2013 |