aws

Guía del usuario de

Amazon Security Lake



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Security Lake: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es Amazon Security Lake? 1
Información general de Security Lake 2
Características de Security Lake 2
Acceder a Security Lake 4
Servicios relacionados 4
Conceptos y terminología 6
Introducción 8
Inscríbase en una Cuenta de AWS 8
Configurando su Cuenta de AWS 8
Identifique la cuenta que usará para habilitar Security Lake 9
Consideraciones a la hora de habilitar Security Lake 9
Uso de la consola 10
Paso 1: Configurar las fuentes 10
Paso 2: Defina la configuración de almacenamiento y acumule las regiones (opcional) 12
Paso 3: Revisar y crear un lago de datos 13
Paso 4: Vea y consulte sus propios datos 13
Paso 5: Crear suscriptores 14
Uso de la API AWS CLI o 14
Paso 1: Crear funciones de IAM 14
Paso 2: Habilitar Amazon Security Lake 15
Paso 3: Configurar las fuentes 16
Paso 4: Configurar los ajustes de almacenamiento y agrupar las regiones (opcional) 17
Paso 5: Vea y consulte sus propios datos 18
Paso 6: Crear suscriptores 19
Administración de varias cuentas 20
Consideraciones importantes para administradores de Security Lake delegados 21
Permisos de IAM necesarios para designar un administrador delegado 22
Designar al administrador delegado de Security Lake y añadir cuentas de miembros 23
Editar la configuración de la nueva cuenta en la consola 25
Eliminación al administrador delegado de Security Lake 26
Acceso de confianza de Security Lake 27
Administración de regiones de 29
Comprobación del estado de la región 29
Cambiar la configuración de la región 30

Configuración de regiones acumulativas ... 32
Rol de IAM para la replicación de datos ... 33
Función de IAM que se debe registrar AWS Glue particiones ... 36
Añadir regiones acumulativas ... 37
Actualizar o eliminar regiones acumulativas ... 38
Administración de fuentes ... 40
Recopilación de datos de Servicios de AWS ... 40
Prerrequisito: verificar permisos ... 41
Agregar una Servicio de AWS como fuente ... 42
Obtener el estado de la recopilación de fuentes ... 44
Actualización de los permisos de los roles ... 45
Eliminar un Servicio de AWS como fuente ... 47
CloudTrail registros de eventos ... 48
Registros de auditoría de Amazon EKS ... 50
Registros de consultas de Route 53 Resolver ... 50
Resultados del CSPM de Security Hub ... 51
Logs de flujo de VPC ... 52
AWS WAF registros ... 52
Eliminar un Servicio de AWS como fuente ... 47
Recopilación de datos de orígenes personalizados ... 54
Requisitos de partición para la ingesta de fuentes personalizadas ... 56
Requisitos previos para añadir un origen personalizado ... 57
Adición de un origen personalizado ... 61
Eliminación de un origen personalizado ... 65
Gestión de suscriptores ... 67
Acceso a los datos de los suscriptores ... 68
Requisitos previos ... 68
Crear un suscriptor con acceso a datos ... 72
Actualización de un suscriptor de datos ... 76
Eliminar un suscriptor de datos ... 77
Acceso a consultas de suscriptores ... 78
Requisitos previos ... 78
Crear un suscriptor con acceso a las consultas ... 81
Edición de un suscriptor con acceso a consultas ... 84
Consultas de Security Lake ... 89
Security Lake consulta la fuente, versión 1 ... 89

Tabla de orígenes de registro 90
Región de base de datos 91
Fecha de partición 92
Consultas de CloudTrail datos 94
Consultas para los registros de consultas de los solucionadores de Route 53 96
Consultas sobre los hallazgos del CSPM de Security Hub 98
Consultas de registros de flujo de Amazon VPC 101
Security Lake consulta la versión 2 de la fuente 105
Tabla de orígenes de registro 90
Región de base de datos 91
Fecha de partición 92
Consultando los observables de Security Lake 109
Consultas de CloudTrail datos 110
Consultas para los registros de consultas del solucionador de Route 53 112
Consultas sobre los hallazgos del CSPM de Security Hub 114
Consultas de registros de flujo de Amazon VPC 117
Consultas para los registros de auditoría de Amazon EKS 120
Consultas para registros de la AWS WAF versión 2 121
Administración del ciclo de vida 125
Administración de retención 125
Consideraciones importantes sobre la configuración de retención en Security Lake 125
Configurar los ajustes de retención al activar Security Lake 126
Actualización de la configuración de retención 127
Regiones acumulativas 129
Open Cybersecurity Schema Framework (OCSF) 130
¿Qué es OCSF? 130
Clases de eventos de OCSF 130
Identificación del origen de OCSF 130
Integraciones 134
Servicio de AWS integraciones 134
Integración de Amazon Bedrock 136
Integración con Amazon Detective 137
Integración OpenSearch de Amazon Service 137
Integración del proceso OpenSearch de ingestión de Amazon Service 138
Integración de consultas directas sin ETL de Amazon OpenSearch Service 138
Integración rápida 140

Integración de Amazon SageMaker AI 142
Integración de AWS AppFabric 143
AWS Security Hub CSPM integración 143
Third-party integraciones 145
Integración de consultas 146
Accenture – MxDR 146
Aqua Security 147
Barracuda – Protección de correo electrónico 147
Booz Allen Hamilton 147
Software y soluciones digitales de Bosch – AiShield 147
ChaosSearch 148
Seguridad de Cisco – Firewall seguro 148
Claridad – Cúpula 148
Soluciones CMD 148
Confluent – Conector de fregadero Amazon S3 149
Seguridad de contraste 149
Cribl – Search 149
Cribl – De streaming 149
CrowdStrike – Falcon Data Replicator 150
CrowdStrike – SIEM de próxima generación 150
CyberArk – Plataforma unificada de seguridad e identificación 150
Ciberseguridad en la nube – Cloud Fastener 150
DataBahn 150
Darktrace – Cyber AI Loop 151
Datadog 151
Deloitte – MXDR Cyber Analytics e IA Engine (CAE) 151
Devo 151
DXC – SecMon 152
Eviden – Isaac (anteriormente Atos) 152
ExtraHop – Reveal (x) 360 152
Falco, compinche 152
Fortinet: firewall nativo en la nube 153
Gigamon – Inteligencia de metadatos de aplicaciones 153
Hoop Cyber 153
HTCD – AI-First Plataforma de seguridad en la nube 153
IBM – QRadar 154

Infosys 154
Incorporado 154
Kyndryl – AIOps 154
Encajes – Polígrafo 155
Laminar 155
MegazoneCloud 155
Mónada 155
NETSCOUT – Ciberinteligencia de Omnis 156
Netskope – CloudExchange 156
New Relic ONE 156
Okta – Workforce Identity Cloud 156
Orca – Plataforma de seguridad en la nube 157
Palo Alto Networks – Prisma Cloud 157
Palo Alto Networks – VOLAR 157
Pantera 157
Ping Identity – PingOne 158
PwC – Centro de fusión 158
Query.AI – Consulta la búsqueda federada 158
Rapid7 – InsightIDR 158
RipJar – Laberinto para la investigación de amenazas 159
Sailpoint 159
Securonix 159
SentinelOne 159
Sentra – Plataforma de seguridad del ciclo de vida de los datos 160
SOC Prime 160
Splunk 160
Stellar Cyber 160
Sumo Logic 161
Swimlane – Turbina 161
Sysdig Secure 161
Garra 161
Tanium 162
TCS 162
Tego Cyber 162
Tines – No-code automatización de la seguridad 162
Torq – Plataforma de automatización de seguridad empresarial 163

Trellix – XDR 163
Trend Micro – CloudOne 163
Uptycs – Uptycs XDR 164
Vectra AI – Vectra Detect para AWS 164
VMware Aria Automation para nubes seguras 164
Wazuh 164
Wipro 165
Wiz – CNAPP 165
Zscaler – Control de postura de Zscaler 165
Seguridad 166
Identity and Access Management 167
Público 167
Autenticación con identidades 167
Administración del acceso con políticas 169
Cómo funciona Security Lake con IAM 171
Ejemplos de políticas basadas en identidades 179
AWS políticas administradas 184
Cómo utilizar roles vinculados a servicios 193
Protección de datos 203
Cifrado en reposo 204
Cifrado en tránsito 207
Desactivación del uso de los datos para mejorar el servicio 207
Validación de conformidad 208
Prácticas recomendadas de seguridad para Security Lake 208
Otorgar los permisos mínimos posibles a los usuarios de Security Lake 208
Ver la página de resumen de Resumen 209
Intégrelo con Security Hub (CSPM). 209
Eliminar AWS Lambda 209
Supervisión de los eventos de Security Lake 209
Resiliencia 209
Seguridad de la infraestructura 211
Configuración y análisis de vulnerabilidades en Security Lake 211
Puntos de conexión de VPC (AWS PrivateLink) 211
Consideraciones sobre los puntos finales de VPC de Security Lake 212
Creación de un punto final de VPC de interfaz para Security Lake 212
Creación de una política de puntos finales de VPC para Security Lake 213

Subredes compartidas 213
Monitorización 214
CloudWatch métricas de Amazon Security Lake 214
Registro de llamadas a la API 217
Información sobre Security Lake en CloudTrail 217
Descripción de las entradas de los archivos de registro de Security Lake 218
Etiquetado de recursos 220
Conceptos básicos del etiquetado 220
Uso de etiquetas en políticas de IAM 222
Adición de etiquetas a recursos 223
Edición de etiquetas para recursos 226
Revisión de etiquetas para recursos 228
Eliminación de etiquetas de recursos 230
Resolución de problemas 233
Solución de problemas del estado del lago de datos 233
Solución de problemas de Lake Formation 234
Tabla no encontrada 234
400 AccessDenied 235
SYNTAX_ERROR 235
No se pudo agregar el ARN principal de la persona que llamó a Lake Formation 235
CreateSubscriber with Lake Formation no creó una nueva invitación para compartir recursos de RAM 236
Solución de problemas de consultas en Amazon Athena 236
Las consultas no devuelven nuevos objetos al lago de datos 236
No se puede acceder a AWS Glue las tablas 237
Solución de problemas de Organizations 237
Error de acceso denegado 238
Solución de problemas de IAM 238
No tengo autorización para realizar una acción en Security Lake 238
Quiero ampliar los permisos más allá de la política gestionada 239
No estoy autorizado a realizar el iam: PassRole 239
Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Security Lake 239
Precios de Security Lake 241
Revisar el uso de los costos estimados 243
Regiones y puntos de conexión compatibles 245

Desactivación de Security Lake 246
Historial de revisión 249
..... cclvii

¿Qué es Amazon Security Lake?

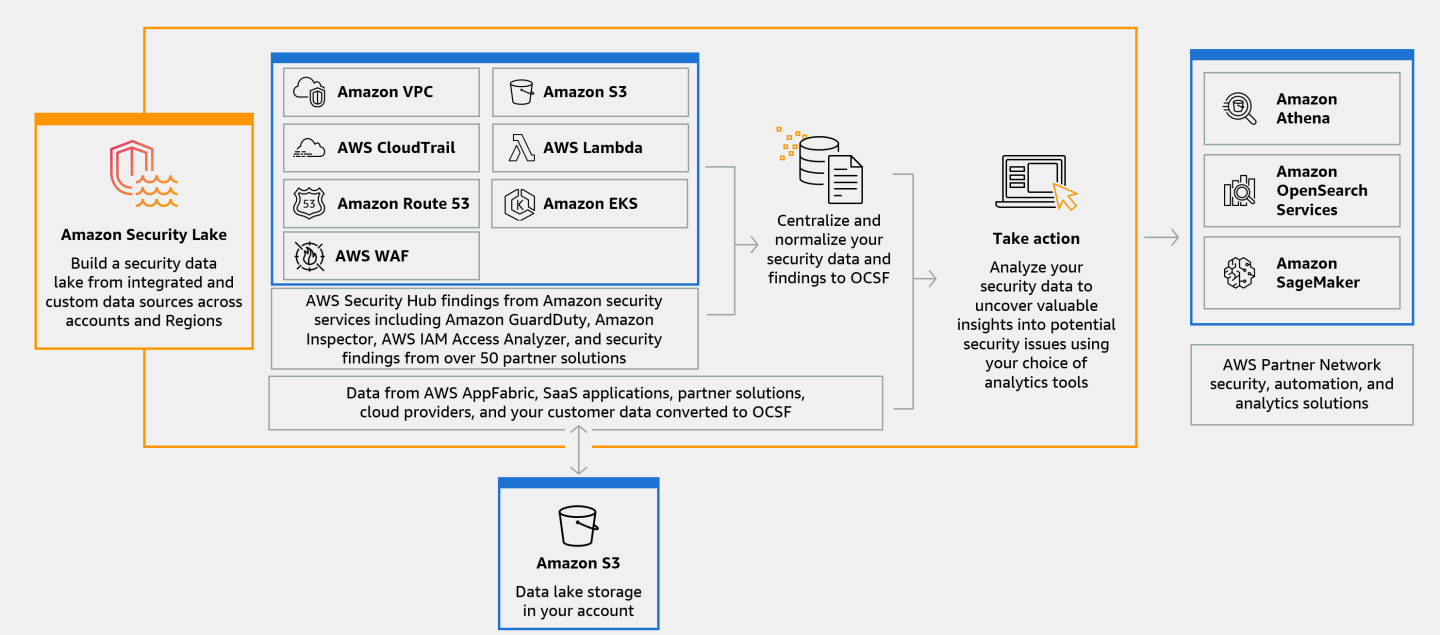
Amazon Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Security Lake para centralizar automáticamente los datos de seguridad de los AWS entornos, los proveedores de SaaS, las fuentes locales, en la nube y las fuentes de terceros en un lago de datos diseñado específicamente que se almacena en su. Cuenta de AWS Security Lake le ayuda a analizar los datos de seguridad para que pueda comprender mejor su postura de seguridad en toda la organización. Con Security Lake, también puede mejorar la protección de sus cargas de trabajo, aplicaciones y datos.

El lago de datos está respaldado por buckets de Amazon Simple Storage Service (Amazon S3) y usted retiene la propiedad de sus datos.

Security Lake automatiza la recopilación de datos de registros y eventos relacionados con la seguridad procedentes de Servicios de AWS integrados y de servicios de terceros. También le ayuda a gestionar el ciclo de vida de los datos con configuraciones de retención y replicación personalizables. Security Lake convierte los datos ingeridos al formato Apache Parquet y a un esquema estándar de código abierto denominado Open Cybersecurity Schema Framework (OCSF). Gracias a la compatibilidad con OCSF, Security Lake normaliza y combina los datos de seguridad de una amplia gama de AWS fuentes de datos de seguridad empresarial.

Otros Servicios de AWS servicios, incluidos los de terceros, pueden suscribirse a los datos almacenados en Security Lake para responder a los incidentes y analizar los datos de seguridad.

Información general de Security Lake



Características de Security Lake

Estas son algunas de las principales formas en las que Security Lake le ayuda a centralizar, administrar y suscribirse a los datos de registros y eventos relacionados con la seguridad.

Agregación de datos a su cuenta

Security Lake crea un lago de datos de seguridad especialmente diseñado en su cuenta. Security Lake recopila datos de registros y eventos de orígenes de datos en la nube, en las instalaciones y personalizadas de todas las cuentas y regiones. El lago de datos está respaldado por buckets de Amazon Simple Storage Service (Amazon S3) y usted retiene la propiedad de sus datos.

Variedad de orígenes de registros y eventos compatibles

Security Lake recopila registros y eventos de seguridad de varias fuentes, incluidos los servicios locales y de terceros. Servicios de AWS Tras ingerir los registros, independientemente del origen, puede acceder a ellos de forma centralizada y gestionar su ciclo de vida. Para obtener información detallada sobre los orígenes desde los que Security Lake recopila los registros y eventos, consulte Administración de fuentes en Security Lake

Transformación y normalización de datos

Security Lake divide automáticamente los datos entrantes de los Servicios de AWS compatibles de forma nativa y los convierte a un formato Parquet eficiente en términos de almacenamiento y consulta. También transforma los datos admitidos Servicios de AWS de forma nativa en el esquema de código abierto del Open Cybersecurity Schema Framework (OCSF). Esto hace que los datos sean compatibles con otros proveedores Servicios de AWS y con proveedores externos sin necesidad de un procesamiento posterior. Dado que Security Lake normaliza los datos, muchas soluciones de seguridad pueden consumir estos datos en paralelo.

Múltiples niveles de acceso para los suscriptores

Los suscriptores consumen los datos almacenados en Security Lake. Puede elegir el nivel de acceso de un suscriptor a sus datos. Los suscriptores solo pueden consumir datos de los orígenes y en las Regiones de AWS que especifique. Los suscriptores pueden recibir notificaciones automáticas sobre nuevos objetos a medida que se escriben en el lago de datos. O bien, los suscriptores pueden consultar los datos del lago de datos. Security Lake crea e intercambia automáticamente las credenciales necesarias entre Security Lake y el suscriptor.

Multi-account y gestión de datos multirregional

Puede activar Security Lake de forma centralizada en todas las regiones en las que esté disponible y en varias Cuentas de AWS. En Security Lake, también puede designar regiones acumulables para consolidar los registros de seguridad y los datos de eventos de varias regiones. Esto puede ayudarle a cumplir con los requisitos de conformidad con la residencia de datos.

Configurable y personalizable

Security Lake es un servicio configurable y personalizable. Puede especificar las fuentes, cuentas y regiones para las que desea configurar la recopilación de registros. También puede especificar el nivel de acceso del suscriptor al lago de datos.

Gestión y optimización del ciclo de vida de los datos

Security Lake gestiona el ciclo de vida de sus datos con configuraciones de retención personalizables y los costos de almacenamiento con una organización automática del almacenamiento en niveles. Security Lake divide y convierte automáticamente los datos de seguridad entrantes a un formato Apache Parquet eficiente en términos de almacenamiento y consulta.

Acceder a Security Lake

Para obtener una lista de las regiones en las que Security Lake está disponible actualmente, consulte Regiones y puntos finales de Security Lake. Para obtener más información sobre las regiones, consulte los puntos de conexión de servicio de AWS en Referencia general de AWS.

En cada región, puede acceder a Security Lake de cualquiera de las siguientes formas:

Consola de administración de AWS

Consola de administración de AWS Es una interfaz basada en navegador que puede usar para crear y administrar recursos. AWS La consola de Security Lake proporciona acceso a su cuenta y sus recursos de Security Lake. Puede realizar la mayoría de las tareas de Security Lake mediante la consola de Security Lake.

API de Security Lake

Para acceder a Security Lake de manera programática, utilice la API de Security Lake y emita solicitudes HTTPS directamente al servicio. Para obtener más información, consulte la Referencia de la API de Security Lake.

AWS Command Line Interface (AWS CLI)

Con ella AWS CLI, puede emitir comandos en la línea de comandos del sistema para realizar las tareas y AWS tareas de Security Lake. Usar la línea de comandos puede ser más rápido y práctico que usar la consola. Las herramientas de línea de comandos también son útiles si desea crear scripts que realicen tareas. Para obtener información sobre la instalación y el uso del AWS CLI, consulte el AWS Command Line Interface.

AWS SDKs

AWS proporciona SDK que constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas, como Java, Go, Python, C++ y.NET. Los SDK proporcionan un acceso práctico y programático a Security Lake y a otros sitios. Servicios de AWS También permiten realizar tareas como firmar solicitudes criptográficamente, administrar errores y reintentar solicitudes automáticamente. Para obtener información sobre la instalación y el uso de los AWS SDK, consulte Herramientas sobre las que construir. AWS

Servicios relacionados

Las siguientes son otras de las Servicios de AWS que usa Security Lake:

- Amazon EventBridge: Security Lake lo utiliza EventBridge para notificar a los suscriptores cuando se escriben objetos en el lago de datos.
- AWS Glue— Security Lake utiliza AWS Glue rastreadores para crear las AWS Glue Data Catalog tablas y enviar los datos recién escritos al catálogo de datos. Security Lake también almacena los metadatos de las particiones para AWS Lake Formation las tablas del catálogo de datos.
- AWS Lake Formation: Security Lake crea una tabla de Lake Formation independiente para cada origen que aporta datos a Security Lake. Las tablas de Lake Formation contienen información sobre los datos de cada origen, incluida la información sobre el esquema, la partición y la ubicación de los datos. Los suscriptores tienen la opción de consumir datos consultando las tablas de Lake Formation.
- AWS Lambda: Security Lake utiliza las funciones de Lambda para admitir trabajos de extracción, transformación y carga (ETL) en datos sin procesar y para registrar particiones para los datos de origen AWS Glue.
- Amazon S3: Security Lake almacena sus datos como objetos de Amazon S3. Las clases de almacenamiento y la configuración de retención se basan en las ofertas de Amazon S3. Security Lake no es compatible con Amazon S3 Select.
- Amazon Simple Queue Service: Security Lake usa Amazon SQS para permitir el procesamiento basado en eventos y administrar las notificaciones.

Security Lake recopila datos de fuentes personalizadas, además de lo siguiente: Servicios de AWS

- AWS CloudTrail eventos de administración y datos (S3, Lambda)
- Registros de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS)
- Registros de consultas de Amazon Route 53 Resolver
- AWS Security Hub CSPM hallazgos
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF Registros v2

Para obtener más información acerca de estos orígenes, consulte Recopilación de datos de Servicios de AWS en Security Lake. Puede consumir los objetos de Amazon S3 de su lago de datos de seguridad creando un suscriptor que pueda leer los datos del esquema OCSF. También puede consultar datos mediante Amazon Athena, Amazon Redshift y los servicios de suscripción de terceros que se integran con. AWS Glue

Conceptos y terminología

En esta sección se describen los conceptos y términos clave que le ayudarán a utilizar Amazon Security Lake.

Región contribuyente

Una o más Regiones de AWS que aportan datos a una región acumulada.

Lago de datos

Sus datos persistentes almacenados en Amazon Simple Storage Service (Amazon S3) y gestionados por Security Lake. Security Lake utiliza AWS Glue para enviar los datos recién escritos al catálogo de datos. Security Lake también crea una AWS Lake Formation tabla para cada fuente que aporta datos al lago de datos. En general, un lago de datos almacena lo siguiente:

- Datos estructurados y no estructurados
- Datos sin procesar y datos transformados

Security Lake es un servicio de lago de datos diseñado para recopilar registros y eventos relacionados con la seguridad.

Open Cybersecurity Schema Framework (OCSF)

Un esquema de código abierto estandarizado para registros y eventos de seguridad. Fue desarrollado por otros líderes AWS de la industria de la seguridad en varios dominios de seguridad. Security Lake convierte automáticamente los registros y eventos que recopila Servicios de AWS en el esquema OCSF. Las fuentes personalizadas convierten sus registros y eventos en OCSF antes de enviarlos a Security Lake.

Región acumulativa

Y Región de AWS eso consolida los registros de seguridad y los eventos de una o más regiones contribuyentes. Especificar una o más regiones acumulativas puede ayudarle a cumplir con los requisitos de conformidad regionales.

Origen

Un conjunto de registros y eventos generados a partir de un único sistema que coincide con una clase de evento específica de OCSF. Security Lake puede recopilar datos de un origen. Un origen

puede ser otro Servicio de AWS o un servicio de terceros. En el caso de las fuentes de terceros, debe convertir los datos al esquema OCSF antes de enviarlos a Security Lake.

Suscriptor

Un servicio que consume registros y eventos de Security Lake. Un suscriptor puede ser un servicio Servicio de AWS ajeno o un tercero.

Introducción a Amazon Security Lake

En los temas de esta sección se explica cómo habilitar y empezar a usar Security Lake. Aprenderá a configurar los ajustes de su lago de datos y a configurar la recopilación de registros. Puede habilitar y usar Security Lake a través de Consola de administración de AWS o mediante programación. Sea cual sea el método que utilice, primero debe configurar un usuario administrativo Cuenta de AWS y uno. Los pasos siguientes varían según el método de acceso.

La consola de Security Lake ofrece un proceso simplificado para empezar y crea todas las funciones AWS Identity and Access Management (IAM) necesarias para crear su lago de datos.

Si accede a Security Lake mediante programación, es necesario crear algunas funciones AWS Identity and Access Management (de IAM) para configurar su lago de datos.

> **Important**
>
> Security Lake no admite la reposición de eventos de fuentes de registro AWS sin procesar existentes que se generaron antes de habilitar Security Lake.

Temas

- Inscríbase en una Cuenta de AWS
- Configurando su Cuenta de AWS
- Consideraciones a la hora de habilitar Security Lake
- Habilitar Security Lake mediante la consola
- Habilitar Security Lake mediante programación

Inscríbase en una Cuenta de AWS

Para empezar AWS, necesitas un Cuenta de AWS. Para obtener información sobre cómo crear un Cuenta de AWS, consulte Cómo empezar con un Cuenta de AWS en la Guía de AWS Account Management referencia.

Configurando su Cuenta de AWS

Antes de poder activar Amazon Security Lake, debe tener una Cuenta de AWS.

Identifique la cuenta que usará para habilitar Security Lake

Security Lake se integra AWS Organizations para administrar la recopilación de registros en varias cuentas de una organización. Si desea usar Security Lake para una organización, debe usar su cuenta de administración de Organizations para designar un administrador delegado de Security Lake. Luego, debe usar las credenciales del administrador delegado para habilitar Security Lake, agregar cuentas de miembros y habilitar Security Lake para ellos. Para obtener más información, consulte Administrar varias cuentas con AWS Organizations en Security Lake.

Como alternativa, puede usar Security Lake sin la integración de Organizations para una cuenta independiente que no forme parte de una organización.

Consideraciones a la hora de habilitar Security Lake

Antes de habilitar Security Lake, tenga en cuenta lo siguiente:

- Security Lake proporciona características de administración entre regiones, lo que significa que puede crear su lago de datos y configurar la recopilación de registros entre Regiones de AWS. Para habilitar Security Lake en todas las regiones compatibles, puede elegir cualquier punto de conexión regional compatible. También puede añadir regiones acumulativas para agregar datos de varias regiones a una sola región.
- Recomendamos activar Security Lake en todas las Regiones de AWS compatibles. Si lo hace, Security Lake puede recopilar datos relacionados con actividades no autorizadas o inusuales, incluso en las regiones que no utiliza activamente. Si Security Lake no está activado en todas las regiones compatibles, se reduce su capacidad de recopilar datos de otros servicios que se utilizan en varias regiones.
- Al activar Security Lake por primera vez en una región, se crean las siguientes funciones vinculadas al servicio para su cuenta:
  - AWSServiceRoleForSecurityLake: Esta función incluye los permisos para llamar a otras personas Servicios de AWS en tu nombre y gestionar el lago de datos de seguridad. Si habilita Security Lake como administrador delegado de Security Lake, Security Lake crea el rol vinculado a servicios en cada cuenta de miembro de la organización.
  - AWSServiceRoleForSecurityLakeResourceManagement: Security Lake utiliza esta función para realizar una supervisión continua y mejorar el rendimiento, lo que puede reducir la latencia y los costes. Este rol vinculado a servicios confía en el servicio `resource-management.securitylake.amazonaws.com` para asumir el rol. Habilitar esta función de servicio también le otorgará acceso a Lake Formation.

Para obtener información sobre cómo afecta esto a las cuentas existentes que habilitaban Security Lake antes del 17 de abril de 2025, consulteUpdate for existing accounts.

Para obtener información sobre cómo funcionan las funciones vinculadas a servicios, consulte Uso de permisos de funciones vinculadas a servicios en la Guía del usuario de IAM.

- Security Lake no admite el bloqueo de objetos de Amazon S3. Cuando se crean los buckets del lago de datos, el bloqueo de objetos de S3 está desactivado de forma predeterminada. Al habilitar el bloqueo de objetos en un bucket, se interrumpe la entrega de datos de registro normalizados al lago de datos.
- Si va a volver a habilitar Security Lake en una región, debe eliminar la AWS Glue base de datos correspondiente a la región del uso anterior de Security Lake.

Habilitar Security Lake mediante la consola

En este tutorial se explica cómo habilitar y configurar Security Lake a través del Consola de administración de AWS. Como parte de ello Consola de administración de AWS, la consola de Security Lake ofrece un proceso simplificado para empezar y crea todas las funciones AWS Identity and Access Management (IAM) necesarias para crear su lago de datos.

Paso 1: Configurar las fuentes

Security Lake recopila datos de registros y eventos de diversos orígenes y de todas las Cuentas de AWS y Regiones de AWS. Siga estas instrucciones para identificar qué datos desea que Security Lake recopile. Solo puede usar estas instrucciones para agregar un Servicio de AWS compatible de forma nativa como origen. Para obtener información acerca de cómo agregar un origen personalizado, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Para configurar la recopilación de fuentes de registro

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione una región. Puede activar Security Lake en la región actual y en otras regiones durante la incorporación.
3. Elija Comenzar.
4. En Seleccionar fuentes de registros y eventos, elija una de las siguientes opciones para la selección de fuentes:

a. Ingesta AWS las fuentes predeterminadas: si eliges la opción recomendada, CloudTrail los eventos de datos de S3 no AWS WAF se incluyen para la ingesta de forma predeterminada. Esto se debe a que la ingesta de un gran volumen de ambos tipos de fuentes podría afectar significativamente a los costos de uso. Para ingerir estas fuentes, primero seleccione la opción Ingerir AWS fuentes específicas y, a continuación, seleccione estas fuentes de la lista de fuentes de registros y eventos.

b. Ingesta AWS fuentes específicas: con esta opción, puede seleccionar una o más fuentes de registros y eventos que desee ingerir.

> **Note**
>
> Al habilitar Security Lake en una cuenta por primera vez, todos los orígenes de registros y eventos seleccionados formarán parte de un periodo de prueba gratuito de 15 días. Para obtener más información sobre las estadísticas de uso, consulte Revisar el uso de los costos estimados.

5. En Versiones, elija la versión de la fuente de datos desde la que desee ingerir las fuentes de registros y eventos. Para obtener más información acerca de las versiones, consulte Identificación del origen de OCSF.

> **Important**
>
> Si no tiene los permisos de rol necesarios para habilitar la nueva versión de la fuente de AWS registro en la región especificada, póngase en contacto con el administrador de Security Lake. Para obtener más información, consulte Actualizar los permisos de los roles.

6. En Seleccionar regiones, elija si desea ingerir los orígenes de registros y eventos de todas las regiones compatibles o de regiones específicas. Si elige Regiones específicas, seleccione las regiones de las que deseas ingerir los datos.
7. Para seleccionar cuentas, lleve a cabo los siguientes pasos:

   1. Elija si Security Lake ingerirá datos de todas las cuentas o de cuentas específicas de su organización. Security Lake se habilitará para estas cuentas con los ajustes que elija durante esta configuración.

2. La casilla Habilitar automáticamente Security Lake para las nuevas cuentas de la organización está seleccionada de forma predeterminada. Esta configuración de activación automática se aplicará Cuentas de AWS cuando se unan a tu organización. Puede editar la configuración de activación automática en cualquier momento.

> **Note**
>
> La configuración de activación automática solo se aplicará a las cuentas cuando se unan a tu organización, no a las cuentas existentes. Para obtener más información, consulte Editar la configuración de la nueva cuenta en la consola.

8. Para Acceso al servicio, cree un nuevo rol de IAM o utilice un rol de IAM existente que dé permiso a Security Lake para recopilar datos de sus fuentes y añadirlos a su lago de datos. Un rol se utiliza en todas las regiones en las que se habilita Security Lake.
9. Elija Siguiente.

Paso 2: Defina la configuración de almacenamiento y acumule las regiones (opcional)

Puede especificar la clase de almacenamiento de Amazon S3 en la que desea que Security Lake almacene los datos y durante cuánto tiempo. También puede especificar una región acumulativa para consolidar los datos de varias regiones. Estos son pasos opcionales. Para obtener más información, consulte Administración del ciclo de vida en Security Lake.

Para configurar los ajustes de almacenamiento y acumulación

1. Si desea consolidar los datos de varias regiones contribuyentes en una región acumulativa, en Seleccionar regiones de acumulación, elija Agregar región de acumulación. Especifique la región acumulativa y las regiones que contribuirán a ella. Puede configurar una o más regiones acumulativas.
2. En Seleccionar clases de almacenamiento, elija una de Amazon S3. La clase de almacenamiento predeterminada es S3 Standard. Indique un período de retención (en días) si desea que los datos pasen a otra clase de almacenamiento después de ese tiempo y seleccione Añadir transición. Una vez finalizado el período de retención, los objetos caducan y Amazon

S3 los elimina. Para obtener más información acerca de las clases de almacenamiento y la retención de Amazon S3, consulte Administración de retención.

3. Si seleccionó una región acumulativa en el primer paso, para Acceso al servicio, cree un nuevo rol de IAM o utilice un rol de IAM existente que dé permiso a Security Lake para replicar datos en varias regiones.
4. Elija Siguiente.

Paso 3: Revisar y crear un lago de datos

Revise los orígenes de los que Security Lake recopilará datos, sus regiones acumulativas y su configuración de retención. A continuación, cree su lago de datos.

Para revisar y crear el lago de datos

1. Al habilitar Security Lake, revise Orígenes de registros y eventos, Regiones, Regiones acumulativas y Clases de almacenamiento.
2. Seleccione Crear.

Tras crear el lago de datos, verá la página Resumen en la consola de Security Lake. En esta página se ofrece un resumen del número de regiones y regiones acumulativas, información sobre los suscriptores y los problemas.

El menú Problemas muestra un resumen de los problemas de los últimos 14 días que están afectando al servicio Security Lake o a sus buckets de Amazon S3. Para obtener más información sobre cada problema, puede ir a la página de problemas de la consola de Security Lake.

Paso 4: Vea y consulte sus propios datos

Tras crear el lago de datos, puede utilizar Amazon Athena o servicios similares para ver y consultar los datos de AWS Lake Formation bases de datos y tablas. Cuando utiliza la consola, Security Lake concede automáticamente permisos de visualización de la base de datos al rol que utilice para habilitar Security Lake. Como mínimo, el rol debe tener permisos de analista de datos. Para obtener más información sobre los niveles de permisos, consulte la referencia sobre los permisos de IAM y las personas de Lake Formation. Para obtener instrucciones sobre cómo conceder permisos SELECT, consulte Concesión de permisos de catálogo de datos mediante el método de recurso indicado en la Guía para desarrolladores de AWS Lake Formation .

Paso 5: Crear suscriptores

Después de crear su lago de datos, puede añadir suscriptores para consumir sus datos. Los suscriptores pueden consumir datos accediendo directamente a los objetos de sus buckets de Amazon S3 o consultando el lago de datos. Para obtener más información sobre los suscriptores, consulte Gestión de suscriptores en Security Lake.

Habilitar Security Lake mediante programación

En este tutorial se explica cómo habilitar y empezar a usar Security Lake mediante programación. La API de Amazon Security Lake le proporciona un acceso completo y programático a su cuenta, datos y recursos de Security Lake. Como alternativa, puede utilizar las herramientas de línea de AWS comandos (AWS Command Line Interfaceo las AWS Herramientas para PowerShell) o los AWS SDK para acceder a Security Lake.

Paso 1: Crear funciones de IAM

Si accede a Security Lake mediante programación, es necesario crear algunos roles AWS Identity and Access Management (de IAM) para configurar su lago de datos.

> **Important**
>
> No es necesario crear estas funciones de IAM si utiliza la consola de Security Lake para habilitar y configurar Security Lake.

Debe crear roles en IAM si va a realizar una o más de las siguientes acciones (elija los enlaces para ver más información sobre los roles de IAM para cada acción):

- Creación de un origen personalizado: los orígenes personalizados son orígenes distintos de los Servicios de AWS compatibles de forma nativa y que envían datos a Security Lake.
- Crear un suscriptor con acceso a los datos: los suscriptores con permisos pueden acceder directamente a los objetos de S3 desde su lago de datos.
- Crear un suscriptor con acceso a consultas: los suscriptores con permisos pueden consultar datos de Security Lake mediante servicios como Amazon Athena.
- Configuración de una región acumulativa: una región acumulativa consolida los datos de varias Regiones de AWS.

Tras crear los roles mencionados anteriormente, asocie la política AmazonSecurityLakeAdministrator AWS administrada al rol que está utilizando para habilitar Security Lake. Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Security Lake.

Adjunte la política AmazonSecurityLakeMetaStoreManager AWS administrada para crear su lago de datos o consulte los datos de Security Lake. Esta política es necesaria para que Security Lake admita tareas de extracción, transformación y carga (ETL) en datos sin procesar de registros y eventos que recibe de las fuentes.

Paso 2: Habilitar Amazon Security Lake

Para habilitar Security Lake mediante programación, utilice la CreateDataLakeoperación de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el comando create-data-lake. En su solicitud, utilice el campo `region` del objeto `configurations` para especificar el código de región de la región en la que se va a habilitar Security Lake. Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.

Ejemplo 1

El siguiente comando de ejemplo habilita Security Lake en las `us-east-1` regiones y. `us-east-2` En ambas regiones, este lago de datos está cifrado con claves administradas de Amazon S3. Los objetos caducan después de 365 días y los objetos pasan a la clase de almacenamiento `ONEZONE_IA` S3 después de 60 días. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}},
 {"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Ejemplo 2

El siguiente comando de ejemplo habilita Security Lake en la `us-east-2` región. Este lago de datos está cifrado con una clave gestionada por el cliente que se creó en AWS Key Management

Service (AWS KMS). Los objetos caducan después de 500 días y los objetos pasan a la clase de almacenamiento `GLACIER` S3 después de 30 días. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}}]' \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

> **Note**
>
> Si ya ha activado Security Lake y desea actualizar los ajustes de configuración de una región o fuente, utilice la UpdateDataLakeoperación o, si utiliza el comando AWS CLIupdate-data-lake. No utilice la operación. `CreateDataLake`

Paso 3: Configurar las fuentes

Security Lake recopila datos de registros y eventos de diversos orígenes y de todas las Cuentas de AWS y Regiones de AWS. Siga estas instrucciones para identificar qué datos desea que Security Lake recopile. Solo puede usar estas instrucciones para agregar un Servicio de AWS compatible de forma nativa como origen. Para obtener información acerca de cómo agregar un origen personalizado, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Para definir una o más fuentes de recopilación mediante programación, utilice la CreateAwsLogSourceoperación de la API de Security Lake. Para cada origen, especifique un valor regional único para el parámetro `sourceName`. Si lo desea, utilice parámetros adicionales para limitar el alcance del origen a cuentas específicas (`accounts`) o a una versión específica (`sourceVersion`).

> **Note**
>
> Si no incluye un parámetro opcional en la solicitud, Security Lake la aplicará a todas las cuentas o a todas las versiones del origen especificado, en función del parámetro que excluya. Por ejemplo, si es el administrador delegado de Security Lake de una organización y excluye el parámetro `accounts`, Security Lake aplicará su solicitud a todas las cuentas de

la organización. Del mismo modo, si excluye el parámetro `sourceVersion`, Security Lake aplicará su solicitud a todas las versiones del origen especificado.

Si su solicitud especifica una región en la que no ha activado Security Lake, se produce un error. Para solucionar este error, asegúrese de que la matriz `regions` especifique solo las regiones en las que ha activado Security Lake. Como alternativa, puede habilitar Security Lake en la región y después enviar la solicitud de nuevo.

Al habilitar Security Lake en una cuenta por primera vez, todos los orígenes de registros y eventos seleccionados formarán parte de un periodo de prueba gratuito de 15 días. Para obtener más información sobre las estadísticas de uso, consulte Revisar el uso de los costos estimados.

Paso 4: Configurar los ajustes de almacenamiento y agrupar las regiones (opcional)

Puede especificar la clase de almacenamiento de Amazon S3 en la que desea que Security Lake almacene los datos y durante cuánto tiempo. También puede especificar una región acumulativa para consolidar los datos de varias regiones. Estos son pasos opcionales. Para obtener más información, consulte Administración del ciclo de vida en Security Lake.

Para definir un objetivo objetivo mediante programación al habilitar Security Lake, utilice el CreateDataLakefuncionamiento de la API de Security Lake. Si ya ha activado Security Lake y quiere definir un objetivo objetivo, utilice la UpdateDataLakeoperación, no la `CreateDataLake` operación.

Para cualquiera de las dos operaciones, utilice los parámetros compatibles para especificar los ajustes de configuración que desee:

- Para especificar una región acumulada, utilice el `region` campo para especificar la región en la que desea aportar datos a las regiones acumuladas. En la `regions` matriz del `replicationConfiguration` objeto, especifique el código de región de cada región acumulada. Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.
- Para especificar la configuración de retención de sus datos, utilice los parámetros `lifecycleConfiguration`:
  - Para `transitions`, especifique el número total de días (`days`) que desea almacenar los objetos de S3 en una clase de almacenamiento de Amazon S3 determinada (`storageClass`).

- Para `expiration`, especifique el número total de días que desea almacenar los objetos en Amazon S3, utilizando cualquier clase de almacenamiento, una vez creados los objetos. Una vez finalizado el período de retención, los objetos caducan y Amazon S3 los elimina.

Security Lake aplica la configuración de retención especificada a la región que especifique en el campo `region` del objeto `configurations`.

Por ejemplo, el siguiente comando crea un lago de datos con una `ap-northeast-2` región acumulativa. La `us-east-1` región aportará datos a la `ap-northeast-2` región. En este ejemplo también se establece un período de caducidad de 10 días para los objetos que se agreguen al lago de datos.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":10}}}]' \
--meta-store-manager-role-arn "arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

Ya ha creado su lago de datos. Utilice el ListDataLakesfuncionamiento de la API de Security Lake para verificar la activación de Security Lake y la configuración de su lago de datos en cada región.

Si surgen problemas o errores al crear su lago de datos, puede ver una lista de excepciones mediante la ListDataLakeExceptionsoperación y notificar a los usuarios las excepciones mediante la CreateDataLakeExceptionSubscriptionoperación. Para obtener más información, consulte Solución de problemas del estado del lago de datos.

Paso 5: Vea y consulte sus propios datos

Tras crear el lago de datos, puede utilizar Amazon Athena o servicios similares para ver y consultar los datos de AWS Lake Formation bases de datos y tablas. Al activar Security Lake mediante programación, los permisos de visualización de la base de datos no se conceden automáticamente. La cuenta de administrador del lago de datos AWS Lake Formation debe conceder `SELECT` permisos a la función de IAM que desee utilizar para consultar las bases de datos y tablas pertinentes. Como mínimo, el rol debe tener permisos de analista de datos. Para obtener más información sobre los niveles de permisos, consulte la referencia sobre los permisos de IAM y las personas de Lake Formation. Para obtener instrucciones sobre cómo conceder permisos `SELECT`, consulte

Concesión de permisos de catálogo de datos mediante el método de recurso indicado en la Guía para desarrolladores de AWS Lake Formation .

Paso 6: Crear suscriptores

Después de crear su lago de datos, puede añadir suscriptores para consumir sus datos. Los suscriptores pueden consumir datos accediendo directamente a los objetos de sus buckets de Amazon S3 o consultando el lago de datos. Para obtener más información sobre los suscriptores, consulte Gestión de suscriptores en Security Lake.

Administrar varias cuentas con AWS Organizations en Security Lake

Puede usar Amazon Security Lake para recopilar registros de seguridad y eventos de varias Cuentas de AWS. Para ayudar a automatizar y agilizar la administración de varias cuentas, le recomendamos encarecidamente que integre Security Lake con AWS Organizations.

La cuenta de administración es la cuenta que usa para crear la organización en Organizations. Si desea usar Security Lake con Organizations, la cuenta de administración debe designar una cuenta de administrador de Security Lake delegada para la organización.

El administrador de Security Lake delegado puede habilitar Security Lake y configurar los ajustes de Security Lake para las cuentas de los miembros. El administrador delegado puede recopilar registros y eventos de toda la organización en cualquier Regiones de AWS lugar en el que Security Lake esté habilitado (independientemente del punto final regional que esté utilizando actualmente). El administrador delegado también puede configurar Security Lake para que recopile automáticamente los datos de registro y eventos de las nuevas cuentas de la organización.

El administrador de Security Lake delegado tiene acceso a los datos de registros y eventos de las cuentas asociadas de los miembros. En consecuencia, puede configurar Security Lake para recopilar datos propiedad de las cuentas asociadas de los miembros. También puede conceder permiso a los suscriptores para que consuman los datos que pertenecen a las cuentas asociadas de los miembros.

Para habilitar Security Lake en varias cuentas de la organización, la cuenta de administración de la organización debe designar una cuenta de administrador de Security Lake delegada para la organización. A continuación, el administrador delegado puede habilitar y configurar Security Lake para la organización.

> **Important**
>
> Use la RegisterDataLakeDelegatedAdministrator API de Security Lake para permitir que Security Lake acceda a su organización y registre al administrador delegado de las organizaciones.
> Si utiliza las API de Organizations para registrar un administrador delegado, es posible que los roles vinculados a servicios de Organizations no se creen correctamente. Para garantizar una funcionalidad completa, utilice las API de Security Lake.

Para obtener información sobre la configuración de Organizations, consulte Creación y administración de una organización en la Guía del usuario de AWS Organizations .

> **Para las cuentas de Security Lake existentes**
>
> Si habilitó Security Lake antes del 17 de abril de 2025, le recomendamos que habilite elService-linked permisos de rol (SLR) para la administración de recursos. Al usar esta cámara réflex, puede seguir realizando mejoras continuas de monitoreo y rendimiento, lo que puede reducir la latencia y los costos. Para obtener información sobre los permisos asociados a esta cámara réflex, consulte. Service-linked permisos de rol (SLR) para la administración de recursos
> Si utiliza la consola Security Lake, recibirá una notificación en la que se le pedirá que habilite la. AWSServiceRoleForSecurityLakeResourceManagement Si la usa AWS CLI, consulte Creación de la función vinculada al servicio de Security Lake.

Consideraciones importantes para administradores de Security Lake delegados

Tenga en cuenta los siguientes factores que definen cómo se comporta un administrador delegado en Security Lake:

El administrador delegado es el mismo en todas las regiones.

- Al crear el administrador delegado, se convierte en el administrador delegado de cada región en la que active Security Lake.

Se recomienda configurar la cuenta de archivo de registro como la administradora delegada de Security Lake.

- La cuenta Log Archive está dedicada a ingerir y archivar todos los registros relacionados con la seguridad. Cuenta de AWS El acceso a esta cuenta suele estar limitado a unos pocos usuarios, como auditores y equipos de seguridad para investigar el cumplimiento. Recomendamos configurar la cuenta de archivo de registro como administradora delegada de Security Lake para que pueda ver los registros y eventos relacionados con la seguridad con un cambio de contexto mínimo.

- Además, recomendamos que solo un grupo mínimo de usuarios tenga acceso directo a la cuenta de archivo de registro. Fuera de este grupo selecto, si un usuario necesita acceder a los datos

que recopila Security Lake, puede añadirlo como suscriptor de Security Lake. Para obtener más información acerca de cómo añadir un suscriptor, consulte Gestión de suscriptores en Security Lake.

Si no utilizas el AWS Control Tower servicio, es posible que no tengas una cuenta de Log Archive. Para obtener más información sobre la cuenta de archivo de registro, consulte Unidad organizativa de seguridad: cuenta de archivo de registro en la Arquitectura de referencia de seguridad de AWS .

Una organización solo puede tener un administrador delegado.

Solo puede tener un administrador delegado de Security Lake para cada organización.

La cuenta de administración de la organización no puede ser el administrador delegado.

De acuerdo con las prácticas recomendadas de AWS seguridad y el principio de privilegios mínimos, la cuenta de administración de tu organización no puede ser el administrador delegado.

El administrador delegado debe formar parte de una organización activa.

Al eliminar una organización, la cuenta de administrador delegado ya no puede administrar Security Lake. Debe designar un administrador delegado de otra organización o usar Security Lake con una cuenta independiente que no forme parte de una organización.

Permisos de IAM necesarios para designar un administrador delegado

Al designar al administrador delegado de Security Lake, debe tener permisos para habilitar Security Lake y utilizar determinadas operaciones de AWS Organizations API que se enumeran en la siguiente declaración de política.

Puede añadir la siguiente declaración al final de una política AWS Identity and Access Management (IAM) para conceder estos permisos.

```
{
    "Sid": "Grant permissions to designate a delegated Security Lake administrator",
    "Effect": "Allow",
    "Action": [
        "securitylake:RegisterDataLakeDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
```

```
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Designar al administrador delegado de Security Lake y añadir cuentas de miembros

Elija el método de acceso para designar la cuenta de administrador de Security Lake delegado para su organización. Solo la cuenta de administración de una organización puede designar la cuenta de administrador delegado para su organización. La cuenta de administración de una organización no puede ser la cuenta de administrador delegado para su organización.

> **Note**
>
> - La cuenta de administración de la organización debe usar la operación `RegisterDataLakeDelegatedAdministrator` de Security Lake para designar la cuenta de administrador de Security Lake delegada. No se admite la designación del administrador delegado de Security Lake mediante Organizations.
> - Si desea cambiar el administrador delegado de la organización, primero debe eliminar el administrador delegado actual. Después puede designar un nuevo administrador delegado.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.

   Inicie sesión con las credenciales de la cuenta de administración de su organización.

2. - Si Security Lake aún no está activado, seleccione Comenzar y, a continuación, designe al administrador de Security Lake delegado en la página Habilitar Security Lake.
   - Si Security Lake ya está activado, designe al administrador de Security Lake delegado en la página Configuración.

3. En Delegar la administración en otra cuenta, introduce el Cuenta de AWS identificador de 12 dígitos de tu cuenta de Log Archive.

   Recomendamos usar el archivo de registros como administrador delegado de Security Lake. Para obtener más información, consulte Consideraciones importantes para administradores de Security Lake delegados.
4. Elija Delegar. Si Security Lake aún no está habilitado, cuando se designe el administrador delegado, Security Lake se habilitará para esa cuenta en la región actual.

API

Para designar al administrador delegado mediante programación, utilice el RegisterDataLakeDelegatedAdministrator funcionamiento de la API de Security Lake. Debe invocar la operación desde la cuenta de administración de la organización. Si utilizas el AWS CLI, ejecuta el register-data-lake-delegated-administrator comando desde la cuenta de administración de la organización. En tu solicitud, usa el `accountId` parámetro para especificar el identificador de cuenta de 12 dígitos de la Cuenta de AWS que vas a designar como la cuenta de administrador delegado de la organización.

Por ejemplo, el siguiente AWS CLI comando designa al administrador delegado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake register-data-lake-delegated-administrator \
--account-id 123456789012
```

El administrador delegado también puede automatizar la recopilación de datos de registro y eventos de AWS de las nuevas cuentas de la organización. Con esta configuración, Security Lake se habilita automáticamente en las cuentas nuevas cuando las cuentas se agregan a la organización en AWS Organizations. Como administrador delegado, puede habilitar esta configuración mediante el CreateDataLakeOrganizationConfiguration funcionamiento de la API de Security Lake o, si utiliza la CLI de AWS, ejecutando el create-data-lake-organization-configuration comando. En su solicitud, también puede especificar algunos ajustes de configuración para las cuentas nuevas.

Por ejemplo, el siguiente AWS CLI comando habilita automáticamente Security Lake y la recopilación de registros de consultas de resolución, AWS Security Hub CSPM hallazgos y registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) de Amazon Route 53 en las

nuevas cuentas de la organización. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-data-lake-organization-configuration \
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"ROUTE53"},{"sourceName":"SH_FINDINGS"},{"sourceName":"VPC_FLOW"}]}]'
```

Cuando la cuenta de administración de la organización designe el administrador delegado, el administrador puede habilitar y configurar Security Lake en la organización. Esto incluye habilitar y configurar Security Lake para recopilar datos de AWS registro y eventos de cuentas individuales de la organización. Para obtener más información, consulte Recopilación de datos de Servicios de AWS en Security Lake.

Puede usar la GetDataLakeOrganizationConfiguration operación para obtener detalles sobre la configuración actual de su organización para las nuevas cuentas de miembros.

Editar la configuración de activación automática para las nuevas cuentas de la organización

Un administrador delegado de Security Lake puede ver y editar la configuración de activación automática de las cuentas cuando se unen a su organización. Security Lake ingiere los datos en función de esta configuración únicamente para las cuentas nuevas, no para las cuentas existentes.

Siga los pasos siguientes para editar la configuración de las nuevas cuentas de la organización:

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, elija Cuentas.
3. En la página Cuentas, expanda la sección Configuración de una nueva cuenta. Puede ver qué fuentes ingiere Security Lake de cada región.
4. Seleccione Editar para editar esta configuración.
5. En la página Editar la configuración de la nueva cuenta, lleve a cabo los siguientes pasos:
   a. En Select Regions, seleccione una o más regiones de las que desee actualizar las fuentes de las que desea ingerir los datos. A continuación, elija Siguiente.
   b. En Seleccionar fuentes, elija una de las siguientes opciones para seleccionar fuentes:

i. Ingerir AWS fuentes predeterminadas: si eliges la opción recomendada, CloudTrail los eventos de datos de S3 no AWS WAF se incluyen para la ingesta de forma predeterminada. Esto se debe a que la ingesta de grandes volúmenes de ambos tipos de fuentes puede tener un impacto significativo en los costos de uso. Para ingerir estas fuentes, primero seleccione la opción Ingerir AWS fuentes específicas y, a continuación, seleccione estas fuentes en la lista de fuentes de registros y eventos.

ii. Ingerir AWS fuentes específicas: con esta opción, puede seleccionar una o más fuentes de registros y eventos que desee ingerir.

iii. No ingerir ninguna fuente: seleccione esta opción si no desea ingerir ninguna fuente de las regiones que seleccionó en el paso anterior.

iv. Elija Siguiente.

> **Note**
>
> Al habilitar Security Lake en una cuenta por primera vez, todos los orígenes de registros y eventos seleccionados formarán parte de un periodo de prueba gratuito de 15 días. Para obtener más información sobre las estadísticas de uso, consulte Revisar el uso de los costos estimados.

c. Tras revisar los cambios, selecciona Aplicar.

Cuando una persona Cuenta de AWS se una a tu organización, esta configuración se aplicará a esa cuenta de forma predeterminada.

Eliminación al administrador delegado de Security Lake

Solo la cuenta de administración de una organización puede eliminar la cuenta de administrador de Security Lake delegado para su organización. Si desea cambiar el administrador delegado de la organización, elimine el administrador delegado actual y después designe el nuevo administrador delegado.

> **Important**
>
> Al eliminar el administrador delegado de Security Lake, se elimina el lago de datos y se desactiva Security Lake para las cuentas de la organización.

No puede cambiar ni quitar el administrador delegado mediante la consola de Security Lake. Estas tareas solo se pueden realizar mediante programación.

Para eliminar al administrador delegado mediante programación, utilice la DeregisterDataLakeDelegatedAdministrator operación de la API de Security Lake. Debe invocar la operación desde la cuenta de administración de la organización. Si utilizas la AWS CLI, ejecuta el deregister-data-lake-delegated-administrator comando desde la cuenta de administración de la organización.

Por ejemplo, el siguiente AWS CLI comando elimina al administrador delegado de Security Lake.

```
$ aws securitylake deregister-data-lake-delegated-administrator
```

Para mantener la designación de administrador delegado pero cambiar los ajustes de configuración automática de las cuentas de DeleteDataLakeOrganizationConfiguration los miembros nuevos, utilice la API de Security Lake o, si utiliza AWS CLI, el delete-data-lake-organization-configuration comando. Solo el administrador delegado puede cambiar esta configuración para la organización.

Por ejemplo, el siguiente AWS CLI comando detiene la recopilación automática de las conclusiones del CSPM de Security Hub de las nuevas cuentas de miembros que se unen a la organización. Las nuevas cuentas de miembros no aportarán las conclusiones del CSPM de Security Hub al lago de datos una vez que el administrador delegado invoque esta operación. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake delete-data-lake-organization-configuration \
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"SH_FINDINGS"}]}]'
```

Acceso de confianza de Security Lake

Después de configurar Security Lake para una organización, la cuenta de AWS Organizations administración puede habilitar el acceso confiable con Security Lake. El acceso de confianza permite a Security Lake crear un rol vinculado al servicio de IAM y realizar tareas en su organización y en las cuentas de esta en su nombre. Para obtener más información, consulte Utilización de AWS Organizations con otros Servicios de AWS en la Guía del usuario de AWS Organizations .

Como usuario de la cuenta de administración de la organización, puede deshabilitar el acceso de confianza con Security Lake en AWS Organizations. Para obtener instrucciones sobre cómo

deshabilitar el acceso de confianza, consulte Cómo habilitar o deshabilitar el acceso de confianza en la Guía del usuario de AWS Organizations

Recomendamos deshabilitar el acceso confiable si el administrador delegado Cuenta de AWS está suspendido, aislado o cerrado.

Administración de regiones en Security Lake

Amazon Security Lake puede recopilar los registros de seguridad y los eventos Regiones de AWS en los que hayas habilitado el servicio. Para cada región, sus datos se almacenan en un bucket de Amazon S3 diferente. Puede especificar diferentes configuraciones de lago de datos (por ejemplo, diferentes orígenes y ajustes de retención) para diferentes regiones. También puede definir una más regiones acumulativas para consolidar los datos de varias regiones.

Comprobación del estado de la región

Security Lake puede recopilar datos en varios Regiones de AWS. Para realizar un seguimiento del estado de su lago de datos, puede resultar útil entender cómo está configurada actualmente cada región. Elija el método de acceso que prefiera y siga estos pasos para obtener el estado actual de una región.

Console

Para comprobar el estado de la región

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, elija Regiones. Aparecerá la página Regiones, que ofrece un resumen de las regiones en las que Security Lake está activado actualmente.
3. Seleccione una región y, a continuación, elija Editar para ver los detalles de esa región.

API

Para conocer el estado de la recopilación de registros en la región actual, utilice el GetDataLakeSources funcionamiento de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el get-data-lake-sources comando. Para el `accounts` parámetro, especifique uno o más Cuenta de AWS identificadores en forma de lista. Si su solicitud se realiza correctamente, Security Lake devuelve una instantánea de las cuentas de la región actual, que incluye AWS las fuentes de las que Security Lake recopila datos y el estado de cada fuente. Si no incluye el `accounts` parámetro, la respuesta incluye el estado de la recopilación de registros de todas las cuentas en las que Security Lake está configurado en la región actual.

Por ejemplo, el siguiente AWS CLI comando recupera el estado de recopilación de registros de las cuentas especificadas en la región actual. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake get-data-lake-sources \
--accounts "123456789012" "111122223333"
```

El siguiente AWS CLI comando muestra el estado de recopilación de registros de todas las cuentas y fuentes habilitadas en la región especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake get-data-lake-sources \
--regions "us-east-1" \
--query 'dataLakeSources[].[account,sourceName]'
```

Para determinar si ha habilitado Security Lake para una región, utilice la ListDataLakes operación. Si está utilizando el AWS CLI, ejecute el list-data-lakes comando. Para el parámetro `regions`, especifique el código de región de la región; por ejemplo, `us-east-1` para la región Este de EE. UU. (Norte de Virginia). Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS. La operación `ListDataLakes` devuelve los ajustes de configuración del lago de datos para cada región que especifique en su solicitud. Si no especifica una región, Security Lake devuelve los ajustes de estado y configuración de su lago de datos en cada región en la que Security Lake esté disponible.

Por ejemplo, el siguiente AWS CLI comando muestra el estado y los ajustes de configuración de su lago de datos en la `eu-central-1` región. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake list-data-lakes \
--regions "us-east-1" "eu-central-1"
```

Cambiar la configuración de la región

Elija el método que prefiera y siga estas instrucciones para actualizar la configuración del lago de datos en una o más Regiones de AWS.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, elija Regiones.
3. Seleccione una región y, a continuación, elija Editar.
4. Marque la casilla de verificación Anular los orígenes de todas las cuentas en <Región> para confirmar que las selecciones que realice aquí anulan las selecciones anteriores de esta región.
5. En Seleccionar clases de almacenamiento, elija Añadir transición para añadir nuevas clases de almacenamiento a tus datos.
6. En Etiquetas, puede asignar o editar las etiquetas de la región. Una etiqueta es una etiqueta que puede definir y asignar a ciertos tipos de AWS recursos, incluida la configuración del lago de datos para su región Cuenta de AWS en particular. Para obtener más información, consulte Etiquetado de los recursos de Security Lake.
7. Para convertir una región en una región acumulativa, seleccione Regiones acumulativas (en Configuración) en el panel de navegación. Después elija Modificar. En la sección Seleccionar regiones de acumulación, elija Añadir región de acumulación. Seleccione las regiones que contribuyen y dé permiso a Security Lake para replicar datos en varias regiones. Cuando termine, seleccione Guardar para guardar sus cambios.

API

Para actualizar la configuración regional de su lago de datos mediante programación, utilice el UpdateDataLake funcionamiento de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el update-data-lake comando. Para el parámetro `region`, especifique el código de región de la región para la que quiere hacer cambios; por ejemplo, `us-east-1` para la región Este de EE. UU. (Norte de Virginia). Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.

Utilice parámetros adicionales para especificar un nuevo valor para cada configuración que desee cambiar, por ejemplo, la clave de cifrado (`encryptionConfiguration`) y la configuración de retención (`lifecycleConfiguration`).

Por ejemplo, el siguiente AWS CLI comando actualiza la configuración de caducidad de los datos y de transición de clases de almacenamiento para la `us-east-1` región. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ update-data-lake \
--configurations '[{"region":"us-east-1","lifecycleConfiguration": {"expiration":
{"days":500},"transitions":[{"days":45,"storageClass":"ONEZONE_IA"}]}}]'
```

Configuración de regiones acumulativas en Security Lake

Una región acumulativa consolida los datos de una o más regiones contribuyentes. Especificar una región acumulativa puede ayudarle a cumplir con los requisitos de conformidad regionales.

Debido a las limitaciones de Amazon S3, no se admite la replicación desde un lago de datos regional cifrado con clave administrada por el cliente (CMK) a un lago de datos regional cifrado administrado por S3 (cifrado predeterminado).

Important

Si ha creado una fuente personalizada, para garantizar que los datos de origen personalizados se replican correctamente en el destino, Security Lake recomienda seguir las prácticas recomendadas que se describen en la sección Prácticas recomendadas para la ingesta de fuentes personalizadas. La replicación no se puede realizar en datos que no sigan el formato de ruta de datos de la partición S3, tal como se describe en la página.

Antes de añadir una región acumulativa, primero debe crear dos funciones diferentes en AWS Identity and Access Management (IAM):

- Rol de IAM para la replicación de datos
- Función de IAM que se debe registrar AWS Glue particiones

Note

Security Lake crea estas funciones de IAM o utiliza las funciones existentes en su nombre cuando utiliza la consola de Security Lake. Sin embargo, debe crear estas funciones cuando utilice la API de Security Lake o AWS CLI.

Rol de IAM para la replicación de datos

Este rol de IAM otorga permiso a Amazon S3 para replicar registros y eventos de origen en varias regiones.

Para conceder estos permisos, cree un rol de IAM que comience con el prefijo `SecurityLake` y adjunte el siguiente ejemplo de política al rol. Necesitará el nombre de recurso de Amazon (ARN) del rol al crear una región acumulativa en Security Lake. En esta política, `sourceRegions` son regiones contribuyentes y `destinationRegions` son regiones acumulativas.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadS3ReplicationSetting",
      "Action": [
        "s3:ListBucket",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectRetention",
        "s3:GetObjectLegalHold"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*",
        "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    },
    {
      "Sid": "AllowS3Replication",
```

```
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[destinationRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    }
  ]
}
```

Para conceder permiso a Amazon S3 para asumir el rol, asigne la siguiente política de confianza al rol:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3ToAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Si usa una clave administrada por el cliente desde AWS Key Management Service (AWS KMS) para cifrar su lago de datos de Security Lake, debe conceder los siguientes permisos además de los permisos de la política de replicación de datos.

```
{
    "Action": [
        "kms:Decrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "s3.{sourceRegion1}.amazonaws.com",
                "s3.{sourceRegion2}.amazonaws.com"
                ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion1}*",
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion2}*"
            ]
        }
    },
    "Resource": [
        "{sourceRegion1KmsKeyArn}",
        "{sourceRegion2KmsKeyArn}"
    ]
},
{
    "Action": [
        "kms:Encrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
            "s3.{destinationRegion1}.amazonaws.com",
            ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{destinationRegion1}*",
            ]
        }
    },
    "Resource": [
            "{destinationRegionKmsKeyArn}"
```

```
    ]
}
```

Para obtener más información sobre las funciones de replicación, consulte la sección Configuración de permisos en la Guía del usuario de Amazon Simple Storage Service.

Función de IAM que se debe registrar AWS Glue particiones

Esta función de IAM otorga permisos para una AWS Lambda función de actualización de particiones utilizada por Security Lake para registrar AWS Glue particiones para los objetos de S3 que se replicaron desde otras regiones. Si no se crea este rol, los suscriptores no pueden consultar los eventos de esos objetos.

Para conceder estos permisos, cree un rol con el nombre `AmazonSecurityLakeMetaStoreManager` (es posible que ya lo haya creado al incorporarse a Security Lake). Para obtener más información sobre este rol, incluido una política de ejemplo, consulte Paso 1: Crear funciones de IAM.

En la consola de Lake Formation, también debe conceder los permisos `AmazonSecurityLakeMetaStoreManager` como administrador del lago de datos siguiendo estos pasos:

1. Abra la consola de Lake Formation en. https://console.aws.amazon.com/lakeformation/
2. Inicie sesión como usuario administrativo.
3. Si aparece la ventana de bienvenida a Lake Formation, elija el usuario de IAM que creó o seleccionó en el Paso 1 y, a continuación, elija Comenzar.
4. Si no aparece la ventana de bienvenida a Lake Formation, siga estos pasos para configurar un administrador de Lake Formation.
    1. En el panel de navegación, en Permisos, elija Roles y tareas administrativas. En la sección Administradores de lago de datos de la página de la consola, seleccione Elegir administradores.
    2. En el cuadro de diálogo Administrar administradores de lagos de datos, para los usuarios y roles de IAM, elija el rol de AmazonSecurityLakeMetaStoreManager IAM que creó y, a continuación, elija Guardar.

Para obtener más información sobre cómo cambiar los permisos de los administradores de lagos de datos, consulte Crear un administrador de lagos de datos en la Guía para AWS Lake Formation desarrolladores.

Añadir regiones acumulativas

Elija el método de acceso que prefiera y siga estos pasos para añadir una región acumulativa.

> **Note**
>
> Una región puede aportar datos a varias regiones acumulativas. Sin embargo, una región acumulativa no puede ser una región que contribuya a otra región acumulativa.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, en Configuración, seleccione Regiones acumulativas.
3. Seleccione Modificar y, a continuación, seleccione Añadir región acumulativa.
4. Especifique la región acumulativa y las regiones que contribuirán. Repita este paso si desea agregar varias regiones acumulativas.
5. Si es la primera vez que agrega una región acumulativa, para Acceso al servicio, cree un nuevo rol de IAM o utilice un rol de IAM existente que dé permiso a Security Lake para replicar datos en varias regiones.
6. Cuando termine, elija Guardar.

También puede añadir una región acumulativa al embarcar en Security Lake. Para obtener más información, consulte Introducción a Amazon Security Lake.

API

Para agregar una región acumulativa mediante programación, utilice la UpdateDataLake operación de la API de Security Lake. Si está utilizando la AWS CLI, ejecute el comando. update-data-lake En su solicitud, utilice el campo `region` para especificar la región que desea que aporte datos a la región acumulativa. En la `regions` matriz del `replicationConfiguration` parámetro, especifique el código de región para cada región acumulada. Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.

Por ejemplo, el siguiente comando se establece `ap-northeast-2` como una región de resumen. La `us-east-1` región aportará datos a la `ap-northeast-2` región. Este ejemplo también establece un período de caducidad de 365 días para los objetos que se agregan al lago de datos. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":365}}}]'
```

También puede añadir una región acumulativa al embarcar en Security Lake. Para ello, utilice la CreateDataLake operación (o, si utiliza AWS CLI, el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/update-data-lake.html create-data-lake). Para obtener más información sobre la configuración de las regiones acumulativas durante la incorporación, consulte. Introducción a Amazon Security Lake

Actualizar o eliminar regiones acumulativas

Elija el método de acceso que prefiera y siga estos pasos para actualizar o eliminar las regiones acumulativas en Security Lake.

Console

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/
2. En el panel de navegación, en Configuración, seleccione Regiones acumulativas.
3. Elija Modificar.
4. Para cambiar las regiones contribuyentes por una región acumulativa, especifique las regiones contribuyentes actualizadas en la fila correspondiente a la región acumulativa.
5. Para eliminar una región acumulativa, seleccione Eliminar en la fila de regiones acumulativas.
6. Cuando termine, elija Guardar.

API

Para configurar las regiones acumulativas mediante programación, utilice el UpdateDataLake funcionamiento de la API de Security Lake. Si está utilizando la AWS CLI, ejecute el comando. update-data-lake En su solicitud, utilice los parámetros compatibles para especificar la configuración de región acumulativa:

- Para añadir una región contribuyente, utilice el campo `region` para especificar el código de la región que desee añadir. En la matriz `regions` del objeto `replicationConfiguration`, especifique el código de región de cada región acumulativa a la que desee aportar datos. Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.
- Para eliminar una región contribuyente, utilice el campo `region` para especificar el código de la región que desee eliminar. No especifique ningún valor para los parámetros `replicationConfiguration`.

Por ejemplo, el siguiente comando configura ambas regiones `us-east-1` y las configura `us-east-2` como regiones contribuyentes. Ambas regiones contribuirán con datos a la región `ap-northeast-3` acumulada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":365}}},
{"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","replicationConfiguration": {"regions": ["ap-
northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeS3ReplicationRole"}, "lifecycleConfiguration": {"expiration":
{"days":500},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}}]'
```

Administración de fuentes en Security Lake

Las fuentes son registros y eventos generados a partir de un único sistema que coinciden con una clase de evento específica del Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake esquema. Amazon Security Lake puede recopilar registros y eventos de diversas fuentes, incluidas fuentes compatibles de forma nativa Servicios de AWS y personalizadas de terceros.

Security Lake ejecuta tareas de extracción, transformación y carga (ETL) en datos de origen sin procesar y convierte los datos al formato Apache Parquet y al esquema OCSF. Tras el procesamiento, Security Lake almacena los datos de origen en un bucket de Amazon Simple Storage Service (Amazon S3) en Cuenta de AWS Región de AWS el que se generaron los datos. Security Lake crea un bucket de Amazon S3 diferente para cada región en la que se habilita el servicio. Cada fuente recibe un prefijo independiente en el bucket de S3 y Security Lake organiza los datos de cada fuente en un conjunto de AWS Lake Formation tablas independiente.

Temas

- Recopilación de datos de Servicios de AWS en Security Lake
- Recopilación de datos de fuentes personalizadas en Security Lake

Recopilación de datos de Servicios de AWS en Security Lake

Amazon Security Lake puede recopilar registros y eventos de los siguientes Servicios de AWS compatibles de forma nativa:

- AWS CloudTrail eventos de administración y datos (S3, Lambda)
- Registros de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS)
- Registros de consultas de Amazon Route 53 Resolver
- AWS Security Hub CSPM hallazgos
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF registros v2

Security Lake transforma automáticamente estos datos a Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake y al formato Apache Parquet.

> **Tip**
>
> Para agregar uno o más de los servicios anteriores como fuente de registro en Security Lake, no necesita configurar el inicio de sesión de estos servicios por separado, excepto los eventos CloudTrail de administración. Si tiene el registro configurado en estos servicios, no necesita cambiar la configuración de registro para añadirlos como fuentes de registro en Security Lake. Security Lake extrae los datos directamente de estos servicios a través de un flujo de eventos independiente y duplicado.

Prerrequisito: verificar permisos

Para agregar uno Servicio de AWS como fuente en Security Lake, debe tener los permisos necesarios. Compruebe que la política AWS Identity and Access Management (IAM) asociada al rol que utiliza para agregar una fuente tenga permiso para realizar las siguientes acciones:

- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:GetDatabase`
- `glue:GetTable`
- `glue:UpdateTable`
- `iam:CreateServiceLinkedRole`
- `s3:GetObject`
- `s3:PutObject`

Se recomienda que el rol tenga las siguientes condiciones y alcance de recursos para los `s3:PutObject` permisos `S3:getObject` y.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUpdatingSecurityLakeS3Buckets",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::aws-security-data-lake*",
              "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
    }
    ]
}
```

Estas acciones le permiten recopilar registros y eventos del an Servicio de AWS y enviarlos a la AWS Glue base de datos y tabla correctas.

Si utilizas una AWS KMS clave para cifrar tu lago de datos desde el lado del servidor, también necesitarás permiso para hacerlo. `kms:DescribeKey`

Agregar un Servicio de AWS como fuente

Después de agregar una Servicio de AWS fuente, Security Lake comienza a recopilar automáticamente los registros y eventos de seguridad de la misma. Estas instrucciones le indican cómo agregar una fuente compatible de forma nativa Servicio de AWS en Security Lake. Para obtener instrucciones sobre cómo añadir un origen personalizado, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Console

Para agregar un AWS fuente de registro (consola)

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, elija Orígenes.
3. Seleccione Servicio de AWS aquella de la que desea recopilar datos y elija Configurar.
4. En la sección Configuración de la fuente, habilite la fuente y seleccione la versión de la fuente de datos que desea usar para la ingesta de datos. De forma predeterminada, Security Lake ingiere la versión más reciente de la fuente de datos.

> **Important**
>
> Si no tiene los permisos de rol necesarios para habilitar la nueva versión de la fuente de AWS registro en la región especificada, póngase en contacto con su administrador de Security Lake. Para obtener más información, consulte Actualizar los permisos de los roles.

Para que los suscriptores puedan incorporar la versión seleccionada de la fuente de datos, también debes actualizar la configuración de los suscriptores. Para obtener más información sobre cómo editar un suscriptor, consulte Administración de suscriptores en Amazon Security Lake.

Si lo desea, puede optar por incorporar únicamente la versión más reciente e inhabilitar todas las versiones de origen anteriores utilizadas para la ingesta de datos.

5. En la sección Regiones, seleccione las regiones en las que desea recopilar datos para la fuente. Security Lake recopilará datos del origen de todas las cuentas de las regiones seleccionadas.
6. Elija Habilitar.

API

Para agregar una fuente de AWS registro (API)

Para agregar una Servicio de AWS fuente mediante programación, utilice la CreateAwsLogSource operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/create-aws-log-source.html create-aws-log-source. Los parámetros `sourceName` y `regions` son obligatorios. Si lo desea, puede limitar el alcance de la fuente a una fuente específica o específica. `accounts` `sourceVersion`

> **Important**
>
> Cuando no proporciona un parámetro en el comando, Security Lake asume que el parámetro que falta se refiere a todo el conjunto. Por ejemplo, si no proporciona el

`accounts` parámetro, el comando se aplica a todo el conjunto de cuentas de su organización.

En el siguiente ejemplo, se agregan los registros de flujo de la VPC como fuente en las cuentas y regiones designadas. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

> **Note**
>
> Si aplicas esta solicitud a una región en la que no has habilitado Security Lake, recibirás un error. Puedes resolver el error habilitando Security Lake en esa región o usando el `regions` parámetro para especificar solo las regiones en las que hayas habilitado Security Lake.

```
$ aws securitylake create-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions=["us-east-2"],sourceVersion="2.0"
```

Obtener el estado de la recopilación de fuentes

Elija su método de acceso y siga los pasos para obtener una instantánea de las cuentas y fuentes en las que está habilitada la recopilación de registros en la región actual.

Console

Para conocer el estado de la recopilación de registros en la región actual

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, elija Cuentas.
3. Pase el cursor sobre el número de la columna Fuentes para ver qué registros están habilitados para la cuenta seleccionada.

API

Para conocer el estado de la recopilación de registros en la región actual, utilice el GetDataLakeSources funcionamiento de la API de Security Lake. Si usa el comando get-data-lake-sources AWS CLI, ejecute el comando https://docs.aws.amazon.com/cli/latest/reference/securitylake/get-data-lake-sources.html get-data-lake-sources. Para el `accounts` parámetro, puede especificar uno o más Cuenta de AWS ID en forma de lista. Si su solicitud se realiza correctamente, Security Lake devuelve una instantánea de las cuentas de la región actual, que incluye AWS las fuentes de las que Security Lake recopila datos y el estado de cada fuente. Si no incluye el `accounts` parámetro, la respuesta incluye el estado de la recopilación de registros de todas las cuentas en las que Security Lake está configurado en la región actual.

Por ejemplo, el siguiente AWS CLI comando recupera el estado de recopilación de registros de las cuentas especificadas en la región actual. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake get-data-lake-sources \
--accounts "123456789012" "111122223333"
```

Actualización de los permisos de rol en Security Lake

Si no dispone de los recursos o los permisos de rol necesarios (nueva AWS Lambda función y cola de Amazon Simple Queue Service (Amazon SQS)) para incorporar datos de una nueva versión de la fuente de datos, debe actualizar los permisos de su `AmazonSecurityLakeMetaStoreManagerV2` rol y crear un nuevo conjunto de recursos para procesar los datos de sus fuentes.

Elija el método que prefiera y siga las instrucciones para actualizar los permisos de su rol y crear nuevos recursos para procesar los datos de una nueva versión de una fuente de AWS registro en una región específica. Esta acción se realiza una sola vez, ya que los permisos y los recursos se aplican automáticamente a las futuras versiones de las fuentes de datos.

Console

Para actualizar los permisos de los roles (consola)

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.

   Inicie sesión con las credenciales del administrador delegado de Security Lake.
2. En el panel de navegación, en Configuración, seleccione General.

3. Elija Actualizar los permisos de los roles.
4. En la sección Acceso al servicio, realice una de las siguientes acciones:
   - Crear y usar un nuevo rol de servicio: puede usar el AmazonSecurityLakeMetaStoreManagerV2 rol creado por Security Lake.
   - Usar un rol de servicio existente: puede elegir un rol de servicio existente en la lista de nombres de roles de servicio.
5. Seleccione Aplicar.

API

Para actualizar los permisos de los roles (API)

Para actualizar los permisos mediante programación, utilice la UpdateDataLake operación de la API de Security Lake. Para actualizar los permisos mediante AWS CLI, ejecute el update-data-lake comando.

Para actualizar los permisos de su rol, debe adjuntar la AmazonSecurityLakeMetastoreManager política al rol.

Eliminar el AmazonSecurityLakeMetaStoreManager rol

> **Important**
>
> Tras actualizar los permisos de su rol a`AmazonSecurityLakeMetaStoreManagerV2`, confirme que el lago de datos funciona correctamente antes de eliminar el `AmazonSecurityLakeMetaStoreManager` rol anterior. Se recomienda esperar al menos 4 horas antes de eliminar el rol.

Si decide eliminar el rol, primero debe eliminarlo de `AmazonSecurityLakeMetaStoreManager` AWS Lake Formation.

Siga estos pasos para eliminar el `AmazonSecurityLakeMetaStoreManager` rol de la consola de Lake Formation.

1. Inicia sesión en y abre la Consola de administración de AWS consola de Lake Formation en https://console.aws.amazon.com/lakeformation/.

2. En la consola de Lake Formation, en el panel de navegación, elija Funciones y tareas administrativas.
3. Eliminar `AmazonSecurityLakeMetaStoreManager` de cada región.

Eliminar un Servicio de AWS como fuente de Security Lake

Elija su método de acceso y siga estos pasos para eliminar una fuente de Security Lake compatible de forma nativa Servicio de AWS . Puede eliminar un origen de una o más regiones. Al eliminar el origen, Security Lake deja de recopilar datos de ese origen en las regiones y cuentas especificadas, y los suscriptores ya no pueden consumir nuevos datos del origen. Sin embargo, los suscriptores pueden seguir consumiendo los datos que Security Lake recopiló del origen antes de la eliminación. Solo puede usar estas instrucciones para eliminar un Servicio de AWS compatible de forma nativa como origen. Para obtener información acerca de cómo eliminar un origen personalizado, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Console

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/
2. En el panel de navegación, elija Orígenes.
3. Seleccione un origen y elija Desactivar.
4. Seleccione una o varias regiones en las que desee dejar de recopilar datos de este origen. Security Lake dejará de recopilar datos del origen de todas las cuentas de las regiones seleccionadas.

API

Para eliminar una Servicio de AWS fuente mediante programación, utilice la DeleteAwsLogSource operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/delete-aws-log-source.html delete-aws-log-source. Los parámetros `sourceName` y `regions` son obligatorios. Si lo desea, puede limitar el alcance de la eliminación a uno específico o específico. `accounts` `sourceVersion`

> **Important**
>
> Cuando no proporciona un parámetro en el comando, Security Lake asume que el parámetro que falta se refiere a todo el conjunto. Por ejemplo, si no proporciona el

`accounts` parámetro, el comando se aplica a todo el conjunto de cuentas de su organización.

En el siguiente ejemplo, se eliminan los registros de flujo de la VPC como fuente en las cuentas y regiones designadas.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

En el siguiente ejemplo, se elimina Route 53 como fuente en la cuenta y las regiones designadas.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

Los ejemplos anteriores están formateados para Linux, macOS o Unix y utilizan la barra invertida (\) como continuación de línea para mejorar la legibilidad.

CloudTrail registros de eventos en Security Lake

AWS CloudTrail le proporciona un historial de las llamadas a la AWS API de su cuenta, incluidas las llamadas a la Consola de administración de AWS API realizadas mediante los AWS SDK, las herramientas de línea de comandos y ciertos AWS servicios. CloudTrail también le permite identificar qué usuarios y cuentas llamaron a AWS las API de los servicios compatibles CloudTrail, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Security Lake puede recopilar los registros asociados a los eventos CloudTrail de administración y CloudTrail los eventos de datos para S3 y Lambda. CloudTrail los eventos de administración, los eventos de datos de S3 y los eventos de datos de Lambda son tres fuentes independientes en Security Lake. Como resultado, tienen valores diferentes para `sourceName` cuando se agrega uno de ellos como origen de registro ingerido. Los eventos de administración, también conocidos como eventos del plano de control, proporcionan información sobre las operaciones de administración que se realizan en los recursos de su Cuenta de AWS empresa. CloudTrail Los eventos de datos, también conocidos como operaciones del plano de datos, muestran las operaciones de recursos

realizadas en o dentro de los recursos de su Cuenta de AWS. Estas operaciones suelen ser actividades de gran volumen.

Para recopilar los eventos CloudTrail de administración en Security Lake, debe tener al menos un registro organizativo CloudTrail multirregional que recopile los eventos de CloudTrail administración de lectura y escritura. El registro debe estar habilitado para el registro de seguimiento. Si tiene el registro configurado en los otros servicios, no necesita cambiar la configuración de registro para añadirlos como fuentes de registro en Security Lake. Security Lake extrae los datos directamente de estos servicios a través de un flujo de eventos independiente y duplicado.

Un seguimiento de múltiples regiones distribuye los archivos de registro desde múltiples regiones a un único bucket de Amazon Simple Storage Service (Amazon S3) para una única Cuenta de AWS. Si ya tiene un registro multirregional administrado a través de la CloudTrail consola o no es AWS Control Tower necesario realizar ninguna otra acción.

- Para obtener información sobre cómo crear y administrar un recorrido CloudTrail, consulte Crear un recorrido para una organización en la Guía del AWS CloudTrail usuario.
- Para obtener información sobre cómo crear y administrar un registro AWS Control Tower, consulte la Guía del AWS Control Tower usuario para registrar AWS Control Tower acciones. AWS CloudTrail

Cuando agrega CloudTrail eventos como fuente, Security Lake comienza inmediatamente a recopilar sus registros de CloudTrail eventos. Consume los eventos CloudTrail de administración y datos directamente CloudTrail a través de un flujo de eventos independiente y duplicado.

Security Lake no administra sus CloudTrail eventos ni afecta a las CloudTrail configuraciones existentes. Para administrar el acceso y la retención de sus CloudTrail eventos directamente, debe usar la consola de CloudTrail servicio o la API. Para obtener más información, consulte Visualización de CloudTrail eventos con historial de eventos en la Guía del AWS CloudTrail usuario.

La siguiente lista proporciona enlaces al GitHub repositorio a la referencia cartográfica sobre cómo Security Lake normaliza CloudTrail los eventos según el OCSF.

GitHub Repositorio de eventos de OCSF CloudTrail

- Versión de origen 1 (v1.0.0-rc.2)
- Versión de origen 2 (v1.1.0) https://github.com/ocsf/examples/tree/main/mappings/markdown/AWS/v1.1.0/CloudTrail

Registros de auditoría de Amazon EKS en Security Lake

Cuando agrega los registros de auditoría de Amazon EKS como fuente, Security Lake comienza a recopilar información detallada sobre las actividades realizadas en los recursos de Kubernetes que se ejecutan en los clústeres de Elastic Kubernetes Service (EKS). Los registros de auditoría de EKS lo ayudan a detectar actividades potencialmente sospechosas en sus clústeres de EKS dentro del Amazon Elastic Kubernetes Service.

Security Lake consume los eventos del registro de auditoría de EKS directamente desde la función de registro del plano de control de Amazon EKS a través de un flujo de registros de auditoría independiente y duplicado. Este proceso está diseñado para no requerir una configuración adicional ni afectar a las configuraciones de registro existentes del plano de control de Amazon EKS que pueda tener. Para obtener más información, consulte Registros del plano de control del clúster de Amazon EKS en la Guía del usuario de Amazon EKS.

Los registros de auditoría de Amazon EKS solo se admiten en la versión 1.1.0 de OCSF. Para obtener información sobre cómo Security Lake normaliza los eventos de los registros de auditoría de EKS con OCSF, consulte la referencia de mapeo de los eventos de los registros de auditoría de Amazon EKS en el repositorio de GitHub OCSF (v1.1.0).

Las consultas de resolución de Route 53 registran en Security Lake

Los registros de consultas de Route 53 Resolver rastrean las consultas de DNS realizadas por los recursos dentro de Amazon Virtual Private Cloud (Amazon VPC). Esto le ayuda a entender cómo funcionan sus aplicaciones y a detectar las amenazas de seguridad.

Cuando agrega los registros de consultas de resolución de Route 53 como origen en Security Lake, Security Lake comienza inmediatamente a recopilar los registros de consultas de resolución directamente desde Route 53 a través de un flujo de eventos independiente y duplicado.

Security Lake no administra los registros de Route 53 ni afecta a las configuraciones de registro de consultas de los solucionadores existentes. Para administrar los registros de consultas de resolución, debe utilizar la consola de servicio de Route 53. Para obtener más información, consulte Administración del registro de consultas de Resolver en la Guía para desarrolladores de Amazon Route 53.

La siguiente lista proporciona enlaces de GitHub repositorios a la referencia cartográfica sobre cómo Security Lake normaliza los registros de Route 53 a OCSF.

GitHub Repositorio OCSF para los registros de Route 53

- Versión de origen 1 (v1.0.0-rc.2)
- Versión de origen 2 (v1.1.0) https://github.com/ocsf/examples/tree/main/mappings/markdown/AWS/v1.1.0/Route53

Hallazgos de Security Hub sobre CSPM en Security Lake

Las conclusiones del CSPM de Security Hub le ayudan a comprender su postura en materia de seguridad AWS y le permiten comprobar que su entorno cumple con los estándares y las mejores prácticas del sector de la seguridad. El CSPM de Security Hub recopila las conclusiones de diversas fuentes, incluidas las integraciones con otras Servicios de AWS integraciones de productos de terceros y las comprueba con los controles del CSPM de Security Hub. El CSPM de Security Hub procesa las conclusiones en un formato estándar denominado formato de búsqueda de seguridad (ASFF). AWS

Cuando agrega los hallazgos del CSPM de Security Hub como fuente en Security Lake, Security Lake comienza inmediatamente a recopilar los hallazgos directamente del CSPM de Security Hub a través de un flujo de eventos independiente y duplicado. Security Lake también transforma los resultados de ASFF a Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake (OCSF).

Security Lake no administra las conclusiones del CSPM de Security Hub ni afecta a la configuración del CSPM de Security Hub. Para administrar las conclusiones del CSPM de Security Hub, debe usar la consola de servicio, la API o la API de Security Hub CSPM. AWS CLI Para obtener más información, consulte Resultados en AWS Security Hub CSPM en la Guía del usuario de AWS Security Hub .

La siguiente lista proporciona enlaces al GitHub repositorio a la referencia cartográfica sobre cómo Security Lake normaliza las conclusiones del CSPM de Security Hub con respecto al OCSF.

GitHub Repositorio OCSF de las conclusiones del CSPM de Security Hub

- Versión de origen 1 (v1.0.0-rc.2) https://github.com/ocsf/examples/tree/main/mappings/markdown/AWS/v1.0.0-rc.2/Security%20Hub
- Versión de origen 2 (v1.1.0) https://github.com/ocsf/examples/tree/main/mappings/markdown/AWS/v1.1.0/Security%20Hub

Registros de flujo de VPC en Security Lake

La característica de los registros de flujo de Amazon VPC captura información sobre el tráfico IP entrante y saliente de las interfaces de red de su entorno de VPC.

Cuando agrega registros de flujo de VPC como origen en Security Lake, Security Lake comienza inmediatamente a recopilar sus registros de flujo de VPC. Consume los registros de flujo de la VPC directamente desde Amazon VPC a través de un flujo de registros de flujo independiente y duplicado.

Security Lake no administra los registros de flujo de VPC ni afecta a las configuraciones de Amazon VPC. Para administrar sus registros de flujo, debe utilizar la consola de servicio de Amazon VPC. Para obtener más información, consulte Uso de registros de flujo en la Guía para desarrolladores de Amazon VPC.

La siguiente lista proporciona enlaces de GitHub repositorios a la referencia cartográfica sobre cómo Security Lake normaliza los registros de flujo de la VPC a OCSF.

GitHub Repositorio OCSF para registros de flujo de VPC

- Versión de origen 1 (v1.0.0-rc.2)
- Versión de origen 2 (v1.1.0) https://github.com/ocsf/examples/tree/main/mappings/markdown/AWS/v1.1.0/VPC%20Flowlogs

AWS WAF inicia sesión en Security Lake

Cuando los agrega AWS WAF como fuente de registros en Security Lake, Security Lake comienza inmediatamente a recopilar los registros. AWS WAF es un firewall de aplicaciones web que puede usar para supervisar las solicitudes web que los usuarios finales envían a sus aplicaciones y para controlar el acceso a su contenido. La información registrada incluye la hora en la que se AWS WAF recibió una solicitud web de su AWS recurso, la información detallada sobre la solicitud y los detalles sobre las reglas a las que se ajustó la solicitud.

Security Lake consume AWS WAF los registros directamente AWS WAF a través de un flujo de registros independiente y duplicado. Este proceso está diseñado para no requerir una configuración adicional ni afectar a las AWS WAF configuraciones existentes. Los registros de Security Lake solo recuperan los datos permitidos por la configuración de la lista de control de acceso AWS WAF web (ACL web). Si la protección de datos está habilitada para la ACL web en las cuentas de Security Lake, los datos generados se redactarán o se codificarán en función de la configuración de la ACL

web. Para obtener información sobre cómo AWS WAF utilizarlos para proteger los recursos de la aplicación, consulte Cómo AWS WAF funciona en la Guía para AWS WAF desarrolladores.

> **Important**
>
> Si utiliza la CloudFront distribución de Amazon como tipo de recurso AWS WAF, debe seleccionar EE.UU. Este (Virginia del Norte) para introducir los registros globales en Security Lake.

AWS WAF los registros solo se admiten en la versión 1.1.0 de OCSF. Para obtener información sobre cómo Security Lake normaliza los eventos de AWS WAF registro a OCSF, consulte la referencia de mapeo en el repositorio de registros de GitHub OCSF (v1.1.0). AWS WAF

Eliminar un Servicio de AWS como fuente

Elija su método de acceso y siga estos pasos para eliminar una fuente de Security Lake compatible de forma nativa Servicio de AWS . Puede eliminar un origen de una o más regiones. Al eliminar el origen, Security Lake deja de recopilar datos de ese origen en las regiones y cuentas especificadas, y los suscriptores ya no pueden consumir nuevos datos del origen. Sin embargo, los suscriptores pueden seguir consumiendo los datos que Security Lake recopiló del origen antes de la eliminación. Solo puede usar estas instrucciones para eliminar un Servicio de AWS compatible de forma nativa como origen. Para obtener información acerca de cómo eliminar un origen personalizado, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Console

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/
2. En el panel de navegación, elija Orígenes.
3. Seleccione un origen y elija Desactivar.
4. Seleccione una o varias regiones en las que desee dejar de recopilar datos de este origen. Security Lake dejará de recopilar datos del origen de todas las cuentas de las regiones seleccionadas.

API

Para eliminar una Servicio de AWS fuente mediante programación, utilice la DeleteAwsLogSource operación de la API de Security Lake. Si usa AWS Command Line

Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/delete-aws-log-source.html delete-aws-log-source. Los parámetros `sourceName` y `regions` son obligatorios. Si lo desea, puede limitar el alcance de la eliminación a uno específico o específico. `accounts` `sourceVersion`

> **Important**
>
> Cuando no proporciona un parámetro en el comando, Security Lake asume que el parámetro que falta se refiere a todo el conjunto. Por ejemplo, si no proporciona el `accounts` parámetro, el comando se aplica a todo el conjunto de cuentas de su organización.

En el siguiente ejemplo, se eliminan los registros de flujo de la VPC como fuente en las cuentas y regiones designadas.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

En el siguiente ejemplo, se elimina Route 53 como fuente en la cuenta y las regiones designadas.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

Los ejemplos anteriores están formateados para Linux, macOS o Unix y utilizan la barra invertida (\) para facilitar la lectura.

Recopilación de datos de fuentes personalizadas en Security Lake

Amazon Security Lake puede recopilar registros y eventos de orígenes de terceros personalizados. Una fuente personalizada de Security Lake es un servicio de terceros que envía registros y eventos de seguridad a Amazon Security Lake. Antes de enviar los datos, la fuente personalizada debe convertir los registros y los eventos al marco abierto de esquemas de ciberseguridad (OCSF) y cumplir con los requisitos de fuente de Security Lake, incluidos los requisitos de particionamiento, formato de archivo en parquet y tamaño y velocidad de los objetos.

Para cada origen personalizado, Security Lake gestiona lo siguiente:

- Proporciona un prefijo único para el origen de su bucket de Amazon S3.
- Crea un rol en AWS Identity and Access Management (IAM) que permite a una fuente personalizada escribir datos en el lago de datos. El límite de permisos para este rol lo establece una política AWS administrada denominada `AmazonSecurityLakePermissionsBoundary`.
- Crea una AWS Lake Formation tabla para organizar los objetos que la fuente escribe en Security Lake.
- Configura un AWS Glue rastreador para particionar los datos de origen. El rastreador lo rellena AWS Glue Data Catalog con la tabla. También descubre automáticamente nuevos datos de origen y extrae las definiciones de los esquemas.

> **Note**
>
> Puede agregar hasta un máximo de 50 fuentes de registro personalizadas en una cuenta.

Para agregar una fuente personalizada a Security Lake, debe cumplir los siguientes requisitos. El incumplimiento de estos requisitos podría afectar al rendimiento y a los casos de uso de la analítica, como las consultas.

- Destino: la fuente personalizada debe poder escribir datos en Security Lake como un conjunto de objetos S3 con el prefijo asignado al origen. En el caso de los orígenes que contienen varias categorías de datos, debe entregar cada clase de evento única de Open Cybersecurity Schema Framework (OCSF) como un origen independiente. Security Lake crea un rol de IAM que permite al origen personalizado escribir en la ubicación especificada del bucket de S3.
- Formato: cada objeto de S3 que se recopile del origen personalizado debe tener el formato de un archivo de Apache Parquet.
- Esquema: se debe aplicar la misma clase de evento de OCSF a cada registro de un Parquet-formatted objeto. Security Lake es compatible con las versiones 1.x y 2.x de Parquet. El tamaño de la página de datos debe limitarse a 1 MB (sin comprimir). El tamaño del grupo de filas no debe ser superior a 256 MB (comprimido). Para la compresión dentro del objeto Parquet, se prefiere el estándar.
- Particionamiento: los objetos deben particionarse por región, AWS cuenta y EventDay. Los objetos deben tener el prefijo. *`source location`*`/region=`*`region`*`/accountId=`*`accountID`*`/eventDay=`*`yyyyMMdd`*`/`

- Tamaño y velocidad del objeto: los archivos enviados a Security Lake deben enviarse en incrementos de entre 5 minutos y 1 día del evento. Los clientes pueden enviar archivos con más frecuencia de 5 minutos si los archivos tienen un tamaño superior a 256 MB. El requisito de objeto y tamaño es optimizar Security Lake para el rendimiento de las consultas. El incumplimiento de los requisitos de fuente personalizados puede afectar al rendimiento de Security Lake.
- Clasificación: dentro de cada Parquet-formatted objeto, los registros deben ordenarse por tiempo para reducir el costo de consultar los datos.

> **Note**
>
> Utilice la herramienta de validación OCSF para verificar si la fuente personalizada es compatible con. `OCSF Schema` En el caso de las fuentes personalizadas, Security Lake admite la versión 1.3 y anteriores de OCSF.

Requisitos de partición para la ingesta de fuentes personalizadas en Security Lake

Para facilitar el procesamiento de datos y las consultas eficientes, debemos cumplir con los requisitos de particionamiento, objetos y tamaño al agregar una fuente personalizada a Security Lake:

Particiones

Los objetos deben particionarse según la ubicación de origen y la Región de AWS fecha Cuenta de AWS.

- La ruta de datos de la partición está formateada como

  `/ext/`*`custom-source-name`*`/region=`*`region`*`/accountId=`*`accountID`*`/eventDay=`*`YYYYMMDD`*.

  Una partición de ejemplo con un nombre de bucket de ejemplo es`aws-security-data-lake-`*`us-west-2-lake-uid`*`/ext/`*`custom-source-name`*`/region=`*`us-west-2`*`/accountId=`*`123456789012`*`/eventDay=`*`20230428`*`/`.

En la siguiente lista se describen los parámetros que se utilizan en la partición de ruta de S3:

- El nombre del bucket de Amazon S3 en el que Security Lake almacena sus datos de origen personalizados.
- `source-location`: prefijo para el origen personalizado de su bucket de S3. Security Lake almacena todos los objetos de S3 de un origen determinado con este prefijo, que es exclusivo de ese origen.
- `region`— Región de AWS al que se cargan los datos. Por ejemplo, debes usarlo para subir datos `US East (N. Virginia)` a tu bucket de Security Lake, en la región de EE. UU. Este (Virginia del Norte).
- `accountId`— Cuenta de AWS ID al que pertenecen los registros de la partición de origen. Para los registros pertenecientes a cuentas externas AWS, recomendamos usar una cadena como `external` `oexternal_externalAccountId`. Al adoptar esta convención de nomenclatura, puede evitar la ambigüedad a la hora de nombrar los ID de cuentas externas para que no entren en conflicto con los ID de AWS cuenta o los ID de cuentas externas mantenidos por otros sistemas de administración de identidades.
- `eventDay`— Marca de hora UTC del registro, truncada a una hora con formato de cadena de ocho caracteres (). `YYYYMMDD` Si los registros especifican una zona horaria diferente en la marca de tiempo del evento, debes convertir la marca de tiempo en UTC para esta clave de partición.

Requisitos previos para agregar una fuente personalizada en Security Lake

Al agregar un origen personalizado, Security Lake crea un rol de IAM que permite al origen escribir datos en la ubicación correcta del lago de datos. El nombre del rol sigue el formato `AmazonSecurityLake-Provider-{name of the custom source}-{region}` Región de AWS en el que se agrega la fuente personalizada. `region` Security Lake adjunta una política al rol que permite el acceso al lago de datos. Si ha cifrado el lago de datos con una AWS KMS clave administrada por el cliente, Security Lake también adjunta una política `kms:Decrypt` y `kms:GenerateDataKey` permisos a la función. El límite de permisos para este rol lo establece una política AWS administrada denominada `AmazonSecurityLakePermissionsBoundary`.

Temas

- Verificar permisos
- Cree una función de IAM para permitir el acceso de escritura a la ubicación del bucket de Security Lake (API) y AWS CLI-único paso)

Verificar permisos

Antes de añadir un origen personalizado, verifique que tenga los permisos para realizar las siguientes acciones.

Para verificar sus permisos, utilice IAM para revisar las políticas de IAM asociadas a su identidad de IAM. A continuación, debe comparar la información de estas políticas con la siguiente lista de acciones que debe poder añadir como un origen personalizado.

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StopCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

Estas acciones le permiten recopilar registros y eventos de una fuente personalizada, enviarlos a la AWS Glue base de datos y tabla correctas y almacenarlos en Amazon S3.

Si utiliza una AWS KMS clave para cifrar su lago de datos desde el lado del servidor, también necesitará permiso para `kms:CreateGrant``kms:DescribeKey`, y. `kms:GenerateDataKey`

> **Important**
>
> Si piensa usar la consola de Security Lake para agregar una fuente personalizada, puede omitir el paso siguiente y continuar con. Agregar una fuente personalizada en Security Lake La consola de Security Lake ofrece un proceso simplificado para empezar y crea todas los roles de IAM necesarios o utiliza las funciones existentes en su nombre.

Si planea usar la API de Security Lake o AWS CLI agregar una fuente personalizada, continúe con el siguiente paso para crear un rol de IAM que permita el acceso de escritura a la ubicación del bucket de Security Lake.

Cree una función de IAM para permitir el acceso de escritura a la ubicación del bucket de Security Lake (API) y AWS CLI-único paso)

Si usa la API de Security Lake o AWS CLI quiere agregar una fuente personalizada, agregue esta función de IAM para conceder AWS Glue permiso para rastrear sus datos de origen personalizados e identificar las particiones en los datos. Estas particiones son necesarias para organizar los datos y crear y actualizar tablas en el catálogo de datos.

Después de crear este rol de IAM, necesitará el nombre de recurso de Amazon (ARN) del rol para añadir un origen personalizado.

Debes adjuntar la política `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS gestionada.

Para conceder los permisos necesarios, también debe crear e integrar la siguiente política integrada en su rol para poder leer los archivos de datos de la fuente personalizada y las tablas create/update del catálogo de AWS Glue datos. Rastreador de AWS Glue

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "S3WriteRead",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
```

```
}
```

Adjunte la siguiente política de confianza para permitir que una Cuenta de AWS persona asuma el rol en función del ID externo:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "glue.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Si el bucket de S3 de la región en la que vas a añadir la fuente personalizada está cifrado con un depósito gestionado por el cliente AWS KMS key, también debes adjuntar la siguiente política al rol y a tu política de claves de KMS:

```
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey"
        "kms:Decrypt"
    ],
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::{{name of S3 bucket created by Security Lake}}"
            ]
        }
    },
    "Resource": [
        "{{ARN of customer managed key}}"
    ]
```

```
}
```

Agregar una fuente personalizada en Security Lake

Tras crear la función de IAM para invocar el AWS Glue rastreador, siga estos pasos para agregar una fuente personalizada en Security Lake.

Console

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea crear la fuente personalizada.
3. Elija Orígenes personalizados en el panel de navegación y, a continuación, elija Crear origen personalizado.
4. En la sección Detalles del origen personalizado, introduzca un nombre único a nivel mundial para el origen personalizado. A continuación, seleccione una clase de evento de OCSF que describa el tipo de datos que el origen personalizado enviará a Security Lake.
5. Para Cuenta de AWS con permiso para escribir datos, introduzca el ID de Cuenta de AWS y el ID externo del origen personalizado que escribirá los registros y eventos en el lago de datos.
6. Para Acceso al servicio, cree y utilice un nuevo rol de servicio o utilice un rol de servicio existente que dé permiso a Security Lake para invocar la AWS Glue.
7. Seleccione Crear.

API

Para agregar una fuente personalizada mediante programación, utilice la CreateCustomLogSource operación de la API de Security Lake. Utilice la operación en el Región de AWS lugar donde desee crear la fuente personalizada. Si usas AWS Command Line Interface (AWS CLI), ejecuta el comando create-custom-log-source.

En su solicitud, utilice los parámetros compatibles para especificar la configuración del origen personalizado:

- `sourceName`— Especifique un nombre para la fuente. El nombre debe ser un valor único a nivel regional.

- `eventClasses`— Especifique una o más clases de eventos de OCSF para describir el tipo de datos que la fuente enviará a Security Lake. Para obtener una lista de las clases de eventos de OCSF admitidas como fuente en Security Lake, consulte Open Cybersecurity Schema Framework (OCSF).
- `sourceVersion`— Si lo desea, especifique un valor para limitar la recopilación de registros a una versión específica de los datos de origen personalizados.
- `crawlerConfiguration`— Especifique el nombre de recurso de Amazon (ARN) del rol de IAM que creó para invocar el rastreador. AWS Glue Para ver los pasos detallados para crear un rol de IAM, consulte Requisitos previos para agregar una fuente personalizada
- `providerIdentity`— Especifique la AWS identidad y el ID externo que utilizará la fuente para escribir los registros y los eventos en el lago de datos.

En el siguiente ejemplo, se agrega una fuente personalizada como fuente de registro en la cuenta del proveedor de registros designado en las regiones designadas. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-custom-log-source \
--source-name EXAMPLE_CUSTOM_SOURCE \
--event-classes '["DNS_ACTIVITY", "NETWORK_ACTIVITY"]' \
--configuration crawlerConfiguration={"roleArn=arn:aws:iam::XXX:role/service-role/
RoleName"},providerIdentity={"externalId=ExternalId,principal=principal"}  \
--region=[“ap-southeast-2”]
```

Mantener actualizados los datos de origen personalizados en AWS Glue

Después de agregar una fuente personalizada en Security Lake, Security Lake crea un AWS Glue rastreador. El rastreador se conecta a su origen personalizado, determina las estructuras de datos y rellena el catálogo de datos de AWS Glue con tablas.

Recomendamos ejecutar el rastreador manualmente para mantener actualizado el esquema de origen personalizado y mantener la funcionalidad de consulta en Athena y otros servicios de consultas. En concreto, debe ejecutar el rastreador si se produce alguno de los siguientes cambios en el conjunto de datos de entrada de un origen personalizado:

- El conjunto de datos tiene una o más columnas nuevas de nivel superior.

- El conjunto de datos tiene uno o más campos nuevos en una columna con un tipo de datos `struct`.

Para obtener instrucciones sobre cómo ejecutar un rastreador, consulte Programar un AWS Glue rastreador en la AWS Glue Guía para desarrolladores.

Security Lake no puede eliminar ni actualizar los rastreadores existentes en su cuenta. Si elimina un origen personalizado, te recomendamos eliminar el rastreador asociado si piensa crear un origen personalizado con el mismo nombre en el futuro.

Clases de eventos de OCSF compatibles

Las clases de eventos del Open Cybersecurity Schema Framework (OCSF) describen el tipo de datos que la fuente personalizada enviará a Security Lake. La lista de clases de eventos compatibles es la siguiente:

```
public enum OcsfEventClass {
    ACCOUNT_CHANGE,
    API_ACTIVITY,
    APPLICATION_LIFECYCLE,
    AUTHENTICATION,
    AUTHORIZE_SESSION,
    COMPLIANCE_FINDING,
    DATASTORE_ACTIVITY,
    DEVICE_CONFIG_STATE,
    DEVICE_CONFIG_STATE_CHANGE,
    DEVICE_INVENTORY_INFO,
    DHCP_ACTIVITY,
    DNS_ACTIVITY,
    DETECTION_FINDING,
    EMAIL_ACTIVITY,
    EMAIL_FILE_ACTIVITY,
    EMAIL_URL_ACTIVITY,
    ENTITY_MANAGEMENT,
    FILE_HOSTING_ACTIVITY,
    FILE_SYSTEM_ACTIVITY,
    FTP_ACTIVITY,
    GROUP_MANAGEMENT,
    HTTP_ACTIVITY,
    INCIDENT_FINDING,
    KERNEL_ACTIVITY,
    KERNEL_EXTENSION,
```

```
    MEMORY_ACTIVITY,
    MODULE_ACTIVITY,
    NETWORK_ACTIVITY,
    NETWORK_FILE_ACTIVITY,
    NTP_ACTIVITY,
    PATCH_STATE,
    PROCESS_ACTIVITY,
    RDP_ACTIVITY,
    REGISTRY_KEY_ACTIVITY,
    REGISTRY_VALUE_ACTIVITY,
    SCHEDULED_JOB_ACTIVITY,
    SCAN_ACTIVITY,
    SECURITY_FINDING,
    SMB_ACTIVITY,
    SSH_ACTIVITY,
    USER_ACCESS,
    USER_INVENTORY,
    VULNERABILITY_FINDING,
    WEB_RESOURCE_ACCESS_ACTIVITY,
    WEB_RESOURCES_ACTIVITY,
    WINDOWS_RESOURCE_ACTIVITY,
    // 1.3 OCSF event classes
    ADMIN_GROUP_QUERY,
    DATA_SECURITY_FINDING,
    EVENT_LOG_ACTIVITY,
    FILE_QUERY,
    FILE_REMEDIATION_ACTIVITY,
    FOLDER_QUERY,
    JOB_QUERY,
    KERNEL_OBJECT_QUERY,
    MODULE_QUERY,
    NETWORK_CONNECTION_QUERY,
    NETWORK_REMEDIATION_ACTIVITY,
    NETWORKS_QUERY,
    PERIPHERAL_DEVICE_QUERY,
    PROCESS_QUERY,
    PROCESS_REMEDIATION_ACTIVITY,
    REMEDIATION_ACTIVITY,
    SERVICE_QUERY,
    SOFTWARE_INVENTORY_INFO,
    TUNNEL_ACTIVITY,
    USER_QUERY,
    USER_SESSION_QUERY,
    // 1.3 OCSF event classes (Win extension)
```

```
    PREFETCH_QUERY,
    REGISTRY_KEY_QUERY,
    REGISTRY_VALUE_QUERY,
    WINDOWS_SERVICE_ACTIVITY
}
```

Eliminar una fuente personalizada de Security Lake

Elimine un origen personalizado para dejar de enviar datos desde el origen a Security Lake. Al eliminar el origen, Security Lake deja de recopilar datos de ese origen en las regiones y cuentas especificadas, y los suscriptores ya no pueden consumir nuevos datos del origen. Sin embargo, los suscriptores pueden seguir consumiendo los datos que Security Lake recopiló del origen antes de la eliminación. Solo puede usar estas instrucciones para eliminar una fuente personalizada. Para obtener información sobre cómo eliminar una fuente compatible de forma nativa, consulte Servicio de AWS. Recopilación de datos de Servicios de AWS en Security Lake

Al eliminar una fuente personalizada en Security Lake, debe deshabilitar cada fuente fuera de la consola de Security Lake con la fuente. Si no se desactiva una integración, es posible que las integraciones de origen sigan enviando registros a Amazon S3.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región de la que desea eliminar la fuente personalizada.
3. En el panel de navegación, elija Orígenes de datos.
4. Seleccione el origen personalizado que desea eliminar.
5. Seleccione Anular el registro de un origen personalizado y, a continuación, seleccione Eliminar para confirmar la acción.

API

Para eliminar una fuente personalizada mediante programación, utilice la DeleteCustomLogSource operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/delete-custom-log-source.html delete-custom-log-source. Utilice la operación en la Región de AWS en la que desee eliminar el origen personalizado.

En la solicitud, utilice el parámetro `sourceName` para especificar el nombre del origen personalizado que se va a eliminar. O bien, especifique el nombre de un origen personalizado y utilice el parámetro `sourceVersion` para limitar el alcance de la eliminación a solo una versión específica de los datos del origen personalizado.

En el siguiente ejemplo, se elimina una fuente de registro personalizada de Security Lake.

Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake delete-custom-log-source \
--source-name EXAMPLE_CUSTOM_SOURCE
```

Gestión de suscriptores en Security Lake

Un suscriptor de Amazon Security Lake consume registros y eventos de Security Lake. Para controlar los costos y cumplir con las mejores prácticas de acceso con privilegios mínimos, usted proporciona a los suscriptores acceso a los datos por fuente. Para obtener más información sobre orígenes, consulte Administración de fuentes en Security Lake.

Security Lake admite dos tipos de acceso de suscriptores:

- Acceso a los datos Los suscriptores con acceso a datos de origen en Amazon Security Lake reciben notificaciones de nuevos objetos para la fuente a medida que los datos se escriben en el bucket de S3. De forma predeterminada, los suscriptores reciben notificaciones sobre nuevos objetos a través de un punto de enlace HTTPS que ellos proporcionan. Como alternativa, los suscriptores pueden recibir notificaciones sobre nuevos objetos sondeando una cola del Amazon Simple Queue Service (Amazon SQS).
- Acceso a consultas: los suscriptores con acceso a consultas pueden consultar los datos que recopila Security Lake. Estos suscriptores consultan directamente las tablas de AWS Lake Formation de su bucket de S3 con servicios como Amazon Athena.

Los suscriptores solo tienen acceso a los datos de origen Región de AWS que haya seleccionado al crear el suscriptor. Para permitir que un suscriptor acceda a los datos de varias regiones, puede especificar la región en la que creó el suscriptor como región acumulativa y hacer que otras regiones le aporten datos. Para obtener más información sobre las regiones acumulables y las regiones contribuyentes, consulte. Administración de regiones en Security Lake

> **Important**
>
> El número máximo de fuentes que Security Lake permite añadir por suscriptor es de 10. Podría ser una combinación de AWS fuentes y fuentes personalizadas.

Temas

- Administración del acceso a los datos para los suscriptores de Security Lake
- Administración del acceso a las consultas para los suscriptores de Security Lake

Administración del acceso a los datos para los suscriptores de Security Lake

Los suscriptores que tienen acceso a los datos de origen de Amazon Security Lake reciben una notificación de la existencia de nuevos objetos para la fuente a medida que los datos se escriben en el bucket de S3. De forma predeterminada, los suscriptores reciben notificaciones sobre los nuevos objetos a través del punto final HTTPS que proporcionan. Como alternativa, los suscriptores pueden recibir notificaciones sobre nuevos objetos consultando una cola de Amazon Simple Queue Service (Amazon SQS).

Los suscriptores reciben una notificación sobre los nuevos objetos de Amazon S3 para una fuente a medida que los objetos se escriben en el lago de datos de Security Lake. Los suscriptores pueden acceder directamente a los objetos de S3 y recibir notificaciones sobre nuevos objetos a través de un punto final de suscripción o consultando una cola de Amazon Simple Queue Service (Amazon SQS). Este tipo de suscripción se identifica `S3` en el `accessTypes` parámetro de la API. CreateSubscriber

Temas

- Requisitos previos para crear un suscriptor con acceso a datos en Security Lake
- Crear un suscriptor con acceso a datos en Security Lake
- Actualización de un suscriptor de datos en Security Lake
- Eliminar un suscriptor de datos de Security Lake

Requisitos previos para crear un suscriptor con acceso a datos en Security Lake

Debe cumplir los siguientes requisitos previos antes de poder crear un suscriptor con acceso a datos en Security Lake.

Verificar permisos

Para verificar sus permisos, utilice IAM para revisar las políticas de IAM asociadas a su identidad de IAM. A continuación, compare la información de esas políticas con la siguiente lista de acciones (permisos) que debe realizar para notificar a los suscriptores cuando se escriban nuevos datos en el lago de datos.

Necesitará permiso para realizar las siguientes acciones:

- iam:CreateRole
- iam:DeleteRolePolicy
- iam:GetRole
- iam:PutRolePolicy
- lakeformation:GrantPermissions
- lakeformation:ListPermissions
- lakeformation:RegisterResource
- lakeformation:RevokePermissions
- ram:GetResourceShareAssociations
- ram:GetResourceShares
- ram:UpdateResourceShare

Además de la lista anterior, también necesitará permiso para realizar las siguientes acciones:

- events:CreateApiDestination
- events:CreateConnection
- events:DescribeRule
- events:ListApiDestinations
- events:ListConnections
- events:PutRule
- events:PutTargets
- s3:GetBucketNotification
- s3:PutBucketNotification
- sqs:CreateQueue
- sqs:DeleteQueue
- sqs:GetQueueAttributes
- sqs:GetQueueUrl
- sqs:SetQueueAttributes

Obtenga el identificador externo del suscriptor

Para crear un suscriptor, además del Cuenta de AWS identificador del suscriptor, también necesitarás obtener su identificador externo. El ID externo es un identificador único que te proporciona el suscriptor. Security Lake agrega el ID externo al rol de IAM del suscriptor que crea. Utiliza el ID externo cuando crea un suscriptor en la consola de Security Lake, a través de la API, o AWS CLI.

Para obtener más información sobre los ID externos, consulte Cómo usar un ID externo para conceder acceso a sus AWS recursos a un tercero en la Guía del usuario de IAM.

> **Important**
>
> Si planea usar la consola de Security Lake para agregar un suscriptor, puede omitir el siguiente paso y continuar a Crear un suscriptor con acceso a datos en Security Lake. La consola de Security Lake ofrece un proceso simplificado para empezar y crea todas los roles de IAM necesarios o utiliza las funciones existentes en su nombre.
> Si tiene pensado utilizar la API de Security Lake o AWS CLI añadir un suscriptor, continúe con el siguiente paso para crear un rol de IAM que le permita invocar EventBridge los destinos de la API.

Cree un rol de IAM para invocar los destinos de API (EventBridge API) y AWS CLI-solo paso)

Si utilizas Security Lake a través de una API o AWS CLI creas un rol en AWS Identity and Access Management (IAM) que conceda a Amazon EventBridge permisos para invocar los destinos de la API y enviar notificaciones de objetos a los puntos de enlace HTTPS correctos.

Tras crear este rol de IAM, necesitarás el nombre de recurso de Amazon (ARN) del rol para crear el suscriptor. Este rol de IAM no es necesario si el suscriptor consulta los datos de una cola de Amazon Simple Queue Service (Amazon SQS) o consulta directamente los datos desde allí. AWS Lake Formation Para obtener más información sobre este tipo de método de acceso a los datos (tipo de acceso), consulte. Administración del acceso a las consultas para los suscriptores de Security Lake

Adjunte la siguiente política a su rol de IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInvokeApiDestination",
            "Effect": "Allow",
            "Action": [
                "events:InvokeApiDestination"
            ],
            "Resource": [
            "arn:aws:events:us-east-1:123456789012:api-destination/
AmazonSecurityLake*/*"
            ]
        }
    ]
}
```

Adjunte la siguiente política de confianza a su función de IAM EventBridge para poder asumirla:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEventBridgeToAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "events.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Security Lake crea automáticamente un rol de IAM que permite al suscriptor leer los datos del lago de datos (o sondear los eventos de una cola de Amazon SQS si ese es el método de

notificación preferido). Este rol se protege mediante una política AWS gestionada denominada. `AmazonSecurityLakePermissionsBoundary`

Crear un suscriptor con acceso a datos en Security Lake

Elija uno de los siguientes métodos de acceso para crear un suscriptor con acceso a los datos actuales Región de AWS.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea crear el suscriptor.
3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, selecciona Crear suscriptor.
5. Para ver los detalles del suscriptor, introduce el nombre del suscriptor y una descripción opcional.

   La región se rellena automáticamente según la selección actual Región de AWS y no se puede modificar.
6. En el caso de las fuentes de registros y eventos, elige qué fuentes está autorizado a consumir el suscriptor.
7. En el método de acceso a los datos, elija S3 para configurar el acceso a los datos para el suscriptor.
8. Para las credenciales del suscriptor, proporcione el Cuenta de AWS ID del suscriptor y el ID externo.
9. (Opcional) Para obtener más información sobre las notificaciones, si desea que Security Lake cree una cola de Amazon SQS que el suscriptor pueda consultar en busca de notificaciones de objetos, seleccione la cola de SQS. Si desea que Security Lake envíe las notificaciones a través de un punto final HTTPS, EventBridge seleccione el punto final de suscripción.

   Si selecciona el punto final de suscripción, haga también lo siguiente:

   a. Introduzca el punto final de la suscripción. Entre los ejemplos de formatos de punto final válidos se incluyen**`http://example.com`**. Si lo desea, también puede proporcionar un nombre de clave HTTPS y un valor de clave HTTPS.

b. Para el acceso a los servicios, cree una nueva función de IAM o utilice una función de IAM existente que dé EventBridge permiso para invocar los destinos de la API y enviar notificaciones de objetos a los puntos finales correctos.

   Para obtener información sobre la creación de un nuevo rol de IAM, consulte Crear un rol de IAM para invocar los destinos de la API. EventBridge

10. (Opcional) En el caso de las etiquetas, introduzca hasta 50 etiquetas para asignárselas al suscriptor.

    Una etiqueta es una etiqueta que se puede definir y asignar a determinados tipos de AWS recursos. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarlo a identificar, clasificar y administrar los recursos de diferentes maneras. Para obtener más información, consulte Etiquetado de los recursos de Security Lake.

11. Seleccione Crear.

API

Para crear un suscriptor con acceso a los datos mediante programación, utilice el CreateSubscriber funcionamiento de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/create-subscriber.html create-subscriber.

En tu solicitud, usa estos parámetros para especificar los siguientes ajustes para el suscriptor:

- Para `sources` ello, especifique cada fuente a la que desea que acceda el suscriptor.
- Para`subscriberIdentity`, especifique el ID de la AWS cuenta y el ID externo que utilizará el suscriptor para acceder a los datos de origen.
- Para`subscriber-name`, especifique el nombre del suscriptor.
- En `accessTypes`, especifique `S3`.

Ejemplo 1

En el siguiente ejemplo, se crea un suscriptor con acceso a los datos de la AWS región actual para la identidad de suscriptor especificada para una AWS fuente.

```
$ aws securitylake create-subscriber \
```

```
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, "sourceVersion": 2.0}}] \
--subscriber-name subscriber name \
--access-types S3
```

Ejemplo 2

El siguiente ejemplo crea un suscriptor con acceso a los datos de la AWS región actual para la identidad de suscriptor especificada para una fuente personalizada.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{"customLogSource": {"sourceName": custom-source-name,
 "sourceVersion": 2.0}}] \
--subscriber-name subscriber name
--access-types S3
```

Los ejemplos anteriores están formateados para Linux, macOS o Unix y utilizan la barra invertida (\) como carácter de continuación de línea para mejorar la legibilidad.

(Opcional) Tras crear un suscriptor, utilice la CreateSubscriberNotification operación para especificar cómo avisar al suscriptor cuando se escriban nuevos datos en el lago de datos para las fuentes a las que desea que acceda el suscriptor. Si utilizas el AWS Command Line Interface (AWS CLI), ejecuta el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/create-subscriber-notification.html create-subscriber-notification.

- Para anular el método de notificación predeterminado (punto final HTTPS) y crear una cola de Amazon SQS, especifique los valores de los parámetros. `sqsNotificationConfiguration`
- Si prefiere la notificación con un punto final HTTPS, especifique los valores de los parámetros. `httpsNotificationConfiguration`
- Para el `targetRoleArn` campo, especifique el ARN del rol de IAM que creó para invocar los destinos de la API EventBridge .

```
$ aws securitylake create-subscriber-notification \
--subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \
--configuration
 httpsNotificationConfiguration={"targetRoleArn"="arn:aws:iam::XXX:role/service-role/RoleName", "endpoint"="https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"}
```

Para obtenerlo`subscriberID`, utilice la ListSubscribers operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando list-subscriber.

```
$ aws securitylake list-subscribers
```

Para cambiar posteriormente el método de notificación (cola de Amazon SQS o punto de enlace HTTPS) para el suscriptor, utilice la UpdateSubscriberNotification operación o, si está utilizando AWS CLI, ejecute el comando update-subscriber-notification. https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/update-subscriber-notification.html También puede cambiar el método de notificación mediante la consola de Security Lake: seleccione el suscriptor en la página de suscriptores y, a continuación, elija Editar.

Ejemplo de mensaje de notificación de objetos

El siguiente ejemplo muestra la notificación de eventos en formato de estructura JSON para la `CreateSubscriberNotification` operación.

```
{
  "source": "aws.s3",
  "time": "2021-11-12T00:00:00Z",
  "account": "123456789012",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ],
  "detail": {
    "bucket": {
      "name": "amzn-s3-demo-bucket"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b57f9512698f4b09e608f4f2a65852e5"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "securitylake.amazonaws.com"
  }
}
```

Actualización de un suscriptor de datos en Security Lake

Puede actualizar un suscriptor cambiando las fuentes de las que consume el suscriptor. También puedes asignar o editar las etiquetas de un suscriptor. Una etiqueta es una etiqueta que puedes definir y asignar a ciertos tipos de AWS recursos, incluidos los suscriptores. Para obtener más información, consulte Etiquetado de los recursos de Security Lake.

Elige uno de los métodos de acceso y sigue estos pasos para definir nuevas fuentes para una suscripción existente.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación izquierdo, elija Suscriptores.
3. Seleccione el suscriptor.
4. Selecciona Editar y, a continuación, realiza una de las siguientes acciones:
   - Para actualizar las fuentes del suscriptor, introduce la nueva configuración en la sección Fuentes de registro y eventos.
   - Para asignar o editar etiquetas para el suscriptor, cámbielas según sea necesario en la sección Etiquetas.
5. Cuando termine, elija Guardar.

API

Para actualizar las fuentes de acceso a los datos de un suscriptor mediante programación, utilice la UpdateSubscriber operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/update-subscriber.html update-subscriber. En tu solicitud, usa los `sources` parámetros para especificar cada fuente a la que deseas que acceda el suscriptor.

```
$ aws securitylake update-subscriber --subscriber-id subscriber ID
```

Para obtener una lista de suscriptores asociados a una organización Cuenta de AWS u organización específica, usa la ListSubscribers operación. Si usas el comando AWS Command Line Interface (AWS CLI), ejecuta el comando list-subscribers.

```
$ aws securitylake list-subscribers
```

Para revisar la configuración actual de un suscriptor en particular, utilice la GetSubscriber operación. Ejecute el comando get-subscriber. A continuación, Security Lake devuelve el nombre y la descripción del suscriptor, el identificador externo y la información adicional. Si usa el AWS Command Line Interface (AWS CLI), ejecute el comando get-subscriber.

Para actualizar el método de notificación de un suscriptor, usa la UpdateSubscriberNotification operación. Si utilizas el AWS Command Line Interface (AWS CLI), ejecuta el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/update-subscriber-notification.html update-subscriber-notification. Por ejemplo, puede especificar un nuevo punto final HTTPS para el suscriptor o cambiar de un punto final HTTPS a una cola de Amazon SQS.

Eliminar un suscriptor de datos de Security Lake

Si ya no desea que un suscriptor consuma datos de Security Lake, puede eliminar al suscriptor siguiendo estos pasos.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación izquierdo, elija Suscriptores.
3. Seleccione el suscriptor que desea eliminar.
4. Elija Eliminar y confirme la acción. Esto eliminará el suscriptor y todos los ajustes de notificación asociados.

API

Según tu situación, realiza una de las siguientes acciones:

- Para eliminar el suscriptor y todos los ajustes de notificación asociados, utilice la DeleteSubscriber operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando delete-subscriber.
- Para retener al suscriptor pero detener las futuras notificaciones al suscriptor, utilice la DeleteSubscriberNotification operación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando ejecutar el comando https://

awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/delete-subscriber-notification.html delete-subscriber-notification.

Administración del acceso a las consultas para los suscriptores de Security Lake

Los suscriptores con acceso a las consultas pueden consultar los datos que recopila Security Lake. Estos suscriptores consultan directamente AWS Lake Formation las tablas de su bucket de S3 con servicios como Amazon Athena. Aunque el motor de consultas principal de Security Lake es Athena, también puede utilizar otros servicios, como Amazon Redshift Spectrum y Spark SQL, que se integran con. AWS Glue Data Catalog

Los suscriptores consultan los datos de origen de AWS Lake Formation las tablas de su bucket de S3 mediante servicios como Amazon Athena. Este tipo de suscripción se identifica `LAKEFORMATION` en el `accessTypes` parámetro de la CreateSubscriber API.

> **Note**
>
> En esta sección se explica cómo conceder acceso a consultas a un suscriptor externo. Para obtener información sobre cómo ejecutar consultas en su propio lago de datos, consultePaso 4: Vea y consulte sus propios datos.

Temas

- Requisitos previos para crear un suscriptor con acceso a las consultas en Security Lake
- Crear un suscriptor con acceso a las consultas en Security Lake
- Editar un suscriptor con acceso a consultas en Security Lake

Requisitos previos para crear un suscriptor con acceso a las consultas en Security Lake

Debe cumplir los siguientes requisitos previos antes de poder crear un suscriptor con acceso a datos en Security Lake.

Verificar permisos

Antes de crear un suscriptor con acceso a las consultas, compruebe que tiene permiso para realizar la siguiente lista de acciones.

Para verificar sus permisos, utilice IAM para revisar las políticas de IAM asociadas a su identidad de IAM. A continuación, compare la información de esas políticas con la siguiente lista de acciones que debe poder realizar para crear un suscriptor con acceso a las consultas.

- `glue:PutResourcePolicy`
- `glue:DeleteResourcePolicy`
- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `lakeformation:GrantPermissions`
- `lakeformation:ListPermissions`
- `lakeformation:RegisterResource`
- `lakeformation:RevokePermissions`
- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

> **Important**
>
> Después de verificar los permisos:
>
> - Si planea usar la consola de Security Lake para agregar un suscriptor con acceso a las consultas, puede omitir el paso siguiente y continuar con Otorgue permisos de administrador a Lake Formation. Security Lake crea todos los roles de IAM necesarios o usa los roles existentes en su nombre.
> - Si planea usar la API o la CLI de Security Lake para agregar un suscriptor con acceso de consulta, continúe con el siguiente paso para crear un rol de IAM para consultar los datos de Security Lake.

Cree una función de IAM para consultar los datos de Security Lake (API) y AWS CLI-solo paso)

Cuando utilice la API de Security Lake o AWS CLI para conceder acceso de consulta a un suscriptor, tendrá que crear un rol denominado`AmazonSecurityLakeMetaStoreManager`. Security Lake usa esta función para registrar AWS Glue particiones y actualizar AWS Glue tablas. Es posible que ya haya creado este rol mientras estaba creando los roles de IAM necesarios.

Otorgue permisos de administrador a Lake Formation

También tendrás que añadir permisos de administrador de Lake Formation a la función de IAM que utilizas para acceder a la consola de Security Lake y añadir suscriptores.

Puedes conceder permisos de administrador a tu rol en Lake Formation siguiendo estos pasos:

1. Abra la consola de Lake Formation en https://console.aws.amazon.com/lakeformation/.
2. Inicie sesión como usuario administrativo.
3. Si aparece la ventana de bienvenida a Lake Formation, elija el usuario de IAM que creó o seleccionó en el Paso 1 y, a continuación, elija Comenzar.
4. Si no aparece la ventana de bienvenida a Lake Formation, siga estos pasos para configurar un administrador de Lake Formation.
    1. En el panel de navegación, en Permisos, elija Roles y tareas administrativas. En la sección Administradores de lago de datos, elija Elegir administradores.
    2. En el cuadro de diálogo Administrar administradores de lagos de datos, para los usuarios y las funciones de IAM, elija la función de administrador utilizada al acceder a la consola de Security Lake y, a continuación, seleccione Guardar.

Para obtener más información sobre cómo cambiar los permisos de los administradores de lagos de datos, consulte Crear un administrador de lagos de datos en la Guía para AWS Lake Formation desarrolladores.

El rol de IAM debe tener `SELECT` privilegios en la base de datos y las tablas a las que desea conceder acceso a un suscriptor. Para obtener instrucciones sobre cómo hacerlo, consulte la Guía para AWS Lake Formation desarrolladores sobre cómo conceder permisos al catálogo de datos mediante el método de recurso con nombre asignado.

Crear un suscriptor con acceso a las consultas en Security Lake

Elige el método que prefieras para crear un suscriptor con acceso a las consultas en la versión actual Región de AWS. Un suscriptor solo puede consultar los datos en los Región de AWS que se creó. Para crear un suscriptor, necesitarás tener el Cuenta de AWS ID y el ID externo del suscriptor. El ID externo es un identificador único que te proporciona el suscriptor. Para obtener más información sobre los ID externos, consulte Cómo usar un ID externo para conceder acceso a sus AWS recursos a un tercero en la Guía del usuario de IAM.

> **Note**
>
> Security Lake no admite la versión 1 del uso compartido de datos entre cuentas de Lake Formation. Debe actualizar a la versión 2 o 3 del uso compartido de datos entre cuentas de Lake Formation. Para ver los pasos para actualizar la configuración de la versión multicuenta a través de la AWS Lake Formation consola o la AWS CLI, consulte Para habilitar la nueva versión en la Guía para AWS Lake Formation desarrolladores.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.

   Inicie sesión en la cuenta de administrador delegado.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea crear el suscriptor.
3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, selecciona Crear suscriptor.
5. Para ver los detalles del suscriptor, introduce un nombre de suscriptor y una descripción opcional.

   La región se rellena automáticamente según la selección actual Región de AWS y no se puede modificar.
6. En el caso de las fuentes de registros y eventos, elija las fuentes que desea que Security Lake incluya al devolver los resultados de las consultas.
7. En el método de acceso a los datos, elija Lake Formation para crear un acceso de consulta para el suscriptor.

8. Para las credenciales del suscriptor, proporcione el Cuenta de AWS ID del suscriptor y el ID externo.
9. (Opcional) En el caso de las etiquetas, introduce hasta 50 etiquetas para asignárselas al suscriptor.

   Una etiqueta es una etiqueta que se puede definir y asignar a determinados tipos de AWS recursos. Cada etiqueta consta de una clave de etiqueta necesaria y un valor de etiqueta opcional. Las etiquetas pueden ayudarlo a identificar, clasificar y administrar los recursos de diferentes maneras. Para obtener más información, consulte Etiquetado de los recursos de Security Lake.
10. Seleccione Crear.

API

Para crear un suscriptor con acceso a las consultas mediante programación, utilice el CreateSubscriber funcionamiento de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/create-subscriber.html create-subscriber.

En tu solicitud, usa estos parámetros para especificar los siguientes ajustes para el suscriptor:

- En `accessTypes`, especifique `LAKEFORMATION`.
- Para `sources` ello, especifique cada fuente que desee que Security Lake incluya al devolver los resultados de la consulta.
- Para`subscriberIdentity`, especifique la AWS identidad y el identificador externo que utiliza el suscriptor para consultar los datos de origen.

El siguiente ejemplo crea un suscriptor con acceso de consulta en la AWS región actual para la identidad del suscriptor especificada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 129345678912,"externalId": 123456789012} \
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, "sourceVersion": 2.0}}] \
--subscriber-name subscriber name \
--access-types LAKEFORMATION
```

Configurar el uso compartido de tablas entre cuentas (paso de suscriptor)

Security Lake utiliza el uso compartido de tablas entre cuentas de Lake Formation para facilitar el acceso de los suscriptores a las consultas. Al crear un suscriptor con acceso a consultas en la consola, la API o la API de Security Lake AWS CLI, Security Lake comparte información sobre las tablas de Lake Formation relevantes con el suscriptor mediante la creación de un recurso compartido en AWS Resource Access Manager (AWS RAM).

Cuando realiza ciertos tipos de modificaciones en un suscriptor con acceso de consulta, Security Lake crea un nuevo recurso compartido. Para obtener más información, consulte Editar un suscriptor con acceso a consultas en Security Lake.

El suscriptor debe seguir estos pasos para consumir los datos de las tablas de Lake Formation:

1. Aceptar el recurso compartido: el suscriptor debe aceptar el recurso compartido que tenga `resourceShareArn` y `resourceShareName` que se genere al crear o editar el suscriptor. Elige uno de los siguientes métodos de acceso:
   - Para consolas y AWS CLI, consulta Aceptar una invitación para compartir recursos de AWS RAM.
   - Para la API, invoca la GetResourceShareInvitations API. Filtra por `resourceShareArn` y `resourceShareName` para encontrar el recurso compartido correcto. Acepta la invitación con la AcceptResourceShareInvitation API.

   La invitación para compartir recursos vence en 12 horas, por lo que debe validarla y aceptarla en un plazo de 12 horas. Si la invitación caduca, seguirás viéndola en ese `PENDING` estado, pero al aceptarla no tendrás acceso a los recursos compartidos. Cuando hayan pasado más de 12 horas, elimina al suscriptor de Lake Formation y vuelve a crearlo para recibir una nueva invitación para compartir recursos.
2. Cree un enlace de recursos a la base de datos compartida: el suscriptor debe crear un enlace de recursos a la base de datos compartida de Lake Formation en AWS Lake Formation (si usa la consola) o AWS Glue (si usa la API/AWS CLI). Este enlace de recursos dirige la cuenta del suscriptor a la base de datos compartida. Elija uno de los siguientes métodos de acceso:
   - Para la consola AWS CLI, consulte Crear un enlace de recursos a una base de datos de catálogo de datos compartida. en la Guía para AWS Lake Formation desarrolladores.
   - Recomendamos que los suscriptores también creen una base de datos única con la CreateDatabase API para almacenar las tablas de enlaces de recursos.

3. Consulte las tablas compartidas: servicios como Amazon Athena pueden hacer referencia a las tablas directamente y los nuevos datos que recopila Security Lake están disponibles automáticamente para su consulta. Las consultas se ejecutan en el Cuenta de AWS suscriptor y los costes derivados de las consultas se facturan al suscriptor. Puede controlar el acceso de lectura a los recursos en su propia cuenta de Security Lake.

Para obtener más información sobre la concesión de permisos entre cuentas, consulte el uso compartido de Cross-account datos en Lake Formation en la Guía para AWS Lake Formation desarrolladores.

Editar un suscriptor con acceso a consultas en Security Lake

Security Lake permite realizar modificaciones en un suscriptor con acceso a consultas. Puede editar el nombre, la descripción, el identificador externo, el principal (Cuenta de AWS ID) y las fuentes de registro del suscriptor que puede consumir. Elija el método que prefiera y siga los pasos para editar un suscriptor con acceso a las consultas en la Región de AWS actual.

> **Note**
>
> Security Lake no admite la versión 1 del uso compartido de datos entre cuentas de Lake Formation. Debe actualizar a la versión 2 o 3 del uso compartido de datos entre cuentas de Lake Formation. Para ver los pasos para actualizar la configuración de la versión multicuenta a través de la AWS Lake Formation consola o la AWS CLI, consulta Cómo habilitar la nueva versión en la Guía para AWS Lake Formation desarrolladores.

Console

En función de los detalles que desee editar, siga los pasos que se indican únicamente para esa acción.

Para editar el nombre del suscriptor

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.

   Inicie sesión en la cuenta de administrador delegado.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea editar los detalles del suscriptor.

3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, utilice el botón de opción para seleccionar el suscriptor que desee editar. El método de acceso a los datos del suscriptor seleccionado debe ser LAKEFORMATION.
5. Elija Editar.
6. Introduzca el nombre del nuevo suscriptor y seleccione Guardar.

Para editar la descripción del suscriptor

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/

   Inicie sesión en la cuenta de administrador delegado.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea editar el suscriptor.
3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, utilice el botón de opción para seleccionar el suscriptor que desee editar. El método de acceso a los datos del suscriptor seleccionado debe ser LAKEFORMATION.
5. Elija Editar.
6. Introduzca la nueva descripción del suscriptor y seleccione Guardar.

Para editar el ID externo

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/

   Inicie sesión en la cuenta de administrador delegado.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea editar los detalles del suscriptor.
3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, utilice el botón de opción para seleccionar el suscriptor que desee editar. El método de acceso a los datos del suscriptor seleccionado debe ser LAKEFORMATION.
5. Elija Editar.
6. Introduzca el nuevo ID externo que ha proporcionado el suscriptor y seleccione Guardar.

Al guardar el nuevo ID externo, se elimina automáticamente el AWS RAM recurso compartido anterior y se crea un nuevo recurso compartido para el suscriptor.

7. El suscriptor debe aceptar el nuevo recurso compartido siguiendo el paso 1 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor). Asegúrese de que el nombre de recurso de Amazon (ARN) que aparece en los detalles del suscriptor sea el mismo que el de la consola de Lake Formation. El enlace de recursos a las tablas compartidas no cambia, por lo que el suscriptor no tiene que crear un nuevo enlace de recursos.

Para editar el principal (Cuenta de AWS ID)

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.

   Inicie sesión en la cuenta de administrador delegado.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea editar los detalles del suscriptor.
3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, utilice el botón de opción para seleccionar el suscriptor que desee editar. El método de acceso a los datos del suscriptor seleccionado debe ser LAKEFORMATION.
5. Elija Editar.
6. Introduzca el ID del Cuenta de AWS del suscriptor y seleccione Guardar.

   Al guardar el nuevo identificador de cuenta, se elimina automáticamente el AWS RAM recurso compartido anterior, por lo que el director anterior no puede consumir las fuentes de registros y eventos. Security Lake crea un nuevo recurso compartido.
7. Con las credenciales de la nueva entidad principal, el suscriptor debe aceptar el nuevo recurso compartido y crear un enlace de recursos a las tablas compartidas. Esto le da a la nueva entidad principal acceso a los recursos compartidos. Para obtener instrucciones, consulte los pasos 1 y 2 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor). Asegúrese de que el ARN que aparece en los detalles del suscriptor sea el mismo que el de la consola de Lake Formation.

Para editar los orígenes de registros y eventos

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.

   Inicie sesión en la cuenta de administrador delegado.
2. Con el Región de AWS selector de la esquina superior derecha de la página, seleccione la región en la que desea editar los detalles del suscriptor.
3. En el panel de navegación izquierdo, elija Suscriptores.
4. En la página Suscriptores, utilice el botón de opción para seleccionar el suscriptor que desee editar. El método de acceso a los datos del suscriptor seleccionado debe ser LAKEFORMATION.
5. Elija Editar.
6. Anule la selección de orígenes existentes o elija las que desea agregar. Si anula la selección de un origen, no tiene que realizar ninguna otra acción por su parte. Si opta por añadir un origen, no se creará ninguna nueva invitación para compartir recursos. Sin embargo, Security Lake actualiza las tablas compartidas de Lake Formation en función de los orígenes añadidos. El suscriptor debe crear un enlace de recursos a las tablas compartidas actualizadas para poder consultar los datos de origen. Para obtener instrucciones, consulte el paso 2 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor).
7. Seleccione Save.

API

Para editar un suscriptor con acceso a las consultas mediante programación, utilice la API UpdateSubscriber de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando https://awscli.amazonaws.com/v2/documentation/api/latest/reference/securitylake/update-subscriber.html update-subscriber. En su solicitud, utilice los parámetros compatibles para especificar la siguiente configuración para el suscriptor:

- Para `subscriberName`, especifique el nombre del nuevo suscriptor.
- Para `subscriberDescription`, especifique la nueva descripción.
- Para ello`subscriberIdentity`, especifique el identificador principal (Cuenta de AWS ID) y el identificador externo que utilizará el suscriptor para consultar los datos de origen. Debe proporcionar la entidad principal y el ID externo. Si desea mantener uno de estos valores sin cambios, transfiera el valor actual.

- Actualizar solo el ID externo: esta acción elimina el recurso compartido de AWS RAM anterior y crea uno nuevo para el suscriptor. El suscriptor debe aceptar el nuevo recurso compartido siguiendo el paso 1 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor). El enlace de recursos a las tablas compartidas no cambia, por lo que el suscriptor no tiene que crear un nuevo enlace de recursos.
- Actualizar solo el principal: esta acción elimina el AWS RAM recurso compartido anterior para que el principal anterior no pueda consumir las fuentes de registro y de eventos. Security Lake crea un nuevo recurso compartido. Con las credenciales de la nueva entidad principal, el suscriptor debe aceptar el nuevo recurso compartido y crear un enlace de recursos a las tablas compartidas. Esto le da a la nueva entidad principal acceso a los recursos compartidos. Para obtener instrucciones, consulte los pasos 1 y 2 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor).

  Para actualizar el identificador externo y la entidad principal, siga los pasos 1 y 2 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor).

- Para `sources`, elimine los orígenes existentes o especifique los orígenes que desee añadir. Si elimina un origen, no tiene que realizar ninguna otra acción por su parte. Si añade un origen, no se creará ninguna nueva invitación para compartir recursos. Sin embargo, Security Lake actualiza las tablas compartidas de Lake Formation en función de los orígenes añadidos. El suscriptor debe crear un enlace de recursos a las tablas compartidas actualizadas para poder consultar los datos de origen. Para obtener instrucciones, consulte el paso 2 en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor).

Consultas de Security Lake

Puede consultar los datos que Security Lake almacena en AWS Lake Formation bases de datos y tablas. También puede crear suscriptores de terceros en la consola, la API o la AWS CLI de Security Lake. Los suscriptores de terceros también pueden consultar los datos de Lake Formation de los orígenes que especifique.

El administrador del lago de datos de Lake Formation debe conceder permisos de `SELECT` en las bases de datos y tablas pertinentes a la identidad de IAM que consulta los datos. También se debe crear un suscriptor en Security Lake antes de que pueda consultar los datos. Para obtener más información sobre cómo crear una suscriptor con acceso de consulta, lea Administración del acceso a las consultas para los suscriptores de Security Lake.

Consulta de datos con la configuración de retención

> La configuración del ciclo de vida de Amazon S3 afecta al tiempo que se conservan los datos, lo que, a su vez, afecta al tiempo en que se pueden realizar consultas. Si ha configurado los ajustes de retención en Security Lake, debe incluir un filtro basado en el tiempo en las consultas para garantizar que los conjuntos de resultados se centren en los archivos de datos que no hayan caducado. Para obtener más información sobre la retención de datos en Security Lake, consulte. Administración del ciclo de vida

Los ejemplos de consultas de las siguientes secciones incluyen filtros basados en el tiempo, como `eventDay` `otime_dt`, para demostrar esta práctica recomendada.

Temas

- Consultas de Security Lake para la versión 1 AWS de la fuente (OCSF 1.0.0-rc.2)
- Consultas de Security Lake para la versión 2 de la AWS fuente (OCSF 1.1.0)

Consultas de Security Lake para la versión 1 AWS de la fuente (OCSF 1.0.0-rc.2)

La siguiente sección proporciona orientación sobre la consulta de datos de Security Lake e incluye algunos ejemplos de consultas de AWS fuentes compatibles de forma nativa con la versión 1 de la fuente.AWS Estas consultas están diseñadas para recuperar datos de una forma específica.Región

de AWS Estos ejemplos utilizan us-east-1, es decir, Este de EE. UU. (Norte de Virginia). Además, las consultas de ejemplo utilizan un parámetro `LIMIT 25` que devuelve hasta 25 registros. Puede omitir este parámetro o ajustarlo según sus preferencias. Para ver más ejemplos, consulte el GitHub directorio de consultas OCSF de Amazon Security Lake.

Las siguientes consultas incluyen filtros basados en el tiempo que se utilizan `eventDay` para garantizar que la consulta se encuentra dentro de los ajustes de retención configurados. Para obtener más información, consulte Querying data with retention settings.

Por ejemplo, si los datos de más de 60 días han caducado, las consultas deben incluir restricciones de tiempo para impedir el acceso a los datos caducados. Para un período de retención de 60 días, incluye la siguiente cláusula en la consulta:

```
...
WHERE eventDay BETWEEN cast(date_format(current_date - INTERVAL '59' day, '%Y%m%d') AS
 varchar)
                  AND cast(date_format(current_date, '%Y%m%d') AS varchar)
...
```

Esta cláusula utiliza 59 días (en lugar de 60) para evitar cualquier superposición de datos o tiempo entre Amazon S3 y Apache Iceberg.

Tabla de orígenes de registro

Al consultar los datos de Security Lake, debe incluir el nombre de la tabla de Lake Formation en la que residen los datos.

```
SELECT *
   FROM
 amazon_security_lake_glue_db_DB_Region.amazon_security_lake_table_DB_Region_SECURITY_LAKE_TABL
   WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
   LIMIT 25
```

Los valores comunes de la tabla de orígenes de registro incluyen los siguientes:

- `cloud_trail_mgmt_1_0`— eventos AWS CloudTrail de gestión

- `lambda_execution_1_0`— eventos CloudTrail de datos para Lambda
- `s3_data_1_0`— eventos CloudTrail de datos para S3
- `route53_1_0`: registros de consultas de Amazon Route 53 Resolver
- `sh_findings_1_0`—AWS Security Hub CSPM hallazgos
- `vpc_flow_1_0`: registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)

Ejemplo: todos los resultados del CSPM de Security Hub de la tabla de la región **`sh_findings_1_0`** us-east-1

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
   LIMIT 25
```

Región de base de datos

Al consultar los datos de Security Lake, debe incluir el nombre de región de base de datos de la que está consultando datos. Para obtener una lista completa de las regiones de bases de datos en las que Security Lake está disponible actualmente, consulte Puntos de conexión de Amazon Security Lake.

Ejemplo: Listar AWS CloudTrail la actividad desde la IP de origen

En el siguiente ejemplo, se enumeran todas las CloudTrail actividades de la IP de origen *192.0.2.1* que se registraron después *20230301* (1 de marzo de 2023), en la tabla *cloud_trail_mgmt_1_0* del *us-east-1*DB_Region.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > '20230301' AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
```

```
    LIMIT 25
```

Fecha de partición

La partición de los datos le permite restringir el volumen de datos que explora cada consulta, lo que mejora el rendimiento y reduce los costos. Security Lake implementa la partición mediante `eventDay`, `region`, y parámetros `accountid`. Las particiones de `eventDay` utilizan el formato `YYYYMMDD`.

Este es un ejemplo de consulta que utiliza la partición de `eventDay`:

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
```

Los valores válidos de `eventDay` incluyen la siguiente información:

Eventos ocurridos en el último año

```
> cast(date_format(current_timestamp - INTERVAL '1' year, '%Y%m%d%H') as
varchar)
```

Eventos ocurridos en el último año

```
> cast(date_format(current_timestamp - INTERVAL '1' month, '%Y%m%d%H')
as varchar)
```

Eventos ocurridos en los últimos 30 días

```
> cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d%H') as
varchar)
```

Eventos ocurridos en las últimas 12 horas

```
> cast(date_format(current_timestamp - INTERVAL '12' hour, '%Y%m%d%H')
as varchar)
```

Eventos ocurridos en los últimos 5 minutos

```
> cast(date_format(current_timestamp - INTERVAL '5' minute, '%Y%m%d%H')
as varchar)
```

Eventos ocurridos entre hace 7 y 14 días

```
BETWEEN cast(date_format(current_timestamp - INTERVAL '14' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '7'
day, '%Y%m%d%H') as varchar)
```

Eventos ocurridos en una fecha específica o después de ella

```
>= '20230301'
```

Ejemplo: lista de todas las CloudTrail actividades de la IP de origen **192.0.2.1** realizadas a partir del 1 de marzo de 2023 en la tabla **cloud_trail_mgmt_1_0**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Ejemplo: lista de toda la CloudTrail actividad de la IP de origen **192.0.2.1** en los últimos 30 días en la tabla **cloud_trail_mgmt_1_0**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Ejemplo de consultas de CloudTrail datos de Security Lake

AWS CloudTrail rastrea la actividad de los usuarios y el uso de la API en Servicios de AWS. Los suscriptores pueden consultar CloudTrail los datos para obtener los siguientes tipos de información:

Estos son algunos ejemplos de consultas de CloudTrail datos para la versión 1 de AWS origen:

Intentos no autorizados Servicios de AWS en los últimos 7 días

```
SELECT
      time,
      api.service.name,
      api.operation,
      api.response.error,
      api.response.message,
      unmapped['responseElements'],
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND api.response.error in (
        'Client.UnauthorizedOperation',
        'Client.InvalidPermission.NotFound',
        'Client.OperationNotPermitted',
        'AccessDenied')
    ORDER BY time desc
    LIMIT 25
```

Lista de toda la CloudTrail actividad desde la IP de origen **`192.0.2.1`** en los últimos 7 días

```
SELECT
      api.request.uid,
      time,
      api.service.name,
      api.operation,
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
```

```
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '127.0.0.1.'
    ORDER BY time desc
    LIMIT 25
```

Lista de toda la actividad de IAM en los últimos 7 días

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND api.service.name = 'iam.amazonaws.com'
    ORDER BY time desc
    LIMIT 25
```

Instancias en las que se utilizó la credencial **`AIDACKCEVSQ6C2EXAMPLE`** en los últimos 7 días

```
SELECT
      actor.user.uid,
      actor.user.uuid,
      actor.user.account_uid,
      cloud.region
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
      LIMIT 25
```

Lista de CloudTrail registros fallidos en los últimos 7 días

```
SELECT
      actor.user.uid,
      actor.user.uuid,
```

```
      actor.user.account_uid,
      cloud.region
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE status='failed' and eventDay BETWEEN cast(date_format(current_timestamp -
 INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp -
 INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Ejemplo de consultas de Security Lake para los registros de consultas del solucionador de Route 53

Los registros de consultas de Amazon Route 53 Resolver rastrean las consultas de DNS realizadas por los recursos dentro de Amazon VPC. Los suscriptores pueden consultar los registros de consultas de Route 53 Resolver para obtener los siguientes tipos de información:

Estos son algunos ejemplos de consultas de los registros de consultas del solucionador de Route 53 para la versión 1 de AWS origen:

Lista de consultas de DNS CloudTrail de los últimos 7 días

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Lista de consultas de DNS que coinciden con **`s3.amazonaws.com`** en los últimos 7 días

```
SELECT
      time,
```

```
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answers
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE query.hostname LIKE 's3.amazonaws.com.' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Lista de consultas de DNS que no se resolvieron en los últimos 7 días

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answers
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE cardinality(answers) = 0 and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Lista de consultas de DNS que se resolvieron en **`192.0.2.1`** en los últimos 7 días

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answer.rdata
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
```

```
    CROSS JOIN UNNEST(answers) as st(answer)
    WHERE answer.rdata='192.0.2.1' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Ejemplo de consultas de Security Lake para encontrar información sobre el CSPM de Security Hub

Security Hub CSPM le proporciona una visión completa del estado de su seguridad y le ayuda a comprobar su entorno según los estándares AWS y las mejores prácticas del sector de la seguridad. Security Hub CSPM produce resultados para los controles de seguridad y recibe los resultados de servicios de terceros.

Estos son algunos ejemplos de consultas de las conclusiones del CSPM de Security Hub:

Nuevos resultados con una gravedad superior o igual a **`MEDIUM`** de los últimos 7 días

```
SELECT
      time,
      finding,
      severity
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0_fi
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND severity_id >= 3
      AND state_id = 1
    ORDER BY time DESC
    LIMIT 25
```

Resultados duplicados en los últimos 7 días

```
SELECT
    finding.uid,
    MAX(time) AS time,
    ARBITRARY(region) AS region,
    ARBITRARY(accountid) AS accountid,
    ARBITRARY(finding) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
```

```
FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H')
 as varchar)
GROUP BY finding.uid
LIMIT 25
```

Todos los resultados no informativos de los últimos 7 días

```
SELECT
      time,
      finding.title,
      finding,
      severity
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE severity != 'Informational' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Resultados dónde el recurso es un bucket de Amazon S3 (sin restricción de tiempo)

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE any_match(resources, element -> element.type = 'amzn-s3-demo-bucket')
   LIMIT 25
```

Resultados con una puntuación del sistema de clasificación de vulnerabilidades comunes (CVSS) superior a **1** (sin restricción de tiempo)

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE any_match(vulnerabilities, element -> element.cve.cvss.base_score > 1.0)
   LIMIT 25
```

Resultados que coinciden con las vulnerabilidades y exposiciones comunes (CVE) **CVE-0000-0000** (sin restricción de tiempo)

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
    LIMIT 25
```

Recuento de productos que han enviado conclusiones desde Security Hub (CSPM) en los últimos 7 días

```
SELECT
      metadata.product.feature.name,
      count(*)
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    GROUP BY metadata.product.feature.name
    ORDER BY metadata.product.feature.name DESC
    LIMIT 25
```

Recuento de los tipos de recursos incluidos en los resultados de los últimos 7 días

```
SELECT
      count(*),
      resource.type
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
        CROSS JOIN UNNEST(resources) as st(resource)
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    GROUP BY resource.type
    LIMIT 25
```

Paquetes vulnerables a causa de los resultados de los últimos 7 días

```
SELECT
      vulnerability
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0,
    UNNEST(vulnerabilities) as t(vulnerability)
```

```
    WHERE vulnerabilities is not null
    LIMIT 25
```

Resultados que han cambiado en los últimos 7 días

```
SELECT
    finding.uid,
    finding.created_time,
    finding.first_seen_time,
    finding.last_seen_time,
    finding.modified_time,
    finding.title,
    state
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    LIMIT 25
```

Ejemplo de consultas de Security Lake para Amazon VPC Flow Logs

Amazon Virtual Private Cloud (Amazon VPC) proporciona detalles acerca del tráfico IP entrante y saliente de las interfaces de red en su VPC.

Estos son algunos ejemplos de consultas de los registros de flujo de Amazon VPC para la versión de AWS origen 1:

Tráfico específico de Regiones de AWS los últimos 7 días

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND region in ('us-east-1','us-east-2','us-west-2')
    LIMIT 25
```

Lista de actividad de la IP **`192.0.2.1`** y el puerto de origen **`22`** en los últimos 7 días

```
SELECT *
```

```
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND src_endpoint.ip = '192.0.2.1'
      AND src_endpoint.port = 22
    LIMIT 25
```

Recuento de direcciones IP de destino distintas en los últimos 7 días

```
SELECT
    COUNT(DISTINCT dst_endpoint.ip)
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    LIMIT 25
```

Tráfico originado en 198.51.100.0/24 en los últimos 7 días

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND split_part(src_endpoint.ip,'.', 1)='198'AND split_part(src_endpoint.ip,'.',
 2)='51'
    LIMIT 25
```

Todo el tráfico HTTPS de los últimos 7 días

```
SELECT
      dst_endpoint.ip as dst,
      src_endpoint.ip as src,
      traffic.packets
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      dst_endpoint.ip,
      traffic.packets,
      src_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

Ordenado por número de paquetes para las conexiones destinadas al puerto **443** en los últimos 7 días

```
SELECT
      traffic.packets,
      dst_endpoint.ip
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      traffic.packets,
      dst_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

Todo el tráfico entre las IP **192.0.2.1** y **192.0.2.2** en los últimos 7 días

```
SELECT
      start_time,
      end_time,
      src_endpoint.interface_uid,
      connection_info.direction,
      src_endpoint.ip,
      dst_endpoint.ip,
      src_endpoint.port,
      dst_endpoint.port,
      traffic.packets,
      traffic.bytes
```

```
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND(
        src_endpoint.ip = '192.0.2.1'
        AND dst_endpoint.ip = '192.0.2.2')
      OR (
        src_endpoint.ip = '192.0.2.2'
        AND dst_endpoint.ip = '192.0.2.1')
    ORDER BY start_time ASC
    LIMIT 25
```

Todo el tráfico entrante de los últimos 7 días

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'ingress'
    LIMIT 25
```

Todo el tráfico saliente de los últimos 7 días

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'egress'
    LIMIT 25
```

Todo el tráfico rechazado de los últimos 7 días

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND type_uid = 400105
    LIMIT 25
```

Consultas de Security Lake para la versión 2 de la AWS fuente (OCSF 1.1.0)

La siguiente sección proporciona orientación sobre la consulta de datos de Security Lake e incluye algunos ejemplos de consultas de AWS fuentes compatibles de forma nativa con la versión 2 de la fuente.AWS Estas consultas están diseñadas para recuperar datos de una forma específica.Región de AWS Estos ejemplos utilizan us-east-1, es decir, Este de EE. UU. (Norte de Virginia). Además, las consultas de ejemplo utilizan un parámetro `LIMIT 25` que devuelve hasta 25 registros. Puede omitir este parámetro o ajustarlo según sus preferencias. Para ver más ejemplos, consulte el GitHub directorio de consultas OCSF de Amazon Security Lake.

Puede consultar los datos que Security Lake almacena en AWS Lake Formation bases de datos y tablas. También puede crear suscriptores de terceros en la consola, la API o la AWS CLI de Security Lake. Los suscriptores de terceros también pueden consultar los datos de Lake Formation de los orígenes que especifique.

El administrador del lago de datos de Lake Formation debe conceder permisos de `SELECT` en las bases de datos y tablas pertinentes a la identidad de IAM que consulta los datos. También se debe crear un suscriptor en Security Lake antes de que pueda consultar los datos. Para obtener más información sobre cómo crear una suscriptor con acceso de consulta, lea Administración del acceso a las consultas para los suscriptores de Security Lake.

Las siguientes consultas incluyen filtros basados en el tiempo que se utilizan `eventDay` para garantizar que la consulta se encuentra dentro de los ajustes de retención configurados. Para obtener más información, consulte Querying data with retention settings.

Por ejemplo, si los datos de más de 60 días han caducado, las consultas deben incluir restricciones de tiempo para impedir el acceso a los datos caducados. Para un período de retención de 60 días, incluye la siguiente cláusula en la consulta:

```
...
WHERE time_dt > DATE_ADD('day', -59, CURRENT_TIMESTAMP)
```

```
...
```

Esta cláusula utiliza 59 días (en lugar de 60) para evitar cualquier superposición de datos o tiempo entre Amazon S3 y Apache Iceberg.

Tabla de orígenes de registro

Al consultar los datos de Security Lake, debe incluir el nombre de la tabla de Lake Formation en la que residen los datos.

```
SELECT *
FROM
 "amazon_security_lake_glue_db_DB_Region"."amazon_security_lake_table_DB_Region_SECURITY_LAKE_T
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Los valores comunes de la tabla de orígenes de registro incluyen los siguientes:

- `cloud_trail_mgmt_2_0`— eventos AWS CloudTrail de gestión
- `lambda_execution_2_0`— eventos CloudTrail de datos para Lambda
- `s3_data_2_0`— eventos CloudTrail de datos para S3
- `route53_2_0`: registros de consultas de Amazon Route 53 Resolver
- `sh_findings_2_0`—AWS Security Hub CSPM hallazgos
- `vpc_flow_2_0`: registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)
- `eks_audit_2_0`— Registros de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS)
- `waf_2_0`— Registros de la versión 2 AWS WAF

Ejemplo: todos los resultados del CSPM de Security Hub de la tabla de la región **`sh_findings_2_0`** us-east-1

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Región de base de datos

Al consultar los datos de Security Lake, debe incluir el nombre de región de base de datos de la que está consultando datos. Para obtener una lista completa de las regiones de bases de datos en las que Security Lake está disponible actualmente, consulte Puntos de conexión de Amazon Security Lake.

Ejemplo: Listar la actividad de Amazon Virtual Private Cloud desde la IP de origen

En el siguiente ejemplo, se enumeran todas las actividades de Amazon VPC desde la IP de origen *192.0.2.1* que se registraron después *20230301* (1 de marzo de 2023), en la tabla *vpc_flow_2_0* del. *us-west-2* DB_Region

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
    WHERE time_dt > TIMESTAMP '2023-03-01'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time_dt desc
LIMIT 25
```

Fecha de partición

La partición de los datos le permite restringir el volumen de datos que explora cada consulta, lo que mejora el rendimiento y reduce los costos. Las particiones funcionan de forma ligeramente diferente en Security Lake 2.0 en comparación con Security Lake 1.0. Security Lake ahora implementa la partición mediante `time_dtregion`, `yaccountid`. Por su parte, Security Lake 1.0 implementó la partición mediante `eventDay` parámetros`region`, `yaccountid`.

Las consultas `time_dt` generarán automáticamente las particiones de fecha de S3 y se pueden consultar como cualquier campo basado en el tiempo en Athena.

Este es un ejemplo de consulta que utiliza la `time_dt` partición para consultar los registros después del 1 de marzo de 2023:

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt > TIMESTAMP '2023-03-01'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
```

```
LIMIT 25
```

Los valores válidos de `time_dt` incluyen la siguiente información:

Eventos ocurridos en el último año

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' YEAR
```

Eventos ocurridos en el último año

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' MONTH
```

Eventos ocurridos en los últimos 30 días

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '30' DAY
```

Eventos ocurridos en las últimas 12 horas

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '12' HOUR
```

Eventos ocurridos en los últimos 5 minutos

```
  WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '5' MINUTE
```

Eventos ocurridos entre hace 7 y 14 días

```
  WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '14' DAY AND
  CURRENT_TIMESTAMP - INTERVAL '7' DAY
```

Eventos ocurridos en una fecha específica o después de ella

```
  WHERE time_dt >= TIMESTAMP '2023-03-01'
```

Ejemplo: lista de toda la CloudTrail actividad desde la IP de origen a **`192.0.2.1`** partir del 1 de marzo de 2023 en la tabla **`cloud_trail_mgmt_1_0`**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Ejemplo: lista de toda la CloudTrail actividad de la IP de origen **`192.0.2.1`** en los últimos 30 días en la tabla **`cloud_trail_mgmt_1_0`**

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Consultando los observables de Security Lake

Observables es una nueva función que ahora está disponible en Security Lake 2.0. El objeto observable es un elemento fundamental que contiene información relacionada que se encuentra en muchos lugares del evento. La consulta de los observables permite a los usuarios obtener información de seguridad de alto nivel a partir de sus conjuntos de datos.

Al consultar elementos específicos dentro de los observables, puede restringir los conjuntos de datos a datos como nombres de usuario específicos, recursos UIDs IPs, hashes y otra información de tipo IOC

Este es un ejemplo de consulta que utiliza la matriz observables para consultar los registros en las tablas VPC Flow y Route53 que contienen el valor IP '172.01.02.03'

```
WITH a AS
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip'),
b as
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
    UNNEST(observables) AS t(observable)
```

```
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip')
SELECT * FROM a
LEFT JOIN b ON a.value=b.value and a.name=b.name
LIMIT 25
```

CloudTrail Ejemplo de consultas de datos de Security Lake

AWS CloudTrail rastrea la actividad de los usuarios y el uso de la API en Servicios de AWS. Los suscriptores pueden consultar CloudTrail los datos para obtener los siguientes tipos de información:

Estos son algunos ejemplos de consultas de CloudTrail datos para la versión 2 de AWS origen:

Intentos no autorizados Servicios de AWS en los últimos 7 días

```
SELECT
    time_dt,
    api.service.name,
    api.operation,
    api.response.error,
    api.response.message,
    api.response.data,
    cloud.region,
    actor.user.uid,
    src_endpoint.ip,
    http_request.user_agent
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.response.error in (
    'Client.UnauthorizedOperation',
    'Client.InvalidPermission.NotFound',
    'Client.OperationNotPermitted',
    'AccessDenied')
ORDER BY time desc
LIMIT 25
```

Lista de toda la CloudTrail actividad desde la IP de origen **`192.0.2.1`** en los últimos 7 días

```
SELECT
    api.request.uid,
```

```
    time_dt,
    api.service.name,
    api.operation,
    cloud.region,
    actor.user.uid,
    src_endpoint.ip,
    http_request.user_agent
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1.'
ORDER BY time desc
LIMIT 25
```

Lista de toda la actividad de IAM en los últimos 7 días

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.service.name = 'iam.amazonaws.com'
ORDER BY time desc
LIMIT 25
```

Instancias en las que se utilizó la credencial **`AIDACKCEVSQ6C2EXAMPLE`** en los últimos 7 días

```
SELECT
      actor.user.uid,
      actor.user.uid_alt,
      actor.user.account.uid,
      cloud.region
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
LIMIT 25
```

Lista de CloudTrail registros fallidos en los últimos 7 días

```
SELECT
      actor.user.uid,
      actor.user.uid_alt,
```

```
      actor.user.account.uid,
      cloud.region
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE status='failed' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND
 CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Ejemplos de consultas para los registros de consultas de Route 53 Resolver

Los registros de consultas de Amazon Route 53 Resolver rastrean las consultas de DNS realizadas por los recursos dentro de Amazon VPC. Los suscriptores pueden consultar los registros de consultas de Route 53 Resolver para obtener los siguientes tipos de información:

Estos son algunos ejemplos de consultas de los registros de consultas de reresolución de Route 53 para la versión 2 de AWS origen:

Lista de consultas de DNS de los CloudTrail últimos 7 días

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Lista de consultas de DNS que coinciden con **`s3.amazonaws.com`** en los últimos 7 días

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
```

```
    query.hostname,
    rcode,
    answers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE query.hostname LIKE 's3.amazonaws.com.' and time_dt BETWEEN CURRENT_TIMESTAMP -
 INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Lista de consultas de DNS que no se resolvieron en los últimos 7 días

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE cardinality(answers) = 0 and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
 AND CURRENT_TIMESTAMP
LIMIT 25
```

Lista de consultas de DNS que se resolvieron en **`192.0.2.1`** en los últimos 7 días

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answer.rdata
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
UNNEST(answers) as st(answer)
WHERE answer.rdata='192.0.2.1'
AND time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Ejemplo de consultas de Security Lake para encontrar información sobre el CSPM de Security Hub

Security Hub CSPM le proporciona una visión completa del estado de su seguridad y le ayuda a comprobar su entorno según los estándares AWS y las mejores prácticas del sector de la seguridad. Security Hub CSPM produce resultados para los controles de seguridad y recibe los resultados de servicios de terceros.

Estos son algunos ejemplos de consultas de los hallazgos de CSPM de Security Hub para la versión 2 AWS de origen:

Nuevos resultados con una gravedad superior o igual a **`MEDIUM`** de los últimos 7 días

```
SELECT
    time_dt,
    finding_info,
    severity_id,
    status
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND severity_id >= 3
    AND status = 'New'
ORDER BY time DESC
LIMIT 25
```

Resultados duplicados en los últimos 7 días

```
SELECT
    finding_info.uid,
    MAX(time_dt) AS time,
    ARBITRARY(region) AS region,
    ARBITRARY(accountid) AS accountid,
    ARBITRARY(finding_info) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY finding_info.uid
LIMIT 25
```

Todos los resultados no informativos de los últimos 7 días

```
SELECT
    time_dt,
    finding_info.title,
    finding_info,
    severity
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE severity != 'Informational' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7'
 DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Resultados dónde el recurso es un bucket de Amazon S3 (sin restricción de tiempo)

```
SELECT *
   FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(resources, element -> element.type = 'amzn-s3-demo-bucket')
LIMIT 25
```

Resultados con una puntuación del sistema de clasificación de vulnerabilidades comunes (CVSS) superior a **1** (sin restricción de tiempo)

```
SELECT
    DISTINCT finding_info.uid
    time_dt,
    metadata,
    finding_info,
    vulnerabilities,
    resource
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
UNNEST(vulnerabilities) AS t(vulnerability),
UNNEST(vulnerability.cve.cvss) AS t(cvs)
WHERE cvs.base_score > 1.0
AND vulnerabilities is NOT NULL
LIMIT 25
```

Resultados que coinciden con las vulnerabilidades y exposiciones comunes (CVE) **CVE-0000-0000** (sin restricción de tiempo)

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
LIMIT 25
```

Recuento de productos que han enviado conclusiones desde Security Hub (CSPM) en los últimos 7 días

```
SELECT
    metadata.product.name,
    count(*)
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY metadata.product.name
ORDER BY metadata.product.name DESC
LIMIT 25
```

Recuento de los tipos de recursos incluidos en los resultados de los últimos 7 días

```
SELECT
    count(*) AS "Total",
    resource.type
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY resource.type
ORDER BY count(*) DESC
LIMIT 25
```

Paquetes vulnerables a causa de los resultados de los últimos 7 días

```
SELECT
    vulnerabilities
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND vulnerabilities is NOT NULL
LIMIT 25
```

Resultados que han cambiado en los últimos 7 días

```
SELECT
    status,
    finding_info.title,
    finding_info.created_time_dt,
    finding_info,
    finding_info.uid,
    finding_info.first_seen_time_dt,
    finding_info.last_seen_time_dt,
    finding_info.modified_time_dt
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Ejemplo de consultas de Security Lake para Amazon VPC Flow Logs

Amazon Virtual Private Cloud (Amazon VPC) proporciona detalles acerca del tráfico IP entrante y saliente de las interfaces de red en su VPC.

Estos son algunos ejemplos de consultas de los registros de flujo de Amazon VPC para la versión 2 AWS de origen:

Tráfico específico de Regiones de AWS los últimos 7 días

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND region in ('us-east-1','us-east-2','us-west-2')
LIMIT 25
```

Lista de actividad de la IP **`192.0.2.1`** y el puerto de origen **`22`** en los últimos 7 días

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1'
AND src_endpoint.port = 22
```

```
LIMIT 25
```

Recuento de direcciones IP de destino distintas en los últimos 7 días

```
SELECT
    COUNT(DISTINCT dst_endpoint.ip) AS "Total"
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Tráfico originado en 198.51.100.0/24 en los últimos 7 días

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND split_part(src_endpoint.ip,'.', 1)='198'AND split_part(src_endpoint.ip,'.', 2)='51'
LIMIT 25
```

Todo el tráfico HTTPS de los últimos 7 días

```
SELECT
    dst_endpoint.ip as dst,
    src_endpoint.ip as src,
    traffic.packets
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    dst_endpoint.ip,
    traffic.packets,
    src_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Ordenado por número de paquetes para las conexiones destinadas al puerto **443** en los últimos 7 días

```
SELECT
    traffic.packets,
```

```
    dst_endpoint.ip
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    traffic.packets,
    dst_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

Todo el tráfico entre las IP **`192.0.2.1`** y **`192.0.2.2`** en los últimos 7 días

```
SELECT
    start_time_dt,
    end_time_dt,
    src_endpoint.interface_uid,
    connection_info.direction,
    src_endpoint.ip,
    dst_endpoint.ip,
    src_endpoint.port,
    dst_endpoint.port,
    traffic.packets,
    traffic.bytes
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND(
    src_endpoint.ip = '192.0.2.1'
AND dst_endpoint.ip = '192.0.2.2')
OR (
    src_endpoint.ip = '192.0.2.2'
AND dst_endpoint.ip = '192.0.2.1')
ORDER BY start_time_dt ASC
LIMIT 25
```

Todo el tráfico entrante de los últimos 7 días

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Inbound'
```

```
LIMIT 25
```

Todo el tráfico saliente de los últimos 7 días

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Outbound'
LIMIT 25
```

Todo el tráfico rechazado de los últimos 7 días

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND action = 'Denied'
LIMIT 25
```

Ejemplo de consultas de Security Lake para los registros de auditoría de Amazon EKS

Los registros de Amazon EKS rastrean la actividad del plano de control y proporcionan registros de auditoría y diagnóstico directamente desde el plano de control de Amazon EKS a CloudWatch los registros de su cuenta. Estos registros hacen que le resulte más fácil asegura y ejecutar los clústeres. Los suscriptores pueden consultar los registros de EKS para obtener los siguientes tipos de información.

Estos son algunos ejemplos de consultas de los registros de auditoría de Amazon EKS para la versión 2 de AWS origen:

Solicitudes a una URL específica en los últimos 7 días

```
SELECT
    time_dt,
    actor.user.name,
    http_request.url.path,
    activity_name
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
```

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND activity_name = 'get'
and http_request.url.path = '/apis/coordination.k8s.io/v1/'
LIMIT 25
```

Actualice las solicitudes de «10.0.97.167» durante los últimos 7 días

```
SELECT
    activity_name,
    time_dt,
    api.request,
    http_request.url.path,
    src_endpoint.ip,
    resources
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '10.0.97.167'
AND activity_name = 'Update'
LIMIT 25
```

Solicitudes y respuestas asociadas al recurso 'kube-controller-manager' durante los últimos 7 días

```
SELECT
    activity_name,
    time_dt,
    api.request,
    api.response,
    resource.name
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0",
UNNEST(resources) AS t(resource)
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND resource.name = 'kube-controller-manager'
LIMIT 25
```

Ejemplo de consultas de Security Lake para registros de la AWS WAF versión 2

AWS WAF es un firewall de aplicaciones web que puede utilizar para supervisar las solicitudes web que los usuarios finales envían a sus aplicaciones y para controlar el acceso a su contenido.

Estos son algunos ejemplos de consultas de los registros de la versión AWS WAF 2 de la versión 2 de AWS origen:

Publica solicitudes desde una IP de origen específica durante los últimos 7 días

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    http_request.http_headers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '100.123.123.123'
AND activity_name = 'Post'
LIMIT 25
```

Solicitudes que coincidieron con un tipo de firewall MANAGED_RULE_GROUP durante los últimos 7 días

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type,
    firewall_rule.condition,
    firewall_rule.match_location,
    firewall_rule.match_details,
    firewall_rule.rate_limit
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND firewall_rule.type = 'MANAGED_RULE_GROUP'
LIMIT 25
```

Solicitudes que coincidieron con una expresión regular de una regla de firewall durante los últimos 7 días

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type,
    firewall_rule.condition,
    firewall_rule.match_location,
    firewall_rule.match_details,
    firewall_rule.rate_limit
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND firewall_rule.condition = 'REGEX'
LIMIT 25
```

Se denegaron las solicitudes de AWS credenciales que activaron la AWS WAF regla en los últimos 7 días

```
SELECT
    time_dt,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND http_request.url.path = '/.aws/credentials'
AND action = 'Denied'
LIMIT 25
```

Obtenga solicitudes de AWS credenciales agrupadas por país durante los últimos 7 días

```
SELECT count(*) as Total,
    src_endpoint.location.country AS Country,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
    AND CURRENT_TIMESTAMP
    AND activity_name = 'Get'
    AND http_request.url.path = '/.aws/credentials'
GROUP BY src_endpoint.location.country,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
```

Administración del ciclo de vida en Security Lake

Puede personalizar Security Lake para almacenar los datos en su lugar preferido Regiones de AWS durante el período de tiempo que prefiera. La administración del ciclo de vida puede ayudarle a cumplir con diferentes requisitos de conformidad.

Administración de retención

Para administrar los datos de manera que se almacenen de forma rentable, puede configurar la retención de los datos mediante los ajustes del ciclo de vida de Security Lake. Esta configuración de retención le ayuda a especificar la clase de almacenamiento de Amazon S3 que prefiera y el período de tiempo durante el cual los objetos de Amazon S3 permanecerán en esa clase de almacenamiento antes de que pasen a otra clase de almacenamiento y caduquen.

> **Warning**
>
> Recomendamos administrar la configuración de retención a través de la consola, la API o la CLI de Security Lake. Esto se debe a que modificar la configuración del ciclo de vida de Amazon S3 directamente en el servicio Amazon S3 puede eliminar metadatos e impedir que acceda a sus datos.

Consideraciones importantes sobre la configuración de retención en Security Lake

Tenga en cuenta las siguientes consideraciones a la hora de gestionar la retención de datos en Security Lake:

- Security Lake no es compatible con Amazon S3 Object Lock. Cuando se crean los buckets del lago de datos, el bloqueo de objetos de S3 está desactivado de forma predeterminada. Al habilitar S3 Object Lock con el modo de retención predeterminado, se interrumpe la entrega de datos de registro normalizados al lago de datos.
- La clase de almacenamiento predeterminada de Amazon S3 es S3 Standard. Si no configura los ajustes de retención, Security Lake utiliza los ajustes predeterminados para una configuración del ciclo de vida de Amazon S3: almacene los datos de forma indefinida mediante la clase de almacenamiento S3 Standard.

- En Security Lake, puede especificar la configuración de retención a nivel de región. Por ejemplo, puede configurar todos los objetos de S3 en una clase específica Región de AWS para que pasen a la clase de almacenamiento S3 Standard-IA 30 días después de que se hayan escrito en el lago de datos.
- Si bien la configuración de retención se aplica únicamente a los datos almacenados en el depósito de S3, los metadatos de Apache Iceberg están excluidos de la política de retención.

Configurar los ajustes de retención al activar Security Lake

Siga estas instrucciones para configurar los ajustes de retención para una o más regiones cuando se incorpore a Security Lake.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Cuando llegue al Paso 2: definir el objetivo del flujo de trabajo de incorporación, elija Añadir transición en Seleccionar clases de almacenamiento. A continuación, elija la clase de almacenamiento de Amazon S3 a la que desea pasar objetos de S3. (La clase de almacenamiento predeterminada, que no aparece indicada, es S3 Standard). Especifique también un período de retención (en días) para esa clase de almacenamiento. Para realizar la transición de los objetos a otra clase de almacenamiento después de ese tiempo, seleccione Añadir transición e introduzca la configuración para la clase de almacenamiento y el período de retención subsiguientes.
3. Para especificar cuándo quiere que caduquen los objetos de S3, elija Añadir transición. A continuación, para la clase de almacenamiento, elija Expirar. Para el periodo de retención, especifique el número total de días que desea almacenar los objetos en Amazon S3, utilizando cualquier clase de almacenamiento, una vez creados los objetos. Una vez finalizado el período, los objetos caducan y Amazon S3 los elimina.
4. Cuando haya terminado, elija Siguiente.

   Los cambios se aplicarán a todas las regiones en las que activó Security Lake durante los pasos de incorporación anteriores.

API

Para configurar los ajustes de retención mediante programación al incorporarse a Security Lake, utilice el CreateDataLakefuncionamiento de la API de Security Lake. Si utiliza la AWS CLI,

ejecute el comando create-data-lake. Especifique la configuración de retención que desee en los `lifecycleConfiguration` parámetros de la siguiente manera:

- Para `transitions`, especifique el número total de días (`days`) que desea almacenar los objetos de S3 en una clase de almacenamiento de Amazon S3 determinada (`storageClass`).
- Para `expiration`, especifique el número total de días que desea almacenar los objetos en Amazon S3, utilizando cualquier clase de almacenamiento, una vez creados los objetos. Una vez finalizado el período, los objetos caducan y Amazon S3 los elimina.

Security Lake aplica la configuración a la región que especifique en el campo `region` del objeto `configurations`.

Por ejemplo, el siguiente comando habilita Security Lake en la `us-east-1` región. En esta región, los objetos caducan después de 365 días y los objetos pasan a la clase de almacenamiento `ONEZONE_IA` S3 después de 60 días. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:securitylake:ap-
northeast-2:123456789012:data-lake/default"
```

Actualización de la configuración de retención

Siga estas instrucciones para actualizar la configuración de retención de una o más regiones después de activar Security Lake.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, elija Regiones.
3. Seleccione una región y, a continuación, elija Editar.

4. En la sección Seleccionar clases de almacenamiento, introduzca la configuración que desee. Para la clase de almacenamiento, elija la clase de almacenamiento de Amazon S3 a la que desea pasar objetos de S3. (La clase de almacenamiento predeterminada, que no aparece indicada, es S3 Standard). Para el periodo de retención, introduzca el número de días que desea almacenar objetos en esa clase de almacenamiento. Puede especificar varias transiciones.

   Para especificar también cuándo quiere que caduquen los objetos de S3, elija Expirar como clase de almacenamiento. Después, para el periodo de retención, especifique el número total de días que desea almacenar los objetos en Amazon S3, utilizando cualquier clase de almacenamiento, una vez creados los objetos. Una vez finalizado el período, los objetos caducan y Amazon S3 los elimina.

5. Cuando termine, elija Guardar.

API

Para actualizar la configuración de retención mediante programación, utilice el UpdateDataLakefuncionamiento de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el update-data-lakecomando. En la solicitud, utilice el `lifecycleConfiguration` parámetro para especificar la nueva configuración:

- Para cambiar la configuración de transición, utilice los parámetros `transitions` para especificar cada nuevo período de tiempo en días (`days`) en el que desee almacenar los objetos de S3 en una clase de almacenamiento de Amazon S3 determinada (`storageClass`).
- Para cambiar el período de retención general, utilice el parámetro `expiration` para especificar el número total de días que desea almacenar los objetos de S3, utilizando cualquier clase de almacenamiento, una vez creados los objetos. Una vez finalizado el período de retención, los objetos caducan y Amazon S3 los elimina.

Security Lake aplica la configuración a la región que especifique en el campo `region` del objeto `configurations`.

El `UpdateDataLake` funcionamiento de la API de Security Lake funciona como una operación «secundaria» que realiza una inserción si el elemento o registro especificado no existe, o una actualización si ya existe. Security Lake almacena de forma segura sus datos en reposo mediante soluciones de AWS cifrado.

Si se omite la clave `encryptionConfiguration` de una región incluida en una llamada de actualización que actualmente usa KMS, se mantendrá la clave de KMS de esa región en su lugar, pero si se especifica una clave, se restablecerá la clave en la misma región.

Por ejemplo, el siguiente AWS CLI comando actualiza la configuración de caducidad de los datos y la configuración de transición al almacenamiento de la `us-east-1` región. En esta región, los objetos caducan después de 500 días y los objetos pasan a la clase de almacenamiento `ONEZONE_IA` S3 después de 30 días. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:securitylake:ap-
northeast-2:123456789012:data-lake/default"
```

Regiones acumulativas

Una región acumulativa consolida los datos de una o más regiones contribuyentes. Esto puede ayudarle a cumplir con los requisitos de conformidad con los datos regionales.

Para obtener instrucciones sobre cómo configurar las regiones acumulables, consulte. Configuración de regiones acumulativas en Security Lake

Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake

¿Qué es OCSF?

El Open Cybersecurity Schema Framework (OCSF) es un esfuerzo colaborativo AWS y de código abierto realizado por socios líderes de la industria de la ciberseguridad. El OCSF proporciona un esquema estándar para los eventos de seguridad comunes, define los criterios de control de versiones para facilitar la evolución del esquema e incluye un proceso de autogobierno para los productores y consumidores de registros de seguridad. El código fuente público de OCSF está alojado en. GitHub

Security Lake convierte automáticamente los registros y eventos que provienen de un esquema de OCSF compatible de forma nativa Servicios de AWS. Tras la conversión a OCSF, Security Lake almacena los datos en un depósito de Amazon Simple Storage Service (Amazon S3) (un depósito Región de AWS por depósito) en su servidor.Cuenta de AWS Los registros y eventos que se escriben en Security Lake desde fuentes personalizadas deben seguir el esquema OCSF y el formato Apache Parquet. Los suscriptores pueden tratar los registros y eventos como registros genéricos de Parquet o aplicar la clase de eventos del esquema OCSF para interpretar con mayor precisión la información contenida en un registro.

Clases de eventos de OCSF

Los registros y eventos de un origen de Security Lake determinada coinciden con una clase de evento específica definida en OCSF. La actividad de DNS, la actividad de SSH y la autenticación son ejemplos de clases de eventos en OCSF. Puede especificar la clase de evento que coincide con un origen determinado.

Identificación del origen de OCSF

El OCSF utiliza una variedad de campos para ayudarle a determinar dónde se originó un conjunto específico de registros o eventos. Estos son los valores de los campos relevantes Servicios de AWS que Security Lake admite de forma nativa como fuentes.

`The OCSF source identification for AWS log sources (Version 1) are listed in the following table.`

origen	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.versión
CloudTrail Eventos de datos Lambda	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail Eventos de gestión	CloudTrail	AWS	Management	API Activity, Authentication o Account Change	1.0.0-rc.2
CloudTrail Eventos de datos de S3	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.0.0-rc.2
CSPM de Security Hub	Security Hub CSPM	AWS	Coincide con el valor CSPM de ProductName Security Hub	Security Finding	1.0.0-rc.2
Logs de flujo de VPC	Amazon VPC	AWS	Flowlogs	Network Activity	1.0.0-rc.2

The OCSF source identification for AWS log sources (Version 2) are listed in the following table.

origen	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.versión
CloudTrail Eventos de datos Lambda	`CloudTrail`	`AWS`	`Data`	`API Activity`	`1.1.0`
CloudTrail Eventos de gestión	`CloudTrail`	`AWS`	`Management`	`API Activity, Authentication o Account Change`	`1.1.0`
CloudTrail Eventos de datos de S3	`CloudTrail`	`AWS`	`Data`	`API Activity`	`1.1.0`
Route 53	`Route 53`	`AWS`	`Resolver Query Logs`	`DNS Activity`	`1.1.0`
CSPM de Security Hub	AWS Coincide con el valor del formato de búsqueda de seguridad (ASFF) `ProductName`	AWS Coincide con el valor del formato de búsqueda de seguridad (ASFF) `CompanyName`	Coincide con `featureName` el valor del ASFF `ProductFields`	`Vulnerability Finding, Compliance Finding, or Detection Finding`	`1.1.0`
Logs de flujo de VPC	`Amazon VPC`	`AWS`	`Flowlogs`	`Network Activity`	`1.1.0`

origen	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.versión
Registros de auditoría de EKS	`Amazon EKS`	`AWS`	`Elastic Kubernetes Service`	`API Activity`	`1.1.0`
AWS WAF Registros v2	`AWS WAF`	`AWS`	—	`HTTP Activity`	`1.1.0`

Integraciones con Security Lake

Amazon Security Lake se integra con productos de otros fabricantes Servicios de AWS y de terceros. Las integraciones pueden enviar datos a Security Lake como origen o consumirlos en Security Lake como suscriptor. En los siguientes temas se explican qué productos Servicios de AWS y los de terceros se integran con Security Lake.

Temas

- Servicio de AWS integraciones con Security Lake
- Third-party integraciones con Security Lake

Servicio de AWS integraciones con Security Lake

Amazon Security Lake se integra con otros Servicios de AWS. Un servicio puede funcionar como una integración de origen, una integración de suscriptor o ambas.

Las integraciones de origen tienen las siguientes propiedades:

- Envío de los datos a Security Lake
- Los datos llegan al esquema de Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake
- Los datos llegan en formato Apache Parquet

Las integraciones de suscriptores pueden acceder a los datos de Security Lake de una de las siguientes maneras:

- Lea los datos de origen de Security Lake a través de un punto final HTTPS
- Lea los datos fuente de Security Lake a través de un Amazon Simple Queue Service (Amazon SQS)
- Consultando directamente los datos de origen mediante AWS Lake Formation

La siguiente tabla proporciona una lista de Servicio de AWS las integraciones compatibles con Security Lake.

Servicio de AWS	Tipo de integración	Description (Descripción)	Cómo funciona la integración
Amazon Bedrock	Suscriptor	Genere AI-powered información para analizar los datos de Security Lake.	Integración de Amazon Bedrock
Amazon Detective	Suscriptor	Analice, investigue e identifique rápidamente la causa raíz de los hallazgos de seguridad o las actividades sospechosas consultando a Security Lake.	Integración con Amazon Detective
OpenSearch Servicio Amazon	Suscriptor	Genere información sobre seguridad a partir de los datos de Security Lake mediante la ingestión de OpenSearch servicios.	Integración OpenSearch de Amazon Service
Canalización OpenSearch de ingestión de Amazon Service	Suscriptor, fuente	Transmita registros, métricas y datos de rastreo a OpenSearch Service and Security Lake.	Integración del proceso OpenSearch de ingestión de Amazon Service
Amazon OpenSearch Service sin ETL	Suscriptor (consulta)	Consulte datos en Security Lake con cero ETL.	Integración de consultas directas sin ETL de Amazon OpenSearch Service

Servicio de AWS	Tipo de integración	Description (Descripción)	Cómo funciona la integración
Rápido	Suscriptor	Visualice, explore e interprete los registros en Security Lake con Quick.	Integración rápida
Amazon SageMaker AI	Suscriptor	Genere AI-powered información para analizar los datos de Security Lake.	Integración de Amazon SageMaker AI
AWS AppFabric	origen	Ingiere y normaliza los registros de las aplicaciones de software como servicio (SaaS) en el formato estándar de Security Lake.	Integración de AWS AppFabric
AWS Security Hub CSPM	origen	Centralice y almacene los hallazgos de seguridad del Security Hub CSPM en el formato estándar de Security Lake.	AWS Security Hub CSPM integración

Integración con Amazon Bedrock

Amazon Bedrock es un servicio totalmente administrado que pone a su disposición modelos fundacionales (FM) de alto rendimiento de las principales startups de IA y Amazon a través de una API unificada. Con la experiencia sin servidor de Amazon Bedrock, puede empezar rápidamente, personalizar de forma privada los modelos básicos con sus propios datos e integrarlos e implementarlos de forma fácil y segura en sus aplicaciones mediante AWS herramientas sin tener que gestionar ninguna infraestructura.

IA generativa

Puede utilizar las capacidades de IA generativa de Amazon Bedrock y la entrada en lenguaje natural de SageMaker AI Studio para analizar los datos en Security Lake y trabajar para reducir el riesgo de su organización y aumentar su postura de seguridad. Puede reducir el tiempo necesario para llevar a cabo una investigación identificando automáticamente las fuentes de datos adecuadas, generando e invocando consultas SQL y visualizando los datos de su investigación. Para obtener más información, consulte Generar información basada en IA para Amazon Security Lake con Amazon SageMaker AI Studio y Amazon Bedrock.

Integración con Amazon Detective

Tipo de integración: suscriptor

Amazon Detective ayuda a analizar, investigar e identificar rápidamente la causa raíz de resultados de seguridad o actividades sospechosas. Detective recopila automáticamente los datos de registro de sus recursos de AWS . A continuación, utiliza el machine learning, el análisis estadístico y la teoría de grafos para generar visualizaciones que lo ayuden a realizar investigaciones sobre la seguridad con mayor rapidez y de forma más eficaz. Las agregaciones de datos, los resúmenes y los contextos prediseñados de Detective ayudan a analizar y determinar rápidamente la naturaleza y el alcance de los posibles problemas de seguridad.

Al integrar Security Lake y Detective, puede consultar los datos de registro sin procesar almacenados por Security Lake desde Detective. Para obtener más información, consulte Integración con Amazon Security Lake.

Integración con Amazon OpenSearch Service

Tipo de integración: suscriptor

Amazon OpenSearch Service es un servicio gestionado que facilita la implementación, el funcionamiento y el escalado de los clústeres de OpenSearch servicios en Nube de AWS. Al utilizar OpenSearch Service Ingestion para incorporar datos a su clúster de OpenSearch servicios, puede obtener información más rápidamente para investigaciones de seguridad urgentes. Puede responder con rapidez a los incidentes de seguridad, lo que le ayuda a proteger los datos y sistemas críticos de su empresa.

OpenSearch Panel de servicios

Tras integrar OpenSearch Service con Security Lake, puede configurar Security Lake para que envíe datos de seguridad de diferentes fuentes a OpenSearch Service mediante la ingesta de OpenSearch servicios sin servidor. Para obtener más información sobre cómo configurar la ingesta de OpenSearch servicios para procesar los datos de seguridad, consulte Generar información de seguridad a partir de los datos de Amazon Security Lake mediante Amazon OpenSearch Service Ingestion.

Después de que OpenSearch Service Ingestion comience a escribir sus datos en su OpenSearch dominio de servicio. Para visualizar los datos mediante los paneles prediseñados, navegue hasta los paneles y elija cualquiera de los paneles instalados.

Integración con Amazon OpenSearch Service Ingestion Pipeline

Tipo de integración: suscriptor, fuente

Amazon OpenSearch Service Ingestion es un recopilador de datos sin servidor totalmente gestionado que transmite registros, métricas y datos de rastreo a OpenSearch Service and Security Lake.

Envíe datos a Security Lake mediante OpenSearch Ingestion Pipeline

Puede utilizar un complemento receptor de Amazon Simple Storage Service (Amazon S3) OpenSearch en Ingestion para enviar datos desde cualquier fuente compatible a Security Lake. Security Lake centraliza automáticamente los datos de seguridad de los AWS entornos, los entornos locales y los proveedores de SaaS en un lago de datos diseñado específicamente. Para obtener más información, consulte Uso de una canalización de OpenSearch ingestión con Amazon Security Lake como sumidero.

Envíe datos desde Security Lake a una canalización OpenSearch de OpenSearch ingestión

Puede usar un complemento fuente de Amazon S3 para incorporar datos a su canalización de OpenSearch ingestión. Para obtener más información, consulte Uso de una canalización de OpenSearch ingestión con Amazon Security Lake como fuente.

Integración con la consulta directa Zero-ETL de Amazon OpenSearch Service

Tipo de integración: suscriptor (consulta)

Puede usar OpenSearch Service Direct Query para analizar los datos en Amazon Security Lake. OpenSearch El servicio ofrece una integración sin ETL como una forma de consultar directamente sus datos en Security Lake mediante OpenSearch SQL o el lenguaje de procesamiento OpenSearch canalizado (PPL) sin incurrir en la fricción de crear canales de ingestión o cambiar de una herramienta de análisis a otra. Este enfoque elimina la necesidad de mover o duplicar los datos, lo que le permite analizar los datos allí donde se encuentran mediante la experiencia Discover en los paneles de control de servicio. OpenSearch Cuando desee pasar de consultar datos en reposo a supervisarlos activamente con paneles, puede crear vistas indexadas de los resultados de las consultas e incorporarlas a un índice de servicios. OpenSearch Para obtener más información sobre las consultas directas, consulta Cómo trabajar con consultas directas en la Guía para desarrolladores de Amazon OpenSearch Service.

OpenSearch El servicio utiliza una recopilación OpenSearch sin servidor para consultar directamente los datos en Security Lake y almacenar las vistas indexadas. Para ello, debe crear una fuente de datos que le permita utilizar las capacidades de OpenSearch cero ETL en los datos de Security Lake. Al crear un origen de datos, puede buscar directamente los datos almacenados en Security Lake, obtener información sobre ellos y analizarlos. Puede acelerar el rendimiento de sus consultas y utilizar OpenSearch análisis avanzados en determinados conjuntos de datos de Security Lake mediante la indexación bajo demanda.

- Para obtener más información sobre la creación de la integración de fuentes de datos de OpenSearch Service, consulte Creación de una integración de fuentes de datos de Amazon Security Lake en la Guía para desarrolladores de Amazon OpenSearch Service.
- Para obtener más información sobre la configuración de la fuente de datos de Security Lake en OpenSearch Service, consulte Configuración de una fuente de datos de Security Lake en OpenSearch Service Dashboards en la Guía para desarrolladores de Amazon OpenSearch Service.

Para obtener más información sobre el uso OpenSearch de Service with Security Lake, utilice los siguientes recursos.

- Presentamos la integración OpenSearch de Amazon Service y Amazon Security Lake para simplificar los análisis de seguridad
- Introducción a Zero-ETL en OpenSearch servicio con Amazon Security Lake

Introducción a Zero-ETL en OpenSearch servicio con Amazon Security Lake

Integración con Amazon Quick

Tipo de integración: suscriptor

Amazon Quick es un servicio de inteligencia empresarial (BI) a escala de nube que puede utilizar para ofrecer información fácil de entender a las personas con las que trabaja, estén donde estén. Quick se conecta a sus datos en la nube y combina datos de muchas fuentes diferentes. Quick ofrece a los responsables de la toma de decisiones la oportunidad de explorar e interpretar la información en un entorno visual interactivo. Tienen acceso seguro a los paneles de control desde cualquier dispositivo de la red y desde dispositivos móviles.

Panel de control rápido

Para visualizar sus datos de Amazon Security Lake en Quick, crear los AWS objetos necesarios e implementar fuentes de datos básicas, conjuntos de datos, análisis, paneles y grupos de usuarios en Quick con respecto a Security Lake. Para obtener instrucciones detalladas, consulta Integración con Amazon Quick.

Para obtener más información sobre la visualización de los datos de Security Lake con Quick, consulte los siguientes recursos.

Visualización de los datos de Security Lake con Quick: serie de aprendizaje rápido de 2024

Operacionalice los registros de ACL AWS WAF web con Security Lake

Integración con Amazon SageMaker AI

Tipo de integración: suscriptor

Amazon SageMaker AI es un servicio de aprendizaje automático (ML) totalmente gestionado. Con Security Lake, los científicos de datos y los desarrolladores pueden crear, entrenar e implementar modelos de aprendizaje automático de forma rápida y segura en un entorno hospedado listo para la producción. Proporciona una experiencia de interfaz de usuario para ejecutar flujos de trabajo de aprendizaje automático que hace SageMaker que las herramientas de aprendizaje automático estén disponibles en varios entornos de desarrollo integrados (IDE).

SageMaker Información sobre IA

Puede generar información de aprendizaje automático para Security Lake con SageMaker AI Studio. Este estudio es un entorno de desarrollo web integrado (IDE) para el aprendizaje automático que proporciona herramientas para que los científicos de datos preparen, creen, entrenen e implementen modelos de aprendizaje automático. Con esta solución, puede implementar rápidamente un conjunto básico de cuadernos de Python centrados en AWS Security Hub CSPMlos hallazgos de Security Lake, que también se pueden ampliar para incorporar otras AWS fuentes o fuentes de datos

personalizadas en Security Lake. Para obtener más información, consulte Generar información de aprendizaje automático para los datos de Amazon Security Lake mediante Amazon SageMaker AI.

Integración con AWS AppFabric

Tipo de integración: origen

AWS AppFabricses un servicio sin código que conecta las aplicaciones de software como servicio (SaaS) de toda la organización, es decir, las aplicaciones de TI y seguridad mediante un esquema estándar y un repositorio central.

¿Cómo recibe Security Lake las conclusiones AppFabric

Puede enviar los datos del registro de AppFabric auditoría a Security Lake seleccionando Amazon Kinesis Data Firehose como destino y configurando Kinesis Data Firehose para entregar los datos en esquema OCSF y formato Apache Parquet a Security Lake.

Requisitos previos

Antes de poder enviar los registros de AppFabric auditoría a Security Lake, debe enviar los registros de auditoría normalizados de OCSF a una transmisión de Kinesis Data Firehose. A continuación, puede configurar Kinesis Data Firehose para que envíe el resultado a su bucket de Amazon S3 de Security Lake. Para obtener más información, consulte Elegir Amazon S3 para su destino en la Guía para desarrolladores de Amazon Kinesis.

Envíe sus conclusiones a Security Lake AppFabric

Para enviar los registros de AppFabric auditoría a Security Lake después de completar el requisito previo anterior, debe habilitar ambos servicios y agregarlos AppFabric como fuente personalizada en Security Lake. Para obtener instrucciones sobre cómo añadir un origen personalizado, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Deje de recibir AppFabric registros en Security Lake

Para dejar de recibir registros de AppFabric auditoría, puede usar la consola de Security Lake, la API de Security Lake o AWS CLI eliminarlos AppFabric como fuente personalizada. Para obtener instrucciones, consulte Eliminar una fuente personalizada de Security Lake.

Integración con AWS Security Hub CSPM

Tipo de integración: origen

AWS Security Hub CSPMle proporciona una visión integral del estado de su seguridad AWS y ayuda a su entorno a cumplir con los estándares y las mejores prácticas del sector de la seguridad. Security Hub CSPM recopila datos de seguridad de todos Cuentas de AWS los servicios y productos de socios externos compatibles y le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios.

Cuando habilita Security Hub CSPM y agrega los hallazgos de CSPM de Security Hub como fuente en Security Lake, Security Hub CSPM comienza a enviar nuevos hallazgos y actualizaciones de los hallazgos existentes a Security Lake.

Cómo recibe Security Lake las conclusiones del CSPM de Security Hub

En Security Hub CSPM, se realiza seguimiento de los problemas de seguridad como resultados. Algunos hallazgos provienen de problemas detectados por otros socios Servicios de AWS o por terceros. Security Hub CSPM también genera sus propios hallazgos mediante la ejecución de controles de seguridad automatizados y continuos según las normas. Las reglas están representadas por controles de seguridad.

Todos los resultados en Security Hub CSPM usan un formato JSON estándar llamado Formato AWS Security Finding (ASFF).

Security Lake recibe los hallazgos del CSPM de Security Hub y los transforma en. Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake

Envíe los resultados del CSPM de su Security Hub a Security Lake

Para enviar las conclusiones de CSPM de Security Hub a Security Lake, debe habilitar ambos servicios y añadir las conclusiones de CSPM de Security Hub como fuente en Security Lake. Para obtener instrucciones sobre cómo agregar una AWS fuente, consulte. Agregar un Servicio de AWS como fuente

Si desea que Security Hub CSPM genere hallazgos de control y los envíe a Security Lake, debe habilitar los estándares de seguridad pertinentes y activar el registro de recursos a nivel regional en. AWS Config Para obtener más información, consulte Habilitar y configurar AWS Config en la Guía del usuario de AWS Security Hub .

Deje de recibir las conclusiones del CSPM de Security Hub en Security Lake

Para dejar de recibir los resultados de CSPM de Security Hub, puede utilizar la consola de CSPM de Security Hub, la API de CSPM de Security Hub o los siguientes temas de la AWS CLI Guía del usuario:AWS Security Hub

- Disabling and enabling the flow of findings from an integration (console) (Desactivación y habilitación del flujo de resultados desde una integración [consola])
- Inhabilitar el flujo de hallazgos de una integración (API de Security Hub, AWS CLI)

Third-party integraciones con Security Lake

Amazon Security Lake se integra con productos de varios proveedores de terceros. Un proveedor puede ofrecer una integración de orígenes, una integración de suscriptores o una integración de servicios. Los proveedores pueden ofrecer uno o más tipos de integración.

Las integraciones de origen tienen las siguientes propiedades:

- Envío de los datos a Security Lake
- Los datos llegan en formato Apache Parquet
- Los datos llegan al esquema de Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake

Las integraciones de suscriptor tienen las siguientes propiedades:

- Lea los datos de origen de Security Lake en un punto de conexión HTTPS o en una cola de Amazon Simple Queue Service (Amazon SQS), o bien consulte directamente los datos de origen de AWS Lake Formation
- Puede leer datos en formato Apache Parquet
- Puede leer datos en el esquema OCSF

Las integraciones de servicios pueden ayudarle a implementar Security Lake y otros en su organización. Servicios de AWS También pueden proporcionar asistencia con la elaboración de informes, los análisis y otros casos de uso.

Para buscar un proveedor asociado específico, consulte el Buscador de soluciones de socios. Para comprar un producto de terceros, consulte AWS Marketplace.

Para solicitar que se le añada como integración de socios o convertirse en socio de Security Lake, envíe un correo electrónico a `<securitylake-partners@amazon.com>`.

Si utilizas integraciones de terceros que envían las conclusiones a AWS Security Hub CSPM, también puedes revisarlas en Security Lake si la integración CSPM de Security Hub para Security

Lake está habilitada. Para obtener información acerca de cómo activar la integración, consulte Integración con AWS Security Hub CSPM. Para obtener una lista de las integraciones de terceros que envían los resultados a Security Hub CSPM, consulte las integraciones de productos de socios de terceros disponibles en la Guía del usuario.AWS Security Hub

Antes de configurar sus suscriptores, compruebe la compatibilidad con el registro OCSF de su suscriptor. Para obtener los detalles más recientes, consulta la documentación de tu suscriptor.

Integración de consultas

Puede consultar los datos que Security Lake almacena en AWS Lake Formation bases de datos y tablas. También puede crear suscriptores de terceros en la consola, la API o AWS Command Line Interface.

El administrador del lago de datos de Lake Formation debe conceder permisos de `SELECT` en las bases de datos y tablas pertinentes a la identidad de IAM que consulta los datos. Debe crear un suscriptor en Security Lake antes de consultar los datos. Para obtener más información sobre cómo crear una suscriptor con acceso de consulta, lea Administración del acceso a las consultas para los suscriptores de Security Lake.

Puede configurar la integración de consultas con Security Lake para los siguientes socios externos.

- Cribl – Search
- IBM – QRadar
- Palo Alto Networks – XSOAR
- Query.AI – Query Federated Search
- SOC Prime
- Splunk – Federated Analytics
- Tego Cyber

Accenture – MxDR

Tipo de integración: suscriptor, servicio

La integración de Accenture's MxDR con Security Lake ofrece la ingesta de datos de registros y eventos en tiempo real, la detección de anomalías gestionadas, la búsqueda de amenazas y las operaciones de seguridad. Esto ayuda a la analítica y a la detección y respuesta gestionadas (MDR).

Como integración de servicio, Accenture también puede ayudarle a implementar Security Lake en su organización.

Documentación de integración

Aqua Security

Tipo de integración: origen

Aqua Security se puede agregar como un origen personalizado para enviar eventos de auditoría a Security Lake. Los eventos de auditoría se convierten al esquema OCSF y al formato Parquet.

Documentación de integración

Barracuda – Protección de correo electrónico

Tipo de integración: origen

Barracuda Email Protection puede enviar eventos a Security Lake cuando se detectan nuevos ataques de correo electrónico de suplantación de identidad. Puede recibir estos eventos junto con otros datos de seguridad en su lago de datos.

Documentación de integración

Booz Allen Hamilton

Tipo de integración: servicio

Como integración de servicios, Booz Allen Hamilton utiliza un enfoque de ciberseguridad basado en datos mediante la fusión de datos y análisis con el servicio de Security Lake.

Enlace de socio

Software y soluciones digitales de Bosch – AiShield

Tipo de integración: origen

AIShieldpowered by Bosch proporciona análisis de vulnerabilidades automatizados y protección de puntos finales para los activos de IA mediante su integración con Security Lake.

Documentación de integración

ChaosSearch

Tipo de integración: suscriptor

ChaosSearch ofrece acceso a datos multimodelo a los usuarios con API abiertas, como Elasticsearch y SQL, o con las interfaces de usuario de Kibana y Superset incluidas de forma nativa. Puede consumir sus datos de Security Lake en ChaosSearch sin límites de retención para supervisar, alertar y detectar amenazas. Esto le ayuda a hacer frente a los complejos entornos de seguridad actuales y a las amenazas persistentes.

Documentación de integración

Seguridad de Cisco – Firewall seguro

Tipo de integración: origen

Al integrar Cisco Secure Firewall con Security Lake, puede almacenar los registros del firewall de forma estructurada y escalable. El cliente Cisco eNcore transmite los registros del firewall desde el Firewall Management Center, realiza la conversión del esquema al esquema OCSF y los almacena en Security Lake.

Documentación de integración

Claridad – Cúpula

Tipo de integración: origen

Claroty xDome envía las alertas detectadas en las redes a Security Lake con una configuración mínima. Las opciones de implementación flexibles y rápidas ayudan a xDome a proteger los activos extendidos de Internet de las cosas (XIoT), que consisten en activos de IoT, IIoT y BMS, dentro de su red, al tiempo que detectan automáticamente los indicadores tempranos de amenazas.

Documentación de integración

Soluciones CMD

Tipo de integración: servicio

CMD Solutions ayuda a las empresas a aumentar su agilidad al integrar la seguridad de forma temprana y continua mediante procesos de diseño, automatización y garantía continua. Como

integración de servicio, CMD Solutions puede ayudarle a implementar Security Lake en su organización.

Enlace de socio

Confluent – Conector de fregadero Amazon S3

Tipo de integración: origen

Confluent conecta, configura y orquesta automáticamente las integraciones de datos con conectores prediseñados y totalmente gestionados. El Confluent S3 Sink Connector le permite tomar datos sin procesar e introducirlos en Security Lake a escala y en formato Parquet nativo.

Documentación de integración

Seguridad de contraste

Tipo de integración: Origen

Producto asociado para la integración: Contrast Assess

Contrast Security Assess es una herramienta de IAST que ofrece detección de vulnerabilidades en tiempo real en aplicaciones web, API y microservicios. Assess se integra con Security Lake para ofrecer visibilidad centralizada de todas sus cargas de trabajo.

Documentación de integración

Cribl – Search

Tipo de integración: suscriptor

Puede utilizar Cribl Search para buscar datos de Security Lake.

Documentación de integración

Cribl – De streaming

Tipo de integración: Origen

Puede utilizar Cribl Stream para enviar datos desde cualquier fuente de terceros de Cribl compatible a Security Lake en el esquema OCSF.

Documentación de integración

CrowdStrike – Falcon Data Replicator

Tipo de integración: Origen

Esta integración extrae datos de forma continua de CrowdStrike Falcon Data Replicator, los transforma en el esquema OCSF y los envía a Security Lake.

Documentación de integración

CrowdStrike – SIEM de próxima generación

Tipo de integración: suscriptor

Simplifique la ingesta de datos de Security Lake con el conector de CrowdStrike Falcon Next-Gen SIEM datos que incluye analizadores de esquemas OCSF nativos. Falcon NG SIEMrevoluciona la detección, la investigación y la respuesta a las amenazas al reunir una profundidad y una amplitud de seguridad incomparables en una plataforma unificada para detener las infracciones.

Documentación de integración

CyberArk – Plataforma unificada de seguridad e identificación

Tipo de integración: origen

CyberArk Audit Adapter, una AWS Lambda función, recopila los eventos de seguridad CyberArk Identity Security Platform y envía los datos a Security Lake en un esquema OCSF.

Documentación de integración

Ciberseguridad en la nube – Cloud Fastener

Tipo de integración: suscriptor

CloudFasteneraprovecha Security Lake para facilitar la consolidación de los datos de seguridad de sus entornos de nube.

Documentación de integración

DataBahn

Tipo de integración: origen

Centralice sus datos de seguridad en Security Lake mediante DataBahn's Security Data Fabric.

Documentación de integración (inicie sesión en el portal de DataBahn para revisar la documentación)

Darktrace – Cyber AI Loop

Tipo de integración: Origen

La integración de Darktrace con Security Lake aporta el poder del autoaprendizaje de Darktrace a Security Lake. La información de Cyber AI Loop se puede correlacionar con otros flujos de datos y elementos del conjunto de seguridad de su organización. La integración registra las infracciones del modelo Darktrace como resultados de seguridad.

Documentación de integración (inicie sesión en el portal de Darktrace para revisar la documentación)

Datadog

Tipo de integración: suscriptor

Datadog Cloud SIEMdetecta las amenazas en tiempo real para su entorno de nube, incluidos los datos de Security Lake, y unifica DevOps los equipos de seguridad en una sola plataforma.

Documentación de integración

Deloitte – MXDR Cyber Analytics e IA Engine (CAE)

Tipo de integración: suscriptor, servicio

Deloitte MXDR CAE le ayuda a almacenar, analizar y visualizar rápidamente sus datos de seguridad estandarizados. El conjunto CAE de capacidades personalizadas de análisis, inteligencia artificial y aprendizaje automático proporciona automáticamente información procesable basada en modelos que se comparan con los OCSF-formatted datos de Security Lake.

Como integración de servicio, Deloitte también puede ayudarle a implementar Security Lake en su organización.

Documentación de integración

Devo

Tipo de integración: suscriptor

El Devo colector de AWS soportes para la ingestión de Security Lake. Esta integración puede ayudarle a analizar y abordar una variedad de casos de uso de seguridad, como la detección de amenazas, la investigación y la respuesta a incidentes.

Documentación de integración

DXC – SecMon

Tipo de integración: suscriptor, servicio

DXC SecMon recopila los eventos de seguridad de Security Lake y los supervisa para detectar posibles amenazas a la seguridad y alertar sobre ellas. Esto ayuda a las organizaciones a comprender mejor su postura de seguridad e identificar y responder proactivamente a las amenazas.

Como integración de servicio, DXC también puede ayudarle a implementar Security Lake en su organización.

Documentación de integración

Eviden – Isaac (anteriormente Atos)

Tipo de integración: suscriptor

La plataforma AIsaac MDR consume los registros de flujo de VPC ingeridos en el esquema OCSF de Security Lake y utiliza modelos de IA para detectar amenazas.

Documentación de integración

ExtraHop – Reveal (x) 360

Tipo de integración: Origen

Puede mejorar la carga de trabajo y la seguridad de las aplicaciones integrando los datos de la red, incluidas las detecciones de IOC, desde ExtraHop Reveal(x) 360, hasta Security Lake en el esquema OCSF

Documentación de integración

Falco, compinche

Tipo de integración: Origen

Falcosidekick recopila y envía los eventos de Falco a Security Lake. Esta integración exporta los eventos de seguridad mediante el esquema OCSF.

Documentación de integración

Fortinet: firewall nativo en la nube

Tipo de integración: origen

Al crear instancias FortiGate de CNF en AWS, puede especificar Amazon Security Lake como destino de salida de registros.

Documentación de integración

Gigamon – Inteligencia de metadatos de aplicaciones

Tipo de integración: Origen

Gigamon Application Metadata Intelligence (AMI) potencia sus herramientas de supervisión de observabilidad, SIEM y rendimiento de la red con atributos de metadatos críticos. Esto ayuda a proporcionar una mayor visibilidad de las aplicaciones para que pueda identificar los cuellos de botella en el rendimiento, los problemas de calidad y los posibles riesgos de seguridad de la red.

Documentación de integración

Hoop Cyber

Tipo de integración: servicio

Hoop Cyber FastStart incluye una evaluación del origen de datos, priorización e incorporación de los orígenes de datos, y ayuda a los clientes a consultar sus datos con las herramientas e integraciones existentes que se ofrecen a través de Security Lake.

Enlace de socio

HTCD – AI-First Plataforma de seguridad en la nube

Tipo de integración: suscriptor

Obtenga la automatización instantánea del cumplimiento, la priorización de los hallazgos de seguridad y los parches personalizados. HTCD puede consultar Security Lake para ayudarlo a descubrir amenazas mediante consultas e información en lenguaje natural. AI-driven

Documentación de integración

IBM – QRadar

Tipo de integración: suscriptor

IBM Security QRadar SIEM with UAX integra Security Lake con una plataforma de análisis que identifica y previene las amenazas en las nubes híbridas. Esta integración admite tanto el acceso a los datos como el acceso a las consultas.

Documentación de integración sobre el consumo de registros AWS CloudTrail

Documentación de integración sobre el uso de Amazon Athena para consultas

Infosys

Tipo de integración: servicio

Infosys le ayuda a personalizar la implementación de Security Lake según las necesidades de su organización y proporciona información personalizada.

Enlace de socio

Incorporado

Tipo de integración: servicio

Insbuilt se especializa en servicios de consultoría en la nube y puede ayudarle a comprender cómo implementar Security Lake en su organización.

Enlace de socio

Kyndryl – AIOps

Tipo de integración: suscriptor, servicio

Kyndrylse integra con Security Lake para proporcionar la interoperabilidad de los ciberdatos, la inteligencia de amenazas y el análisis. AI-powered Como suscriptor de acceso a datos, Kyndryl ingiere los eventos AWS CloudTrail de administración de Security Lake con fines analíticos.

Como integración de servicio, Kyndryl también puede ayudarle a implementar Security Lake en su organización.

Documentación de integración

Encajes – Polígrafo

Tipo de integración: origen

Lacework Polygraph® Data Platformse integra con Security Lake como fuente de datos y proporciona datos de seguridad sobre las vulnerabilidades, los errores de configuración y las amenazas conocidas y desconocidas en su AWS entorno.

Documentación de integración

Laminar

Tipo de integración: Origen

Laminar envía los eventos de seguridad de los datos a Security Lake en un esquema OCSF, lo que los pone a disposición para otros casos de uso de análisis, como la respuesta a incidentes y la investigación.

Documentación de integración

MegazoneCloud

Tipo de integración: servicio

MegazoneCloud se especializa en servicios de consultoría en la nube y puede ayudarle a comprender cómo implementar Security Lake en su organización. Conectamos Security Lake con soluciones ISV integradas para crear tareas personalizadas y generar información personalizada relacionada con las necesidades de los clientes.

Documentación de integración

Mónada

Tipo de integración: Origen

Monad transforma automáticamente sus datos en un esquema OCSF y los envía a su lago de datos de Security Lake.

Documentación de integración

NETSCOUT – Ciberinteligencia de Omnis

Tipo de integración: origen

Al integrarse con Security Lake, NETSCOUT se convierte en un origen personalizado de resultados de seguridad e información de seguridad detallada sobre lo que sucede en la empresa, como las ciberamenazas, los riesgos de seguridad y los cambios en la superficie expuesta a ataques. NETSCOUT CyberStreams y Omnis Cyber Intelligence producen estos resultados en la cuenta del cliente y, luego, se envían a Security Lake en un esquema OCSF. Los datos ingeridos también cumplen con otros requisitos y prácticas recomendadas para un origen de Security Lake, incluidos el formato, el esquema, las particiones y los aspectos relacionados con el rendimiento.

Documentación de integración

Netskope – CloudExchange

Tipo de integración: origen

Netskopele ayuda a reforzar su postura de seguridad al compartir registros relacionados con la seguridad e información sobre amenazas con Security Lake. Netskopelos resultados se envían a Security Lake con un CloudExchange complemento, que se puede lanzar como un entorno basado en Docker dentro AWS o en un centro de datos local.

Documentación de integración

New Relic ONE

Tipo de integración: suscriptor

New Relic ONEes una aplicación para Lambda-based suscriptores. Se implementa en su cuenta, activada por Amazon SQS, y envía los datos a New Relic mediante de claves de licencia de New Relic

Documentación de integración

Okta – Workforce Identity Cloud

Tipo de integración: origen

Oktaenvía registros de identidad a Security Lake en un esquema OCSF a través de una EventBridge integración de Amazon. Okta System Logsen el esquema OCSF, ayudará a los equipos de científicos

de datos y seguridad a consultar los eventos de seguridad mediante un estándar de código abierto. La generación de registros OCSF estandarizados a partir de Okta le ayuda a realizar actividades de auditoría y a generar informes relacionados con la autenticación, la autorización, los cambios de cuentas y los cambios de entidad según un esquema coherente.

Documentación de integración

AWS CloudFormation plantilla para añadir Okta como fuente personalizada en Security Lake

Orca – Plataforma de seguridad en la nube

Tipo de integración: origen

La plataforma de seguridad en la nube Orca sin agentes que AWS se integra con Security Lake mediante el envío de eventos de detección y respuesta (CDR) en la nube en un esquema OCSF.

Documentación de integración (inicie sesión en el portal de Orca para revisar la documentación)

Palo Alto Networks – Prisma Cloud

Tipo de integración: Origen

Palo Alto Networks Prisma Cloud agrega los datos de detección de vulnerabilidades entre las máquinas virtuales de sus entornos nativos en la nube y los envía a Security Lake.

Documentación de integración

Palo Alto Networks – VOLAR

Tipo de integración: Suscriptor

Palo Alto Networks XSOARha creado una integración de suscriptores con XSOAR y Security Lake.

Documentación de integración

Pantera

Tipo de integración: suscriptor

Pantheradmite la ingesta de registros de Security Lake para su uso en la búsqueda y detección.

Documentación de integración

Ping Identity – PingOne

Tipo de integración: Origen

PingOne envía alertas de modificación de cuentas a Security Lake en formato OCSF y Parquet, lo que le permite detectar los cambios en la cuenta y actuar en consecuencia.

Documentación de integración

PwC – Centro de fusión

Tipo de integración: suscriptor, servicio

PwC aporta sus conocimientos y experiencia para ayudar a los clientes a implementar un centro de fusión que satisfaga sus necesidades individuales. Basado en Amazon Security Lake, un centro de fusión ofrece la posibilidad de combinar datos de diversos orígenes para crear una vista centralizada prácticamente en tiempo real.

Documentación de integración

Query.AI – Consulta la búsqueda federada

Tipo de integración: suscriptor

Query Federated Searchpuede consultar directamente cualquier tabla de Security Lake a través de Amazon Athena para respaldar la respuesta a incidentes, las investigaciones, la búsqueda de amenazas y la búsqueda general en una variedad de observables, eventos y objetos del esquema de OCSF.

Documentación de integración

Rapid7 – InsightIDR

Tipo de integración: suscriptor

InsightIDR, la Rapid7 SIEM/XDR solución, puede ingerir registros en Security Lake para detectar amenazas e investigar actividades sospechosas.

Documentación de integración

RipJar – Laberinto para la investigación de amenazas

Tipo de integración: suscriptor

Labyrinth for Threat Investigations proporciona un enfoque empresarial para la exploración de amenazas a gran escala basado en la fusión de datos, con seguridad detallada, flujos de trabajo adaptables e informes.

Documentación de integración

Sailpoint

Tipo de integración: origen

Producto asociado para la integración: SailPoint IdentityNow

Esta integración permite a los clientes transformar los datos de los eventos desde SailPoint IdentityNow. El objetivo de la integración es proporcionar un proceso automatizado que incorpore la actividad de los usuarios y los eventos de gobierno de IdentityNow a Security Lake a fin de mejorar la información que ofrecen los productos de supervisión de incidentes y eventos de seguridad.

Documentación de integración

Securonix

Tipo de integración: suscriptor

Securonix Next-Gen SIEM se integra con Security Lake, lo que permite a los equipos de seguridad ingerir datos con mayor rapidez y ampliar sus capacidades de detección y respuesta.

Documentación de integración

SentinelOne

Tipo de integración: suscriptor

La plataforma SentinelOne Singularity™ XDR amplía la detección y respuesta en tiempo real a las cargas de trabajo de punto de conexión, identidad y de nube que se ejecutan en infraestructuras de nube pública y en las instalaciones, como Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Kubernetes Service (Amazon EKS).

Documentación de integración (inicie sesión en el portal de SentinelOne para revisar la documentación)

Sentra – Plataforma de seguridad del ciclo de vida de los datos

Tipo de integración: Origen

Tras implementar la infraestructura de digitalización Sentra en su cuenta, Sentra busca los resultados y los incorpora a su SaaS. Estos resultados son metadatos que Sentra almacena y, posteriormente, transmite a Security Lake en un esquema OCSF para su consulta.

Documentación de integración

SOC Prime

Tipo de integración: suscriptor

SOC Primese integra con Security Lake a través de Amazon OpenSearch Service y Amazon Athena para facilitar la organización inteligente de los datos y la búsqueda de amenazas en función de los hitos de confianza cero. SOC Primepermite a los equipos de seguridad aumentar la visibilidad de las amenazas e investigar los incidentes sin un volumen abrumador de alertas. Puede ahorrar tiempo de desarrollo con reglas y consultas reutilizables que se pueden convertir automáticamente en Athena y OpenSearch Service en el esquema OCSF.

Documentación de integración

Splunk

Tipo de integración: suscriptor

El Splunk AWS Add-On para Amazon Web Services (AWS) admite la ingestión desde Security Lake. Esta integración le ayuda a acelerar la detección, la investigación y la respuesta a las amenazas al suscribirse a los datos del esquema OCSF de Security Lake.

Documentación de integración

Stellar Cyber

Tipo de integración: suscriptor

Stellar Cyber consume los registros de Security Lake y los agrega al lago de datos de Stellar Cyber. Este conector utiliza el esquema OCSF.

Documentación de integración

Sumo Logic

Tipo de integración: suscriptor

Sumo Logicconsume datos de Security Lake y proporciona una amplia visibilidad en AWS los entornos de nube híbrida y local. Sumo Logic ofrece a los equipos de seguridad una visibilidad completa, automatización y supervisión de amenazas en todas sus herramientas de seguridad.

Documentación de integración

Swimlane – Turbina

Tipo de integración: suscriptor

Swimlane ingiere los datos de Security Lake en un esquema OCSF y los envía a través de manuales de programación simplificados y de gestión de casos para facilitar la detección de amenazas, la investigación y la respuesta a los incidentes con mayor rapidez.

Documentación de integración (inicie sesión en el portal de Swimlane para revisar la documentación)

Sysdig Secure

Tipo de integración: origen

Sysdig Secure'sLa plataforma de protección de aplicaciones nativa de la nube (CNAPP) envía los eventos de seguridad a Security Lake para maximizar la supervisión, agilizar las investigaciones y simplificar el cumplimiento.

Documentación de integración

Garra

Tipo de integración: origen

Producto asociado para la integración: Talon Enterprise Browser

Talon's Enterprise Browser, un entorno de punto de conexión seguro y aislado basado en un navegador, envía acceso de Talon, protección de datos, acciones de SaaS y eventos de seguridad

a Security Lake, lo que proporciona visibilidad y la opción de correlacionar eventos de forma cruzada para la detección, el análisis forense y las investigaciones.

Documentación de integración (inicie sesión en el portal de Talon para revisar la documentación)

Tanium

Tipo de integración: Origen

La plataforma Tanium Unified Cloud Endpoint Detection, Management, and Security proporciona datos de inventario a Security Lake en un esquema OCSF.

Documentación de integración

TCS

Tipo de integración: servicio

TCS AWS Business Unit ofrece innovación, experiencia y talento. Esta integración está impulsada por una década de creación conjunta de valor, un profundo conocimiento del sector, experiencia tecnológica y sabiduría en materia de entrega. Como integración de servicio, TCS puede ayudarle a implementar Security Lake en su organización.

Documentación de integración

Tego Cyber

Tipo de integración: suscriptor

Tego Cyber se integra con Security Lake para ayudarle a detectar e investigar rápidamente posibles amenazas de seguridad. Al correlacionar diversos indicadores de amenazas en amplios periodos de tiempo y orígenes de registros, Tego Cyber descubre amenazas ocultas. La plataforma está enriquecida con inteligencia sobre amenazas altamente contextual, que proporciona precisión e información en la detección e investigación de amenazas.

Documentación de integración

Tines – No-code automatización de la seguridad

Tipo de integración: suscriptor

Tines No-code security automation le ayuda a tomar decisiones más precisas al aprovechar los datos de seguridad centralizados en Security Lake.

Documentación de integración

Torq – Plataforma de automatización de seguridad empresarial

Tipo de integración: origen, suscriptor

Torq se integra perfectamente con Security Lake como origen personalizado y como suscriptor. Torq le ayuda a implementar la automatización y la orquestación a escala empresarial con una plataforma sencilla y sin código.

Documentación de integración

Trellix – XDR

Tipo de integración: origen, suscriptor

Como plataforma XDR abierta, Trellix XDR es compatible con la integración de Security Lake. Trellix XDR puede aprovechar los datos del esquema OCSF para casos de uso de análisis de seguridad. También puede ampliar su lago de datos de Security Lake con más de 1000 fuentes de eventos de seguridad en Trellix XDR. Esto le ayuda a ampliar las capacidades de detección y respuesta de su AWS entorno. Los datos ingeridos se correlacionan con otros riesgos de seguridad, lo que le proporciona los manuales necesarios para responder a un riesgo de manera oportuna.

Documentación de integración

Trend Micro – CloudOne

Tipo de integración: Origen

Trend Micro CloudOne Workload Security envía la siguiente información a Security Lake desde las instancias de Amazon Elastic Compute Cloud (EC2):

- Actividad de consultas de DNS
- Actividad de archivos
- Actividad de red
- Actividad de proceso
- Actividad de Registry Value

- Actividad de la cuenta de usuario

Documentación de integración

Uptycs – Uptycs XDR

Tipo de integración: Origen

Uptycs envía una gran cantidad de datos en un esquema OCSF desde los activos en las instalaciones y en la nube a Security Lake. Los datos incluyen la detección de amenazas de comportamiento en los puntos de conexión y las cargas de trabajo en la nube, las detecciones de anomalías, las infracciones de las políticas, las políticas riesgosas, las configuraciones incorrectas y las vulnerabilidades.

Documentación de integración

Vectra AI – Vectra Detect para AWS

Tipo de integración: origen

Al usarloVectra Detect for AWS, puede enviar alertas de alta fidelidad a Security Lake como una fuente personalizada utilizando una plantilla dedicada CloudFormation .

Documentación de integración

VMware Aria Automation para nubes seguras

Tipo de integración: Origen

Con esta integración, puede detectar errores de configuración en la nube y enviarlos a Security Lake para su análisis avanzado.

Documentación de integración

Wazuh

Tipo de integración: suscriptor

Wazuh tiene como objetivo gestionar de forma segura los datos de los usuarios, proporcionar acceso a las consultas para cada origen y optimizar los costes de consulta.

Documentación de integración

Wipro

Tipo de integración: origen, servicio

Esta integración le permite recopilar datos de la plataforma Wipro Cloud Application Risk Governance (CARG) para ofrecer una visión unificada de sus aplicaciones en la nube y de las políticas de cumplimiento en toda la empresa.

Como integración de servicio, Wipro también puede ayudarle a implementar Security Lake en su organización.

Documentación de integración

Wiz – CNAPP

Tipo de integración: origen

La integración entre Wiz y Security Lake facilita la recopilación de datos de seguridad en la nube en un único lago de datos de seguridad al aprovechar el esquema OCSF, un estándar de código abierto diseñado para un intercambio de datos de seguridad normalizado y ampliable.

Documentación de integración (inicie sesión en el portal de Wiz para revisar la documentación)

Zscaler – Control de postura de Zscaler

Tipo de integración: origen

Zscaler Posture Control™, una plataforma de protección de aplicaciones nativa en la nube, envía los resultados de seguridad a Security Lake en un esquema OCSF.

Documentación de integración

Seguridad en Security Lake

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon Security Lake, consulte AWS Servicios incluidos en el ámbito del programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Security Lake. Los siguientes temas muestran cómo configurar Security Lake para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Security Lake.

Temas

- Gestión de identidad y acceso para Security Lake
- Protección de los datos en Amazon Security Lake
- Validación de la conformidad para Amazon Security Lake
- Prácticas recomendadas de seguridad para Security Lake
- Resiliencia de Amazon Security Lake
- Seguridad de infraestructuras en Amazon Security Lake
- Configuración y análisis de vulnerabilidades en Security Lake
- Amazon Security Lake y puntos de enlace de VPC de interfaz ()AWS PrivateLink
- Supervisión de Amazon Security Lake

Gestión de identidad y acceso para Security Lake

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Security Lake. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración del acceso con políticas
- Cómo funciona Security Lake con IAM
- Ejemplos de políticas basadas en la identidad para Security Lake
- AWS políticas administradas para Security Lake
- Uso de funciones vinculadas a servicios para Security Lake

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de identidad y acceso de Amazon Security Lake).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona Security Lake con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en la identidad para Security Lake).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. 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.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente 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 Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda 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 de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder 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 rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. 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 usuario federado, 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 del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las 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 roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON 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 la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (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 Selección 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 basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en 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 (SCPs): 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 (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener 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 saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Security Lake con IAM

Antes de utilizar IAM para administrar el acceso a Security Lake, obtenga información sobre qué características de IAM están disponibles para utilizar con Security Lake.

Características de IAM que puede utilizar con Amazon Security Lake

Característica de IAM	Compatibilidad con Security Lake
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan Security Lake y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidad para Security Lake

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 la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente 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 la política de JSON de IAM en la Guía del usuario de IAM.

Security Lake es compatible con las políticas basadas en identidad. Para obtener más información, consulte Ejemplos de políticas basadas en la identidad para Security Lake.

Políticas basadas en recursos de Security Lake

Compatibilidad con las políticas basadas en recursos: sí

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 basada en recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

El servicio de Security Lake crea políticas basadas en recursos para los buckets de Amazon S3 que almacenan los datos. No asocie estas políticas basadas en recursos a los buckets de S3. Security Lake crea automáticamente estas políticas en su nombre.

Un ejemplo de recurso es un bucket de S3 con un nombre de recurso de Amazon (ARN) de `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`. En este ejemplo, `region` se trata de una secuencia alfanumérica específica Región de AWS en la que se ha

activado Security Lake y `bucket-identifier` es una cadena alfanumérica única a nivel regional que Security Lake asigna al bucket. Security Lake crea el bucket de S3 para almacenar los datos de esa región. La política de recursos define qué entidades principales pueden realizar acciones en el bucket. Este es un ejemplo de política basada en recursos (política de bucket) que Security Lake asocia al bucket:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        },
        {
            "Sid": "PutSecurityLakeObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "securitylake.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-
east-1:111122223333:*"
                }
            }
        }
    ]
}
```

Para obtener más información acerca de las políticas basadas en recursos, consulte Políticas basadas en identidad y políticas basadas en recursos en la Guía de usuario de IAM.

Acciones de política para Security Lake

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON 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 Security Lake, consulte Acciones definidas por Amazon Security Lake en la referencia de autorizaciones de servicio.

Las acciones de políticas de Security Lake utilizan el siguiente prefijo antes de la acción:

```
securitylake
```

Por ejemplo, para conceder a un usuario permiso para acceder a la información sobre un suscriptor específico, incluya la acción `securitylake:GetSubscriber` en la política asignada a ese usuario. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Security Lake 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.

```
"Action": [
      "securitylake:action1",
      "securitylake:action2"
]
```

Para ver ejemplos de políticas basadas en identidad de Security Lake, consulte Ejemplos de políticas basadas en la identidad para Security Lake.

Recursos de políticas para Security Lake

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON 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). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Security Lake define los siguientes tipos de recursos: el suscriptor y la configuración del lago de datos para un Cuenta de AWS determinado recurso Región de AWS. Puede especificar estos tipos de recursos en las políticas mediante ARNs.

Para obtener una lista de los tipos de recursos de Security Lake y la sintaxis del ARN de cada uno, consulte Tipos de recursos definidos por Amazon Security Lake en la Referencia de autorizaciones de servicio. Para saber qué acciones puede especificar para cada tipo de recurso, consulte Acciones definidas por Amazon Security Lake en la Referencia de autorizaciones de servicio.

Para ver ejemplos de políticas basadas en identidad de Security Lake, consulte Ejemplos de políticas basadas en la identidad para Security Lake.

Claves de condición de política de Security Lake

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON 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. Puede 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 AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Security Lake, consulte Claves de condición de Amazon Security Lake en la Referencia de autorizaciones de servicio. Para saber con qué acciones y recursos puede usar una clave de condición, consulte Acciones definidas por Amazon Security Lake en la Referencia de autorizaciones de servicio. Para ver ejemplos de políticas que utilizan claves de condición, consulte Ejemplos de políticas basadas en la identidad para Security Lake.

Listas de control de acceso (ACLs) en Security Lake

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Security Lake no es compatible ACLs, lo que significa que no se puede adjuntar una ACL a un recurso de Security Lake.

Control de acceso basado en atributos (ABAC) con Security Lake

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 adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del 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 Security Lake (suscriptores) y a la configuración del lago de datos de una persona. Cuenta de AWS Regiones de AWS También puede controlar el acceso a estos tipos de recursos proporcionando información sobre las etiquetas en el elemento `Condition` de una política. Para obtener información acerca del etiquetado de recursos de Security Lake, consulte Etiquetado de los recursos de Security Lake. Para consultar un ejemplo de una política basada en la identidad que controla el acceso a un recurso en función de las etiquetas de ese recurso, consulte Ejemplos de políticas basadas en la identidad para Security Lake.

Uso de credenciales temporales con Security Lake

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza una federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar 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.

Security Lake admite el uso de credenciales temporales.

Sesiones de acceso directo para Security Lake

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que realiza la llamada Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Algunas acciones de Security Lake requieren permisos para realizar acciones adicionales y dependientes en otros Servicios de AWS. Para ver una lista de estas acciones, consulte Acciones definidas por Amazon Security Lake en la referencia de autorizaciones de servicio.

Roles de servicio de Security Lake

Compatible con roles de servicio: No

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 Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Security Lake no asume ni utiliza roles de servicio. Sin embargo, los servicios relacionados EventBridge AWS Lambda, como Amazon y Amazon S3, asumen funciones de servicio cuando utiliza Security Lake. Security Lake utiliza un rol vinculado al servicio para llevar a cabo acciones en su nombre.

> **Warning**
>
> El cambio de los permisos de un rol de servicio podría provocar problemas operativos con el uso de Security Lake. Edite los roles de servicio solo cuando Security Lake proporcione orientación para hacerlo.

Roles vinculados a servicios de Security Lake

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted 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.

Security Lake usa un rol vinculado a servicios de IAM denominado `AWSServiceRoleForAmazonSecurityLake`. El rol vinculado a servicios de Security Lake concede permisos para operar un servicio de lago de datos de seguridad en nombre de los clientes. Este rol vinculado a servicios es un rol de IAM que está vinculado directamente a Security Lake. Security Lake los predefine e incluye todos los permisos que Security Lake necesita para llamar a otras personas Servicios de AWS en tu nombre. Security Lake utiliza esta función vinculada a un servicio en todos los lugares en los Regiones de AWS que Security Lake está disponible.

Para obtener información acerca de cómo crear o administrar el rol vinculado a servicios de Security Lake, consulte Uso de funciones vinculadas a servicios para Security Lake.

Ejemplos de políticas basadas en la identidad para Security Lake

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Security Lake. 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.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Security Lake, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Security Lake en la Referencia de autorización de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Security Lake
- Ejemplo: Permitir que los usuarios vean sus propios permisos
- Ejemplo: Permitir que la cuenta de administración de la organización designe y elimine a un administrador delegado
- Ejemplo: Permitir a los usuarios revisar los suscriptores en función de las etiquetas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Security Lake de la 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:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. 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, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, 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.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para 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.

Uso de la consola de Security Lake

Para acceder a la consola de Amazon Security Lake, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Security Lake que tiene en su cuenta. 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 concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan usar la consola de Security Lake, cree políticas de IAM que les proporcionen acceso a la consola. Para obtener más información, consulte Identidades de IAM en la Guía del usuario de IAM.

Si crea una política que permite a los usuarios o roles usar la consola de Security Lake, asegúrese de que la política incluya las acciones adecuadas para los recursos a los que dichos usuarios o roles necesitan acceder en la consola. De lo contrario, no podrán acceder a esos recursos ni mostrar detalles sobre ellos en la consola.

Por ejemplo, para agregar un origen personalizado mediante la consola, un usuario debe tener la posibilidad de realizar las siguientes acciones:

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StartCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

Ejemplo: Permitir que los usuarios vean 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 completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Ejemplo: Permitir que la cuenta de administración de la organización designe y elimine a un administrador delegado

En este ejemplo se muestra cómo podría crear una política que permita a un usuario de una cuenta de administración de AWS Organizations designar y eliminar el administrador de Security Lake delegado de la organización.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "securitylake:RegisterDataLakeDelegatedAdministrator",
                "securitylake:DeregisterDataLakeDelegatedAdministrator"
            ],
            "Resource": "arn:aws:securitylake:*:*:*"
        }
    ]
}
```

Ejemplo: Permitir a los usuarios revisar los suscriptores en función de las etiquetas

En políticas basadas en la identidad, puede utilizar las condiciones para controlar el acceso a los recursos de Security Lake basados en etiquetas. En este ejemplo se muestra cómo podría crear una política que permita a un usuario revisar a los suscriptores con la consola de Security Lake o con la API de Security Lake. Sin embargo, los permisos solo se conceden si el valor de la etiqueta `Owner` para un suscriptor es el nombre de usuario de dicho usuario.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewSubscriberDetailsIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:GetSubscriber",
            "Resource": "arn:aws:securitylake:*:*:subscriber/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListSubscribersIfOwner",
```

```
            "Effect": "Allow",
            "Action": "securitylake:ListSubscribers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

En este ejemplo, si un usuario que tiene el nombre de usuario `richard-roe` intenta revisar los detalles de los suscriptores individuales, se debe etiquetar al suscriptor con `Owner=richard-roe` o `owner=richard-roe`. De lo contrario, se deniega el acceso al usuario. La clave de la etiqueta de condición `Owner` coincide con los nombres de las claves de condición `Owner` y `owner` porque no distinguen entre mayúsculas y minúsculas. Para obtener más información acerca de cómo utilizar las claves de condición, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM. Para obtener información acerca del etiquetado de recursos de Security Lake, consulte Etiquetado de los recursos de Security Lake.

AWS políticas administradas para Security Lake

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando haya nuevas operaciones de API disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AmazonSecurityLakeMetastoreManager

Amazon Security Lake usa una AWS Lambda función para administrar los metadatos de su lago de datos. Mediante el uso de esta función, Security Lake puede indexar las particiones de Amazon Simple Storage Service (Amazon S3) que contienen sus datos y archivos de datos en las tablas del catálogo de AWS Glue datos. Esta política administrada contiene todos los permisos para que la función Lambda indexe las particiones y los archivos de datos de S3 en las AWS Glue tablas.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `logs`— Permite a los directores registrar la salida de la función Lambda en Amazon Logs. CloudWatch
- `glue`— Permite a los directores realizar acciones de escritura específicas para las tablas del catálogo de AWS Glue datos. Esto también permite a AWS Glue los rastreadores identificar las particiones de los datos.
- `sqs`— Permite a los directores realizar acciones específicas de lectura y escritura para las colas de Amazon SQS que envían notificaciones de eventos cuando se añaden objetos a su lago de datos o se actualizan en él.
- `s3`— Permite a los directores realizar acciones de lectura y escritura específicas para el bucket de Amazon S3 que contiene sus datos.

Para revisar los permisos de esta política, consulte AmazonSecurityLakeMetastoreManager en la Guía de referencia de la política administrada de AWS .

AWS política gestionada: AmazonSecurityLakePermissionsBoundary

Amazon Security Lake crea funciones de IAM para que fuentes personalizadas de terceros escriban datos en el lago de datos y para que los suscriptores personalizados de terceros consuman datos del lago de datos, y utiliza esta política al crear estas funciones para definir el límite de sus

permisos. No es necesario que realice ninguna acción para usar esta política. Si el lago de datos está encriptado con una AWS KMS clave administrada por el cliente `kms:Decrypt` y se agregan `kms:GenerateDataKey` los permisos.

Para revisar los permisos de esta política, consulte AmazonSecurityLakePermissionsBoundary en la Guía de referencia de la política administrada de AWS .

AWS política gestionada: AmazonSecurityLakeAdministrator

Puede adjuntar la `AmazonSecurityLakeAdministrator` política a un director antes de que habilite Amazon Security Lake en su cuenta. Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Security Lake. A continuación, el director puede incorporarse a Security Lake y, posteriormente, configurar las fuentes y los suscriptores en Security Lake.

Esta política incluye las acciones que los administradores de Security Lake pueden realizar en otros AWS servicios a través de Security Lake.

La `AmazonSecurityLakeAdministrator` política no admite la creación de las funciones de utilidad requeridas por Security Lake para administrar la replicación entre regiones de Amazon S3, el registro de nuevas particiones de datos, la ejecución de un rastreador de Glue con los datos agregados a fuentes personalizadas o la notificación de nuevos datos a los suscriptores de puntos finales de HTTPS. AWS Glue Puede crear estas funciones con antelación, tal y como se describe en. Introducción a Amazon Security Lake

Además de la política `AmazonSecurityLakeAdministrator` administrada, Security Lake requiere `lakeformation:PutDataLakeSettings` permisos para las funciones de incorporación y configuración. `PutDataLakeSettings`permite establecer a un director de IAM como administrador de todos los recursos regionales de Lake Formation de la cuenta. Este rol debe estar `iam:CreateRole permission` acompañado de una `AmazonSecurityLakeAdministrator` política adjunta.

Los administradores de Lake Formation tienen acceso total a la consola de Lake Formation y controlan la configuración inicial de los datos y los permisos de acceso. Security Lake asigna el principal que habilita Security Lake y el `AmazonSecurityLakeMetaStoreManager` rol (u otro rol especificado) de administradores de Lake Formation para que puedan crear tablas, actualizar el esquema de las tablas, registrar nuevas particiones y configurar los permisos en las tablas. Debe incluir los siguientes permisos en la política para el usuario o la función de administrador de Security Lake:

> **Note**
>
> Para proporcionar los permisos suficientes para conceder a los suscriptores de Lake Formation el acceso de los suscriptores, Security Lake recomienda agregar los siguientes `glue:PutResourcePolicy` permisos.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutLakeFormationSettings",
      "Effect": "Allow",
      "Action": "lakeformation:PutDatalakeSettings",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowGlueActions",
      "Effect": "Allow",
      "Action": ["glue:PutResourcePolicy", "glue:DeleteResourcePolicy"],
      "Resource": [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    }
  ]
}
```

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `securitylake`— Permite a los directores un acceso total a todas las acciones de Security Lake.
- `organizations`— Permite a los directores recuperar información de AWS las organizaciones sobre las cuentas de una organización. Si una cuenta pertenece a una organización, estos permisos permiten que la consola de Security Lake muestre los nombres y números de las cuentas.
- `iam`— Permite a los directores crear funciones vinculadas a los servicios para Security Lake y Amazon EventBridge, además AWS Lake Formation, es un paso obligatorio para habilitar esos servicios. También permite crear y editar políticas para las funciones de suscriptor y de fuente personalizadas, y los permisos de esas funciones se limitan a lo permitido por la política. `AmazonSecurityLakePermissionsBoundary`
- `ram`— Permite a los directores configurar el acceso Lake Formation basado en consultas por parte de los suscriptores a las fuentes de Security Lake.
- `s3`— Permite a los directores crear y administrar los depósitos de Security Lake y leer el contenido de esos depósitos.
- `lambda`— Permite a los directores administrar las particiones de AWS Glue tablas Lambda utilizadas para actualizar después de la entrega del AWS código fuente y la replicación entre regiones.
- `glue`— Permite a los directores crear y administrar la base de datos y las tablas de Security Lake.
- `lakeformation`— Permite a los directores administrar los Lake Formation permisos de las tablas de Security Lake.
- `events`— Permite a los directores administrar las reglas que se utilizan para notificar a los suscriptores los nuevos datos en las fuentes de Security Lake.
- `sqs`— Permite a los directores crear y administrar las Amazon SQS colas que se utilizan para notificar a los suscriptores los nuevos datos en las fuentes de Security Lake.
- `kms`— Permite a los directores conceder acceso a Security Lake para escribir datos mediante una clave administrada por el cliente.
- `secretsmanager`— Permite a los directores administrar los secretos que se utilizan para notificar a los suscriptores la existencia de nuevos datos en las fuentes de Security Lake a través de terminales HTTPS.

Para revisar los permisos de esta política, consulte AmazonSecurityLakeAdministrator en la Guía de referencia de la política administrada de AWS .

AWS política gestionada: SecurityLakeServiceLinkedRole

Security Lake usa la función vinculada a servicios denominada `AWSServiceRoleForSecurityLake` para crear y operar el lago de datos de seguridad.

No puede adjuntar la política `SecurityLakeServiceLinkedRole` gestionada a sus entidades de IAM. Esta política está vinculada a una función vinculada a un servicio que permite a Security Lake realizar acciones en su nombre. Para obtener más información, consulte los permisos de Service-linked rol en Security Lake.

AWS política gestionada: SecurityLakeResourceManagementServiceRolePolicy

Security Lake utiliza la función vinculada a servicios denominada `AWSServiceRoleForSecurityLakeResourceManagement` para realizar mejoras continuas de supervisión y rendimiento, lo que puede reducir la latencia y los costos. Proporciona acceso para administrar los recursos creados por Security Lake. Otorga a Security Lake la capacidad de eliminar SecurityLake _Glue_Partition_Updater_Lambda. Esta lambda ha quedado obsoleta para los clientes que han realizado una migración de iceberg y han pasado a fuentes de la versión 2. Esta lambda utilizaba el tiempo de ejecución de Python 3.9, que quedará obsoleto en diciembre. En lugar de actualizar el tiempo de ejecución de esta lambda para esos clientes, sería mejor eliminarlos. Tenemos un proceso de recuperación que determinará si el cliente aún necesita la lambda o no y, en caso contrario, la eliminará. Esta actualización de la SLR es necesaria para que podamos eliminar esa lambda.

No puedes adjuntar la política `SecurityLakeResourceManagementServiceRolePolicy` gestionada a tus entidades de IAM. Esta política está vinculada a una función vinculada a un servicio que permite a Security Lake realizar acciones en su nombre. Para obtener más información, consulte los permisos de Service-linked rol para la administración de recursos.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `events`— Permite a los directores enumerar y administrar EventBridge las reglas para el procesamiento de eventos de Security Lake.

- `lambda`— Permite a los directores administrar las funciones y configuraciones de Lambda para el procesamiento de metadatos de Security Lake, incluida la posibilidad de eliminar las funciones de actualización de particiones obsoletas.
- `glue`— Permite a los directores crear particiones, administrar tablas y acceder a las bases de datos del catálogo de AWS Glue datos para administrar los metadatos de Security Lake.
- `s3`— Permite a los directores administrar las configuraciones de los cubos de Amazon S3, las políticas del ciclo de vida y los objetos de metadatos para las operaciones del lago de datos de Security Lake.
- `logs`— Permite a los directores acceder a los flujos de CloudWatch registros y consultar los datos de registro para las funciones de Security Lake Lambda.
- `sqs`— Permite a los directores administrar las colas y los mensajes de Amazon SQS para los flujos de trabajo de procesamiento de datos de Security Lake.
- `lakeformation`— Permite a los directores recuperar la configuración y los permisos del lago de datos para la administración de los recursos de Security Lake.

Para ver más detalles sobre la política, incluyendo la última versión del documento de política JSON, consulte SecurityLakeResourceManagementServiceRolePolicy en la Guía de referencia de políticas administradas de AWS .

AWS política gestionada: AWS GlueServiceRole

La política `AWS GlueServiceRole` administrada invoca al AWS Glue rastreador y permite AWS Glue rastrear los datos de origen personalizados e identificar los metadatos de la partición. Estos metadatos son necesarios para crear y actualizar tablas en el catálogo de datos.

Para obtener más información, consulte Recopilación de datos de fuentes personalizadas en Security Lake.

Security Lake se actualiza a AWS políticas administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas para Security Lake desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de Security Lake.

Cambio	Descripción	Fecha
SecurityLakeResourceManagementServiceRolePolicy— Se actualizó la política existente	Security Lake actualizó la política administrada `SecurityLakeResourceManagementServiceRolePolicy` para agregar `lambda:DeleteFunction` permisos para Glue_Partition_Updater_Lambda las funciones SecurityLake _ obsoletas. Esto permite a Security Lake eliminar las funciones de Lambda obsoletas como parte de la migración a las fuentes de la versión 2 y al formato iceberg.	18 de noviembre de 2025
AWSServiceRoleForSecurityLakeResourceManagement— Política existente actualizada	Esta política se actualizó para reemplazar el `StringLike` operador por el `ArnLike` operador a fin de evaluar las ARN-type `lambda:FunctionArn` claves del bloque de `aws:ResourceAccount` condiciones. Esto proporciona una aplicación más segura.	25 de septiembre de 2025
Service-linked rol para Amazon Security Lake: nuevo rol vinculado a servicios	Hemos agregado un nuevo rol vinculado a un servicio. `AWSServiceRoleForSecurityLakeResourceManagement` Esta función vinculada a un servicio otorga permisos a Security Lake para	14 de noviembre de 2024

Cambio	Descripción	Fecha
	realizar mejoras continuas de monitoreo y rendimiento, lo que puede reducir la latencia y los costos.	
Service-linked rol para Amazon Security Lake: actualización de los permisos de rol vinculados a servicios existentes	Hemos añadido AWS WAF acciones a la política AWS gestionada para la `SecurityLakeServiceLinkedRole` política. Las acciones adicionales permiten a Security Lake recopilar AWS WAF registros cuando está habilitada como fuente de registros en Security Lake.	22 de mayo de 2024
AmazonSecurityLake PermissionsBoundary: actualización de una política actual	Security Lake agregó acciones de SID a la política.	13 de mayo de 2024
AmazonSecurityLake MetastoreManager: actualización de una política actual	Security Lake actualizó la política para agregar una acción de limpieza de metadatos que le permita eliminar los metadatos de su lago de datos.	27 de marzo de 2024

Cambio	Descripción	Fecha
AmazonSecurityLakeAdministrator: actualización de una política actual	Security Lake actualizó la política para permitir `iam:PassRole` la nueva `AmazonSecurityLakeMetastoreManagerV2` función y permitir que Security Lake implemente o actualice los componentes del lago de datos.	23 de febrero de 2024
AmazonSecurityLakeMetastoreManager: política nueva	Security Lake agregó una nueva política administrada que otorga permisos a Security Lake para administrar los metadatos en su lago de datos.	23 de enero de 2024
AmazonSecurityLakeAdministrator: política nueva	Security Lake agregó una nueva política administrada que otorga al principal acceso total a todas las acciones de Security Lake.	30 de mayo de 2023
Security Lake comenzó a rastrear los cambios	Security Lake comenzó a hacer un seguimiento de los cambios en sus políticas AWS administradas.	29 de noviembre de 2022

Uso de funciones vinculadas a servicios para Security Lake

Security Lake utiliza funciones vinculadas a AWS Identity and Access Management servicios (IAM). https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html#iam-term-service-linked-role Un rol vinculado a un servicio es un rol de IAM que está vinculado directamente a Security Lake. Está predefinido por Security Lake e incluye todos los permisos que Security Lake necesita para llamar a otras personas Servicios de AWS en su nombre y operar el servicio de lago de

datos de seguridad. Security Lake utiliza esta función vinculada a un servicio en todos los lugares en los Regiones de AWS que Security Lake está disponible.

La función vinculada a un servicio elimina la necesidad de agregar manualmente los permisos necesarios al configurar Security Lake. Security Lake define los permisos de este rol vinculado a un servicio y, a menos que se defina lo contrario, solo Security Lake puede asumir el rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte los permisos de Service-linked rol en la Guía del usuario de IAM. Solo puede eliminar un rol vinculado a servicios únicamente después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los AWS servicios que funcionan con IAM y busque los servicios que tienen la palabra Sí en la columna de funciones. Service-linked Seleccione una opción Sí con una conexión para revisar la documentación acerca del rol vinculado a un servicio en cuestión.

Temas

- Service-linked permisos de rol (SLR) para Security Lake
- Service-linked permisos de rol (SLR) para la administración de recursos

Service-linked permisos de rol (SLR) para Security Lake

Security Lake usa el rol vinculado a un servicio denominado. `AWSServiceRoleForSecurityLake` Este rol vinculado a servicios confía en el servicio `securitylake.amazonaws.com` para asumir el rol. Para obtener más información sobre las políticas AWS administradas de Amazon Security Lake, consulte la sección de AWS administración de políticas de Amazon Security Lake.

La política de permisos del rol, denominada política AWS gestionada`SecurityLakeServiceLinkedRole`, permite a Security Lake crear y operar el lago de datos de seguridad. También permite a Security Lake realizar tareas como las siguientes en los recursos especificados:

- Use AWS Organizations acciones para recuperar información sobre las cuentas asociadas

- Utilice Amazon Elastic Compute Cloud (Amazon EC2) para recuperar información sobre los registros de flujo de Amazon VPC
- Use AWS CloudTrail acciones para recuperar información sobre el rol vinculado al servicio
- Use AWS WAF acciones para recopilar AWS WAF registros cuando esté habilitada como fuente de registros en Security Lake
- Use `LogDelivery` la acción para crear o eliminar una suscripción de entrega de AWS WAF registros.

Para revisar los permisos de esta política, consulte SecurityLakeServiceLinkedRole en la Guía de referencia de la política administrada de AWS .

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte los permisos de los Service-linked roles en la Guía del usuario de IAM.

Creación del rol vinculado al servicio de Security Lake

No es necesario crear manualmente el rol `AWSServiceRoleForSecurityLake` vinculado al servicio para Security Lake. Cuando habilita Security Lake para usted Cuenta de AWS, Security Lake crea automáticamente el rol vinculado al servicio para usted.

Edición del rol vinculado al servicio de Security Lake

Security Lake no permite editar el rol vinculado al `AWSServiceRoleForSecurityLake` servicio. Una vez creado un rol vinculado a servicios, no puede cambiar el nombre del rol porque varias entidades pueden hacer referencia a este. Sin embargo, puede editar la descripción del rol mediante 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 de Security Lake

No puede eliminar el rol vinculado a un servicio de Security Lake. En su lugar, puede eliminar el rol vinculado al servicio de la consola de IAM, la API o. AWS CLI Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Antes de poder eliminar el rol vinculado a un servicio, primero debe confirmar que el rol no tiene sesiones activas y eliminar todos los recursos que esté utilizando. `AWSServiceRoleForSecurityLake`

> **Note**
>
> Si Security Lake usa el `AWSServiceRoleForSecurityLake` rol cuando intenta eliminar los recursos, es posible que no se eliminen. En ese caso, espere unos minutos e intente de nuevo la operación.

Si elimina el rol `AWSServiceRoleForSecurityLake` vinculado al servicio y necesita volver a crearlo, puede volver a crearlo habilitando Security Lake para su cuenta. Cuando vuelva a habilitar Security Lake, Security Lake volverá a crear automáticamente el rol vinculado al servicio para usted.

compatible Regiones de AWS para el rol vinculado al servicio de Security Lake

Security Lake admite el uso del rol `AWSServiceRoleForSecurityLake` vinculado al servicio en todos los lugares en los que Security Lake Regiones de AWS esté disponible. Para obtener una lista de las regiones en las que Security Lake está disponible actualmente, consulte Regiones y puntos finales de Security Lake.

Service-linked permisos de rol (SLR) para la administración de recursos

Security Lake utiliza la función vinculada a servicios denominada `AWSServiceRoleForSecurityLakeResourceManagement` para realizar mejoras continuas de supervisión y rendimiento, lo que puede reducir la latencia y los costos. Este rol vinculado a servicios confía en el servicio `resource-management.securitylake.amazonaws.com` para asumir el rol. La activación también `AWSServiceRoleForSecurityLakeResourceManagement` le permitirá acceder a Lake Formation y registrar automáticamente los depósitos S3 gestionados por Security Lake en Lake Formation en todas las regiones para mejorar la seguridad.

La política de permisos del rol, denominada política AWS administrada`SecurityLakeResourceManagementServiceRolePolicy`, permite acceder a los recursos creados por Security Lake para administrar los recursos creados por Security Lake, incluida la administración de los metadatos de su lago de datos. Para obtener más información sobre las políticas AWS administradas de Amazon Security Lake, consulte las políticas AWS administradas de Amazon Security Lake.

Esta función vinculada a un servicio permite a Security Lake supervisar el estado de los recursos desplegados por Security Lake (el bucket de S3, AWS Glue las tablas, la cola de Amazon SQS, la función Lambda de Metastore Manager (MSM) y las reglas) en su cuenta. EventBridge Algunos

ejemplos de operaciones que Security Lake puede realizar con esta función vinculada a un servicio son:

- La compactación de archivos de manifiesto de Apache Iceberg, que mejora el rendimiento de las consultas y reduce los tiempos y costos de procesamiento de Lambda MSM.
- Supervise el estado de Amazon SQS para detectar problemas de ingestión.
- Optimice la replicación de datos entre regiones para excluir los archivos de metadatos.

> **Note**
>
> Si no instala la función `AWSServiceRoleForSecurityLakeResourceManagement` vinculada a servicios, Security Lake seguirá funcionando, pero se recomienda encarecidamente aceptar esta función vinculada a servicios para que Security Lake pueda supervisar y optimizar los recursos de su cuenta.

Detalles de los permisos

El rol se configura con la siguiente política de permisos:

- `events`— Permite a los directores administrar EventBridge las reglas necesarias para las fuentes y los suscriptores de registros.
- `lambda`— Permite a los principales administrar la lambda utilizada para actualizar las particiones de las AWS Glue tablas después de la entrega del AWS código fuente y la replicación entre regiones.
- `glue`— Permite a los directores realizar acciones de escritura específicas para las tablas del catálogo de datos. AWS Glue Esto también permite a AWS Glue los rastreadores identificar las particiones de sus datos y permite a Security Lake administrar los metadatos de Apache Iceberg para sus tablas de Apache Iceberg.
- `s3`— Permite a los directores realizar acciones específicas de lectura y escritura en los buckets de Security Lake que contienen los datos de registro y los metadatos de la tabla Glue.
- `logs`— Permite a los directores el acceso de lectura para registrar el resultado de la función Lambda en Logs. CloudWatch

- `sqs`— Permite a los directores realizar acciones de lectura y escritura específicas para las colas de Amazon SQS que reciben notificaciones de eventos cuando se añaden objetos a su lago de datos o se actualizan en él.
- `lakeformation`— Permite a los directores leer la configuración de Lake Formation para detectar errores de configuración.

Para revisar los permisos de esta política, consulte SecurityLakeResourceManagementServiceRolePolicy en la Guía de referencia de la política administrada de AWS .

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte los permisos de los Service-linked roles en la Guía del usuario de IAM.

Creación del rol vinculado al servicio de Security Lake

Puede crear la función `AWSServiceRoleForSecurityLakeResourceManagement` vinculada al servicio para Security Lake mediante la consola de Security Lake o la. AWS CLI

Para crear el rol vinculado a un servicio, debe conceder los siguientes permisos a su usuario o rol de IAM. El rol de IAM debe ser el de administrador de Lake Formation en todas las regiones habilitadas para Security Lake.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLakeFormationActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "AllowIamActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:PutRolePolicy"
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/resource-
management.securitylake.amazonaws.com/
AWSServiceRoleForSecurityLakeResourceManagement",
        "arn:*:iam::*:role/*AWSServiceRoleForLakeFormationDataAccess",
        "arn:*:iam::aws:policy/service-role/AWSGlueServiceRole",
        "arn:*:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager",
        "arn:*:iam::aws:policy/aws-service-role/
SecurityLakeResourceManagementServiceRolePolicy"
      ],
      "Condition": {
        "StringLikeIfExists": {
          "iam:AWSServiceName": [
            "securitylake.amazonaws.com",
            "resource-management.securitylake.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowGlueActionsViaConsole",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:*:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ]
    }
  ]
```

```
}
```

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Para aceptar el nuevo rol vinculado al servicio, haga clic en Habilitar el rol vinculado al servicio en la barra de información de la página de resumen.

Una vez que haya habilitado el rol vinculado a un servicio, no necesitará repetir este proceso para usar Security Lake en el futuro.

CLI

Para crear el rol `AWSServiceRoleForSecurityLakeResourceManagement` vinculado a un servicio de forma programática, utilice el siguiente comando de la CLI.

```
$ aws iam create-service-linked-role
--aws-service-name resource-management.securitylake.amazonaws.com
```

Al crear el rol `AWSServiceRoleForSecurityLakeResourceManagement` vinculado a un servicio mediante AWS CLI, también debe concederle permisos de nivel de tabla de Lake Formation (ALTER, DESCRIBE) a todas las tablas de la base de datos de Security Lake Glue para administrar los metadatos de las tablas y acceder a los datos. Si las tablas de Glue de cualquier región hacen referencia a cubos de S3 de una activación anterior de Security Lake, debes conceder temporalmente los permisos de DATA_LOCATION_ACCESS a la función vinculada al servicio para que Security Lake pueda corregir esta situación.

También tienes que conceder permisos a Lake Formation para la función vinculada al servicio de tu cuenta. `AWSServiceRoleForSecurityLakeResourceManagement`

El siguiente ejemplo muestra cómo conceder los permisos de Lake Formation al rol vinculado a un servicio en la región designada. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws lakeformation grant-permissions --region {region} --principal
 DataLakePrincipalIdentifier={AWSServiceRoleForSecurityLakeResourceManagement ARN} \
--permissions ALTER DESCRIBE --resource '{ "Table": { "DatabaseName":
 "amazon_security_lake_glue_db_{region}", "TableWildcard": {} } }'
```

El siguiente ejemplo muestra el aspecto que tendrá el ARN del rol. Debe editar el ARN del rol para que coincida con su región.

```
"AWS": "arn:[partition]:iam::[accountid]:role/aws-service-
role/resource-management.securitylake.amazonaws.com/
AWSServiceRoleForSecurityLakeResourceManagement"
```

También puedes usar la llamada a la CreateServiceLinkedRole API. En la solicitud, especifique el `AWSServiceName` como`resource-management.securitylake.amazonaws.com`.

Tras habilitar la `AWSServiceRoleForSecurityLakeResourceManagement` función, si utiliza la clave gestionada por el AWS KMS cliente (CMK) para el cifrado, debe permitir que la función vinculada al servicio escriba objetos cifrados en los buckets de S3 de AWS las regiones en las que exista la CMK. En la AWS KMS consola, agregue la siguiente política a la clave de KMS en las regiones en las que existe la AWS CMK. Para obtener más información sobre cómo cambiar la política de claves de KMS, consulte las políticas de claves AWS KMS en la Guía para AWS Key Management Service desarrolladores.

```
{
    "Sid": "Allow SLR",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::[regional-datalake-s3-
bucket-name]"
        },
        "StringLike": {
            "kms:ViaService": "s3.[region].amazonaws.com"
        }
    }
},
```

Edición del rol vinculado al servicio de Security Lake

Security Lake no permite editar el rol vinculado al `AWSServiceRoleForSecurityLakeResourceManagement` servicio. Una vez creado un rol vinculado a servicios, no puede cambiar el nombre del rol porque varias entidades pueden hacer referencia a este. Sin embargo, puede editar la descripción del rol mediante 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 de Security Lake

No puede eliminar el rol vinculado a un servicio de Security Lake. En su lugar, puede eliminar el rol vinculado al servicio de la consola de IAM, la API o. AWS CLI Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Antes de poder eliminar el rol vinculado a un servicio, primero debe confirmar que el rol no tiene sesiones activas y eliminar todos los recursos que esté utilizando. `AWSServiceRoleForSecurityLakeResourceManagement`

> **Note**
>
> Si Security Lake usa el `AWSServiceRoleForSecurityLakeResourceManagement` rol cuando intenta eliminar los recursos, es posible que no se eliminen. En ese caso, espere unos minutos e intente de nuevo la operación.

Si elimina el rol `AWSServiceRoleForSecurityLakeResourceManagement` vinculado al servicio y necesita volver a crearlo, puede volver a crearlo habilitando Security Lake para su cuenta. Cuando vuelva a habilitar Security Lake, Security Lake volverá a crear automáticamente el rol vinculado al servicio para usted.

compatible Regiones de AWS para el rol vinculado al servicio de Security Lake

Security Lake admite el uso del rol `AWSServiceRoleForSecurityLakeResourceManagement` vinculado al servicio en todos los lugares en los que Security Lake Regiones de AWS esté disponible. Para obtener una lista de las regiones en las que Security Lake está disponible actualmente, consulte Regiones y puntos finales de Security Lake.

Protección de los datos en Amazon Security Lake

El modelo de responsabilidad AWS https://aws.amazon.com/compliance/shared-responsibility-model/ se aplica a la protección de datos en Amazon Security Lake. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todo el 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, consulte las Preguntas frecuentes sobre la privacidad de los datos y las condiciones legales de la región de . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios 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.
- Úselo SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure el registro de actividad de los usuarios y de la API con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail rutas para capturar AWS actividades, consulte Cómo trabajar con CloudTrail rutas en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contiene Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por la FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte 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 trabaja con Security Lake u otro tipo de software

Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Amazon Security Lake almacena de forma segura sus datos en reposo mediante soluciones de AWS cifrado. Los registros de seguridad sin procesar y los datos de eventos se almacenan en depósitos de Amazon Simple Storage Service (Amazon S3) multiusuario específicos de la fuente en una cuenta que administra Security Lake. Cada fuente de registro tiene su propio depósito multiusuario. Security Lake cifra estos datos sin procesar con una clave AWS propia de AWS Key Management Service ()AWS KMS. AWS Las claves propias son un conjunto de AWS KMS claves que un AWS servicio (en este caso Security Lake) posee y administra para su uso en varias cuentas. AWS

Security Lake ejecuta trabajos de extracción, transformación y carga (ETL) en datos de registro y eventos sin procesar.

Una vez finalizados los trabajos de ETL, Security Lake crea depósitos S3 de un solo inquilino en su cuenta (un depósito por cada depósito en el Región de AWS que haya habilitado Security Lake). Los datos se almacenan en los buckets S3 de múltiples inquilinos solo de forma temporal hasta que Security Lake pueda entregarlos de manera confiable a los buckets S3 de un solo inquilino. Los buckets de un solo inquino incluyen una política basada en los recursos que permite a Security Lake escribir datos de registro y eventos en los buckets. Para cifrar los datos de su bucket de S3, puede elegir entre una clave de S3-managed cifrado o una clave gestionada por el cliente (from). AWS KMS Ambas opciones utilizan el cifrado simétrico.

Uso de una clave KMS para el cifrado de datos

De forma predeterminada, los datos que Security Lake envía a su bucket de S3 se cifran mediante el cifrado del lado del servidor de Amazon con las claves de cifrado de Amazon S3-managed (). SSE-S3 Para proporcionar una capa de seguridad que pueda administrar directamente, puede utilizar el cifrado del lado del servidor con AWS KMS claves (SSE-KMS) para sus datos de Security Lake.

SSE-KMS no es compatible con la consola de Security Lake. Para usarla SSE-KMS con la API o la CLI de Security Lake, primero debe crear una clave de KMS o usar una clave existente. Es preciso adjuntar una política a la clave que determine qué usuarios pueden utilizar la clave para cifrar y descifrar datos de Security Lake.

Si usa una clave administrada por el cliente para cifrar los datos que están escritos en su bucket de S3, no podrá elegir una clave multirregional. En el caso de las claves administradas por el cliente, Security Lake crea una concesión en su nombre enviando una solicitud `CreateGrant` a AWS KMS. Las concesiones se AWS KMS utilizan para dar a Security Lake acceso a una clave de KMS en una cuenta de cliente.

Security Lake necesita la concesión para utilizar la clave administrada por el cliente para las siguientes operaciones internas:

- Envíe `GenerateDataKey` solicitudes AWS KMS para generar claves de datos cifradas con la clave gestionada por el cliente.
- Envíe `RetireGrant` las solicitudes a AWS KMS. Al realizar actualizaciones en su lago de datos, esta operación permite retirar la subvención que se agregó a la clave de AWS KMS para el procesamiento de ETL.

Security Lake no necesita permisos de `Decrypt`. Cuando los usuarios autorizados de la clave leen datos de Security Lake, S3 administrar el descifrado y los usuarios autorizados pueden leer datos ya sin cifrado. Sin embargo, un suscriptor necesita permisos `Decrypt` para consumir los datos de origen. Para obtener más información acerca de los permisos de suscriptor, consulte Administración del acceso a los datos para los suscriptores de Security Lake.

Si desea usar una clave de KMS existente para cifrar los datos de Security Lake, debe modificar la política de claves de la clave de KMS. La política de claves debe permitir que el rol de IAM asociado a la ubicación del lago de datos de Lake Formation utilice la clave de KMS para descifrar los datos. Para obtener instrucciones sobre cómo cambiar la política de claves de una clave de KMS, consulte Cambiar una política de claves en la Guía para AWS Key Management Service desarrolladores.

Su clave de KMS puede aceptar solicitudes de concesión, lo que permite a Security Lake acceder a la clave, siempre que cree una política de claves o utilice una política de claves existente con los permisos adecuados. Para obtener instrucciones sobre cómo crear una política de claves, consulte Creación de una política de claves en la Guía para desarrolladores de AWS Key Management Service .

Adjunte la siguiente política de claves a la clave de KMS:

```
{
  "Sid": "Allow use of the key",
```

```
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Permisos de IAM necesarios cuando se utiliza una clave administrada por el cliente

Consulte la sección Primeros pasos: requisitos previos para obtener una descripción general de los roles de IAM que debe crear para usar Security Lake.

Al añadir un origen personalizado o un suscriptor, Security Lake crea roles de IAM en su cuenta. Estos roles están diseñados para compartirse con otras identidades de IAM. Permiten que un origen personalizado escriba datos en el lago de datos y que un suscriptor consuma datos del lago de datos. Una política AWS administrada denominada `AmazonSecurityLakePermissionsBoundary` establece los límites de permisos para estas funciones.

Cifrado de colas de Amazon SQS

Al crear el lago de datos, Security Lake crea dos colas de Amazon Simple Queue Service (Amazon SQS) sin cifrar en la cuenta de administrador de Security Lake delegada. Debe cifrar estas colas para proteger los datos. El cifrado del servidor (SSE) predeterminado proporcionado por Amazon Simple Queue Service no es suficiente. Debe crear una clave gestionada por el cliente en AWS Key Management Service (AWS KMS) para cifrar las colas y conceder al principal del servicio Amazon S3 los permisos necesarios para trabajar con las colas cifradas. Para obtener instrucciones sobre cómo conceder estos permisos, consulte ¿Por qué las notificaciones de eventos de Amazon S3 no se envían a una cola de Amazon SQS que utiliza el cifrado del lado del servidor? en el Centro de conocimiento. AWS

Dado que Security Lake AWS Lambda admite trabajos de extracción, transferencia y carga (ETL) en sus datos, también debe conceder permisos a Lambda para administrar los mensajes de las colas de Amazon SQS. Para obtener información, consulte Permisos del rol de ejecución en la Guía para desarrolladores de AWS Lambda .

Cifrado en tránsito

Security Lake cifra todos los datos en tránsito entre los servicios. AWS Security Lake protege los datos en tránsito, a medida que viajan hacia y desde el servicio, cifrando automáticamente todos los datos entre redes mediante el protocolo de cifrado seguridad de la capa de transporte (TLS) 1.2. Las solicitudes HTTPS directas enviadas a las API de Security Lake se firman mediante el Algoritmo AWS Signature versión 4 para establecer una conexión segura.

Desactivación del uso de los datos para mejorar el servicio

Puede optar por no utilizar sus datos para desarrollar y mejorar Security Lake y otros servicios de AWS seguridad mediante la política de AWS Organizations exclusión voluntaria. Puede optar por que se le excluya incluso si Security Lake no recopila actualmente dichos datos. Para más información sobre cómo excluirse, consulte Políticas de exclusión de servicios de IA en la Guía del usuario de AWS Organizations .

En la actualidad, Security Lake no recopila ninguno de los datos de seguridad que procesa en su nombre ni los datos de seguridad que usted carga en su lago de datos de seguridad creado por este servicio. Para desarrollar y mejorar el servicio de Security Lake y las funcionalidades de otros servicios de AWS seguridad, Security Lake puede recopilar dichos datos en el futuro, incluidos los datos que usted cargue de fuentes de datos de terceros. Actualizaremos esta página cuando Security Lake pretenda recopilar dichos datos y describiremos cómo se realizará. Seguirá teniendo la oportunidad de no participar en la recopilación en cualquier momento.

> **Note**
>
> Para poder utilizar la política de exclusión voluntaria, sus AWS cuentas deben ser administradas de forma centralizada por AWS Organizations. Si aún no has creado una organización para tus AWS cuentas, consulta Cómo crear y administrar una organización en la Guía del AWS Organizations usuario.

La exclusión tiene los siguientes efectos:

- Security Lake eliminará los datos que ha recopilado y almacenado antes de su exclusión voluntaria (si los hubiera).
- Tras optar por no participar voluntariamente, Security Lake ya no recopilará ni almacenará estos datos.

Validación de la conformidad para Amazon Security Lake

Nuestra nueva experiencia AWS de registro no está diseñada para cargas de trabajo reguladas. Si utilizas nuestra nueva experiencia de AWS registro, pero quieres utilizarla AWS para cargas de trabajo reguladas, puedes suscribirte a una versión AWS (avanzada) o activar funciones avanzadas para tu entorno. AWS

Para saber si una Servicio de AWS está dentro del ámbito de un programa de cumplimiento específico, consulte Servicios de AWS la sección Alcance por programa de cumplimiento y seleccione el programa de cumplimiento que le interese. Para obtener información general, consulte Programas AWS de cumplimiento Programas .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descargar informes en AWS Artifact .

Su responsabilidad de cumplimiento al usarlos Servicios de AWS viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y normativas aplicables. Para obtener más información sobre su responsabilidad de cumplimiento al usarlos Servicios de AWS, consulte la documentación AWS de seguridad.

Prácticas recomendadas de seguridad para Security Lake

Vea las prácticas recomendadas siguientes para trabajar con Amazon Security Lake.

Otorgar los permisos mínimos posibles a los usuarios de Security Lake

Siga el principio de privilegios mínimos y conceda el conjunto mínimo de permisos de política de acceso a sus usuarios, grupos de usuarios y funciones AWS Identity and Access Management (IAM). Por ejemplo, puede permitir que un usuario de IAM vea una lista de orígenes de registro en Security Lake, pero no cree orígenes ni suscriptores. Para obtener más información, consulte Ejemplos de políticas basadas en la identidad para Security Lake

También puede utilizarlos AWS CloudTrail para realizar un seguimiento del uso de la API en Security Lake. CloudTrail proporciona un registro de las acciones de API realizadas por un usuario, grupo o rol en Security Lake. Para obtener más información, consulte Registro de llamadas a la API de Security Lake mediante CloudTrail.

Ver la página de resumen de Resumen

La página Resumen de la consola de Security Lake proporciona información general sobre los problemas de los últimos 14 días que están afectando al servicio de Security Lake y a los buckets de Amazon S3 en los que se almacenan sus datos. Puede investigar más a fondo estos problemas para mitigar el posible impacto relacionado con la seguridad.

Intégrelo con Security Hub (CSPM).

Integre Security Lake y reciba AWS Security Hub CSPM las conclusiones del CSPM de Security Hub en Security Lake. El CSPM de Security Hub genera hallazgos a partir de muchas integraciones diferentes Servicios de AWS y de terceros. Recibir las conclusiones del CSPM de Security Hub le ayuda a obtener una visión general de su postura en materia de cumplimiento y de si está cumpliendo con las prácticas recomendadas de seguridad. AWS

Para obtener más información, consulte Integración con AWS Security Hub CSPM.

Eliminar AWS Lambda

Al eliminar una AWS Lambda función, te recomendamos que no la deshabilites primero. La desactivación de una función de Lambda antes de eliminarla podría interferir con las capacidades de consulta de datos y, potencialmente, afectar a otras funcionalidades. Es mejor eliminar la función Lambda directamente sin deshabilitarla. Para obtener más información sobre cómo eliminar la función Lambda, consulte AWS Lambda la guía para desarrolladores.

Supervisión de los eventos de Security Lake

Puede supervisar Security Lake mediante las CloudWatch métricas de Amazon. CloudWatch recopila datos sin procesar de Security Lake cada minuto y los procesa para convertirlos en métricas. Puede configurar alarmas que activen notificaciones cuando las métricas coincidan con los umbrales especificados.

Para obtener más información, consulte CloudWatch métricas de Amazon Security Lake.

Resiliencia de Amazon Security Lake

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Estas zonas de disponibilidad ofrecen un medio eficaz de diseñar y utilizar aplicaciones y bases de datos. Las

zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

La disponibilidad de Security Lake está vinculada a la disponibilidad de la región. La distribución en varias zonas de disponibilidad ayuda al servicio a tolerar los fallos en una sola zona de disponibilidad.

La disponibilidad del plano de datos de Security Lake no está vinculada a la disponibilidad de ninguna región. Sin embargo, la disponibilidad del plano de control de Security Lake está estrechamente vinculada a la disponibilidad en la región Este de EE. UU. (Norte de Virginia).

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Security Lake, en la que los datos están respaldados por Amazon Simple Storage Service (Amazon S3), ofrece varias funciones que ayudan a respaldar sus necesidades de respaldo y resiliencia de datos.

Configuración del ciclo de vida

La configuración del ciclo de vida es un conjunto de reglas que definen acciones que Amazon S3 aplica a un grupo de objetos. Con las reglas de configuración del ciclo de vida, puede indicarle a Amazon S3 que pase los objetos a otras clases de almacenamiento más económicas, que los archive o que los elimine. Para obtener más información, consulte Administración del ciclo de vida de almacenamiento en la Guía del usuario de Amazon S3.

Control de versiones

El control de versiones es una forma de conservar diversas variantes de un objeto en el mismo bucket. Puede utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. EL control de versiones ayuda a recuperarse de acciones no deseadas del usuario y de errores de la aplicación. Para obtener más información, consulte Uso del control de versiones en buckets de S3 en la Guía de usuario de Amazon S3.

Clases de almacenamiento

Amazon S3 ofrece una gama de clases de almacenamiento para elegir según los requisitos de la carga de trabajo. Las clases de almacenamiento S3 Standard-IA y S3 One Zone-IA están diseñadas para datos a los que se accede aproximadamente una vez al mes y necesitan acceso en milisegundos. La clase de almacenamiento S3 Glacier Instant Retrieval está diseñada para datos de archivo de larga duración a los que se accede aproximadamente una vez por trimestre

con acceso en milisegundos. Para los datos de archivo que no requieren acceso inmediato, como las copias de seguridad, puede utilizar las clases de almacenamiento S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Para obtener más información, consulte Uso de clases de almacenamiento de Amazon S3 en la Guía para usuarios de Amazon S3.

Seguridad de infraestructuras en Amazon Security Lake

Como servicio gestionado, Amazon Security Lake está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Security Lake 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.

Configuración y análisis de vulnerabilidades en Security Lake

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Amazon Security Lake y puntos de enlace de VPC de interfaz ()AWS PrivateLink

Puede establecer una conexión privada entre su VPC y Amazon Security Lake mediante la creación de un punto de enlace de VPC de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a Security Lake APIs sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. AWS PrivateLink Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con Security Lake. APIs El tráfico entre tu VPC y Security Lake no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía de AWS PrivateLink .

Consideraciones sobre los puntos finales de VPC de Security Lake

Antes de configurar un punto final de VPC de interfaz para Security Lake, asegúrese de revisar las propiedades y limitaciones del punto final de la interfaz en la AWS PrivateLink Guía.

Security Lake permite realizar llamadas a todas sus acciones de API desde su VPC.

Security Lake admite puntos finales de VPC FIPS solo en las siguientes regiones donde existe FIPS:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)

Creación de un punto final de VPC de interfaz para Security Lake

Puede crear un punto de enlace de VPC para el servicio Security Lake mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLI Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree un punto final de VPC para Security Lake con el siguiente nombre de servicio:

- com.amazonaws. *region*.securitylake
- com.amazonaws. *region*.securitylake-fips (punto final FIPS)

Si habilita el DNS privado para el punto final, puede realizar solicitudes de API a Security Lake utilizando su nombre de DNS predeterminado para la región, por ejemplo. `securitylake.us-east-1.amazonaws.com`

Para obtener más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Creación de una política de puntos finales de VPC para Security Lake

Puede adjuntar una política de punto final a su punto final de VPC que controle el acceso a Security Lake. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la Guía de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones de Security Lake

El siguiente es un ejemplo de una política de puntos finales para Security Lake. Cuando se adjunta a un punto final, esta política otorga acceso a las acciones de Security Lake enumeradas a todos los principales de todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers"
         ],
         "Resource":"*"
      }
   ]
}
```

Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes que se compartan con usted. Para obtener información sobre el uso compartido de VPC, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Supervisión de Amazon Security Lake

Security Lake se integra con AWS CloudTrail, que es un servicio que proporciona un registro de las acciones que un usuario, un rol u otro realizó en Security Lake Servicio de AWS. Entre estas se incluyen las acciones realizadas desde la consola de Security Lake y las llamadas mediante programación a las operaciones de la API de Security Lake. Al utilizar la información recopilada por CloudTrail, puede determinar qué solicitudes se realizaron a Security Lake. Para cada solicitud, puede identificar cuándo se realizó, la dirección IP desde la que se realizó, quién la realizó e información adicional. Para obtener más información, consulte Registro de llamadas a la API de Security Lake mediante CloudTrail.

Security Lake y Amazon CloudWatch están integrados, por lo que puede recopilar, ver y analizar las métricas de los registros que recopila Security Lake. CloudWatch Las métricas de su lago de datos de Security Lake se recopilan automáticamente y se actualizan CloudWatch en intervalos de un minuto. También puede configurar una alarma que le envíe una notificación si se llega a un umbral especificado en una métrica de Security Lake. Para ver una lista de todas las métricas a las que envía Security Lake CloudWatch, consulteMétricas y dimensiones de Security Lake.

CloudWatch métricas de Amazon Security Lake

Puedes monitorizar Security Lake con Amazon CloudWatch, que recopila datos sin procesar cada minuto y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre los datos del lago de datos. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales.

Temas

- Métricas y dimensiones de Security Lake
- Visualización CloudWatch de las métricas de Security Lake
- Configurar CloudWatch alarmas para las métricas de Security Lake

Métricas y dimensiones de Security Lake

El espacio de nombres de `AWS/SecurityLake` incluye las siguientes métricas.

Métrica	Description (Descripción)
`ProcessedSize`	El volumen de datos compatibles de forma nativa Servicios de AWS que se encuentra actualmente almacenado en su lago de datos. Unidades: bytes

Las siguientes dimensiones están disponibles para métricas de Security Lake.

Dimensión	Description (Descripción)
`Account`	Métrica de `ProcessedSize` para una Cuenta de AWS específica. Esta dimensión solo está disponible cuando la ves activada. `Per-Account Source Version Metrics` CloudWatch
`Region`	Métrica de `ProcessedSize` para una Región de AWS específica.
`Source`	`ProcessedSize` métrica para una fuente de AWS registro específica.
`SourceVersion`	`ProcessedSize` métrica para una versión específica de una fuente de AWS registro.

Puedes ver las métricas de una cuenta específica Cuentas de AWS (`Per-Account Source Version Metrics`) o de todas las cuentas de una organización (`Per-Source Version Metrics`).

Visualización CloudWatch de las métricas de Security Lake

Puede supervisar las métricas de Security Lake mediante la CloudWatch consola, la propia interfaz CloudWatch de línea de comandos (CLI) o mediante programación mediante la CloudWatch API. Elija el método que prefiera y siga estos pasos para acceder a las métricas de Security Lake.

CloudWatch console

1. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/
2. En el panel de navegación, elija Métricas, Todas las métricas.
3. En la pestaña Explorar, seleccione Security Lake.
4. Seleccione Métricas de versión de origen por cuenta o Métricas de versión por origen.
5. Seleccione una métrica para verla en detalle. También puede hacer lo siguiente:
   - Para ordenar las métricas, utilice el encabezado de columna.
   - Para representar gráficamente una métrica, seleccione su nombre y elija una opción de representación gráfica.
   - Para filtrar por métrica, seleccione el nombre de la métrica y, a continuación, Añadir a búsqueda.

CloudWatch API

Para acceder a las métricas de Security Lake mediante la CloudWatch API, utilice la `GetMetricStatistics`acción.

AWS CLI

Para acceder a las métricas de Security Lake mediante el AWS CLI, ejecute el `get-metric-statistics`comando.

Para obtener más información sobre la supervisión mediante métricas, consulta Cómo usar CloudWatch métricas de Amazon en la Guía del CloudWatch usuario de Amazon.

Configurar CloudWatch alarmas para las métricas de Security Lake

CloudWatch también permite configurar alarmas cuando se alcanza un umbral para una métrica. Por ejemplo, puede configurar una alarma para la ProcessedSizemétrica, de modo que se le notifique cuando el volumen de datos de una fuente específica supere un umbral específico.

Para obtener instrucciones sobre cómo configurar las alarmas, consulta Uso de CloudWatch las alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

Registro de llamadas a la API de Security Lake mediante CloudTrail

Amazon Security Lake se integra con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Security Lake. CloudTrail captura las llamadas a la API de Security Lake como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Security Lake y las llamadas desde el código a las operaciones de la API de Security Lake. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Security Lake. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Security Lake, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre Security Lake en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Security Lake, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los de Security Lake, crea una ruta. Un registro permite CloudTrail entregar eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail

- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Las acciones de Security Lake se registran CloudTrail y se documentan en la referencia de la API de Security Lake. Por ejemplo, las llamadas a las `UpdateDataLake` `CreateSubscriber` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `ListLogSources`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de AWS Identity and Access Management usuario o raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte Elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de registro de Security Lake

CloudTrail los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro para la `GetSubscriber` acción de Security Lake.


```
{
   "eventVersion": "1.08",
   "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE:user",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/user",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
```

```
         "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "Admin"
         },
         "webIdFederationData": {
         },
         "attributes": {
            "creationDate": "2023-05-30T13:27:19Z",
            "mfaAuthenticated": "false"
         }
      }
   },
   "eventTime": "2023-05-30T17:29:17Z",
   "eventSource": "securitylake.amazonaws.com",
   "eventName": "GetSubscriber",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "198.51.100.1",
   "userAgent": "console.amazonaws.com",
   "requestParameters": {
      "subscriberId": "30ed17a3-0cac-4997-a41f-f5a6bexample"
   },
   "responseElements": null,
   "requestID": "d01f0f32-9ec6-4579-af50-e9f14example",
   "eventID": "9c1bff41-0f48-4ee6-921c-ebfd8example",
   "readOnly": false,
   "eventType": "AwsApiCall",
   "managementEvent": true,
   "recipientAccountId": "123456789012",
   "eventCategory": "Management"
}
```

Etiquetado de los recursos de Security Lake

Una etiqueta es una etiqueta opcional que puede definir y asignar a AWS los recursos, incluidos determinados tipos de recursos de Amazon Security Lake. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre recursos o identificar los recursos que respaldan determinados requisitos de cumplimiento o flujos de trabajo.

Puede asignar etiquetas a los siguientes tipos de recursos de Security Lake: los suscriptores y la configuración del lago de datos individual Regiones de AWS. Cuenta de AWS

Temas

- Conceptos básicos del etiquetado
- Uso de etiquetas en políticas de IAM
- Adición de etiquetas a los recursos de Amazon Security Lake
- Edición de etiquetas para los recursos de Amazon Security Lake
- Eliminación de etiquetas de los recursos de Amazon Security Lake

Conceptos básicos del etiquetado

Un recurso puede tener hasta 50 etiquetas. Cada etiqueta está formada por una clave de etiqueta y un valor de etiqueta opcional, ambos definidos por el usuario. Un clave de etiqueta es una etiqueta general que actúa como una categoría para un valor de etiqueta más específicos. Un valor de etiqueta actúa como descriptor de una clave de etiqueta.

Por ejemplo, si agrega suscriptores para analizar los datos de seguridad de diferentes entornos (un conjunto de suscriptores para los datos de nube y otro conjunto para los datos en las instalaciones), puede asignar una clave de etiqueta `Environment` a esos suscriptores. El valor de la etiqueta asociada puede ser `Cloud` para los suscriptores que analizan datos de Servicios de AWS y `On-Premises` para los demás.

A la hora de definir y asignar etiquetas a los recursos de Amazon Security Lake, tenga en cuenta lo siguiente:

- Cada recurso puede tener un máximo de 50 etiquetas.

- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Le recomendamos que defina una estrategia de uso de mayúsculas y minúsculas en las etiquetas e implemente esa estrategia sistemáticamente en todos los recursos.
- Una clave de etiqueta puede tener un máximo de 128 caracteres UTF-8. Una clave de valor puede tener un máximo de 256 caracteres UTF-8. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @
- El `aws:` prefijo está reservado para su uso por AWS. No puede usarlo en las claves o valores de etiqueta que defina. Además, las claves o valores de etiqueta que utilizan este prefijo no se pueden cambiar ni quitar. Las etiquetas que usan este prefijo no cuentan para la cuota de 50 etiquetas por recurso.
- Las etiquetas que asigne estarán disponibles solo para usted Cuenta de AWS y solo en el lugar Región de AWS en el que las asigne.
- Si asigna etiquetas a un recurso mediante Security Lake, las etiquetas se aplicarán únicamente al recurso que esté almacenado directamente en Security Lake, en la Región de AWS correspondiente. No se aplican a ningún recurso de apoyo asociado que Security Lake cree, utilice o mantenga para usted en otros Servicios de AWS. Por ejemplo, si asigna etiquetas a su lago de datos, las etiquetas se aplican únicamente a la configuración de su lago de datos en Security Lake para la región especificada. No se aplican al bucket de Amazon Simple Storage Service (Amazon S3) que almacena los datos de registro y eventos. Para asignar también etiquetas a un recurso asociado, puede usar Grupos de recursos de AWS o el Servicio de AWS que almacena el recurso, por ejemplo, Amazon S3 para un bucket de S3. La asignación de etiquetas a los recursos asociados puede ayudarle a identificar los recursos de apoyo para su lago de datos.
- Si elimina un recurso, también se eliminarán todas las etiquetas que tenga asignadas.

Para obtener más información sobre restricciones, consejos y prácticas recomendadas, consulte Etiquetar sus AWS recursos en la Guía del usuario sobre cómo AWS etiquetar los recursos.

> **Important**
>
> No almacene datos confidenciales en etiquetas. Se puede acceder a las etiquetas desde muchas de ellas Servicios de AWS, entre ellas. Administración de facturación y costos de AWS No se diseñaron para utilizarse con información confidencial.

Para agregar y administrar etiquetas para los recursos de Security Lake, puede usar la consola de Security Lake o la API de Security Lake.

Uso de etiquetas en políticas de IAM

Una vez que comience a etiquetar los recursos, puede definir permisos de recursos basados en etiquetas en las políticas de AWS Identity and Access Management (IAM). Al usar las etiquetas de esta manera, puede implementar un control pormenorizado sobre qué usuarios y roles de su Cuenta de AWS empresa tienen permiso para crear y etiquetar recursos, y qué usuarios y roles tienen permiso para añadir, editar y eliminar etiquetas de manera más general. Para controlar el acceso basándose función de etiquetas, puede utilizar claves de condición relacionadas con las etiquetas en el elemento Condition de las políticas de IAM.

Por ejemplo, puede crear una política que permita a un usuario tener acceso completo a todos los recursos de Amazon Security Lake si la etiqueta `Owner` del recurso especifica su nombre de usuario:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Si define los permisos de nivel de recurso basados en etiquetas, estos entrarán en vigor inmediatamente. Esto significa que sus recursos están más seguros en cuanto se crean y que puede empezar a aplicar el uso de etiquetas de nuevos recursos rápidamente. También puede usar permisos de nivel de recurso para controlar las claves y valores de etiqueta que se pueden asociar a

recursos nuevos y existentes. Para obtener más información, consulte Controlar el acceso a AWS los recursos mediante etiquetas en la Guía del usuario de IAM.

Adición de etiquetas a los recursos de Amazon Security Lake

Para añadir etiquetas a un recurso de Amazon Security Lake, puede usar la consola de Security Lake o la API de Security Lake.

> **Important**
>
> La adición de etiquetas a un recurso puede afectar al acceso al recurso. Antes de añadir una etiqueta a un recurso, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizar etiquetas para controlar el acceso a los recursos.

Console

Al habilitar Security Lake para un suscriptor Región de AWS o al crear uno, la consola de Security Lake ofrece opciones para agregar etiquetas al recurso: la configuración del lago de datos para la región o el suscriptor. Siga las instrucciones de la consola para añadir etiquetas al recurso al crearlo.

Para agregar una o más etiquetas a un recurso existente mediante la consola de Security Lake, siga estos pasos.

Para agregar una etiqueta a un recurso

1. Abra la consola de Security Lake en. https://console.aws.amazon.com/securitylake/
2. Elija una de las siguientes opciones, en función del tipo de recurso al que desea añadir una etiqueta:

   - Para configurar un lago de datos, elija Regiones en el panel de navegación. A continuación, en la tabla Regiones, seleccione la región.
   - Para un suscriptor, elija Suscriptores en el panel de navegación. A continuación, en la tabla Mis suscriptores, seleccione el suscriptor.

     Si el suscriptor no aparece en la table, use el selector de Región de AWS ubicado en la esquina superior derecha de la página para seleccionar la región en la que lo creó. La tabla muestra una lista de los suscriptores existentes solo para la región actual.

3. Elija Edit (Edición de).
4. Expanda la sección Etiquetas. Esta sección muestra una lista de todas las etiquetas asignadas actualmente al recurso.
5. En la sección Etiquetas, elija Añadir nueva etiqueta.
6. En el cuadro Clave, introduzca la clave de etiqueta de la etiqueta que desee añadir al recurso. A continuación, en el cuadro Valor, si lo desea, escriba el valor de la clave.

   Una clave de etiqueta puede incluir hasta 128 caracteres. Un valor de etiqueta puede incluir hasta 256 caracteres. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @
7. Para agregar otra etiqueta al recurso, elija Agregar nueva etiqueta y, a continuación, repita el paso anterior. Puede asignar hasta 50 etiquetas a un recurso.
8. Cuando haya terminado de agregar etiquetas, elija Guardar.

API

Para crear un recurso y añadirle una o más etiquetas mediante programación, utilice la operación `Create` adecuada para el tipo de recurso que desee crear:

- Configuración del lago de datos: utilice la CreateDataLakeoperación o, si utiliza AWS Command Line Interface (AWS CLI), ejecute el create-data-lakecomando.
- Suscriptor: utilice la CreateSubscriberoperación o, si está utilizando la AWS CLI, ejecute el comando create-subscriber.

En la solicitud, utilice el parámetro `tags` para especificar la clave de etiqueta (`key`) y el valor de etiqueta opcional (`value`) de cada etiqueta que desee añadir al recurso. El parámetro `tags` especifica una matriz de JSON. Cada objeto especifica una clave de etiqueta y su valor de etiqueta asociado.

Para añadir una o más etiquetas a un recurso existente, utilice la TagResourceoperación de la API de Security Lake o, si la utiliza AWS CLI, ejecute el comando tag-resource. En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso al que desea añadir una etiqueta. Utilice el parámetro `tags` para especificar la clave de etiqueta (`key`) y el valor de etiqueta opcional (`value`) de cada etiqueta que desee añadir. Como ocurre con las operaciones y comandos `Create`, el parámetro `tags` especifica una matriz de objetos, un objeto para cada clave de etiqueta y su valor de etiqueta asociado.

Por ejemplo, el siguiente AWS CLI comando agrega una clave de `Environment` etiqueta con un valor de `Cloud` etiqueta al suscriptor especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

Donde:

- `resource-arn` especifica el ARN del suscriptor al que se va a añadir una etiqueta.
- *`Environment`* es la clave de etiqueta de la etiqueta que se va a añadir al suscriptor.
- *`Cloud`* es el valor de la etiqueta para la clave especificada (*`Environment`*).

En el siguiente ejemplo, el comando agrega varias etiquetas al suscriptor.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

Para cada objeto de una matriz `tags`, se requieren los argumentos `key` y `value`. Sin embargo, el valor del argumento `value` puede ser una cadena vacía. Si no desea asociar un valor de etiqueta a una clave de etiqueta, no especifique un valor para el argumento `value`. Por ejemplo, el comando siguiente añade una clave de etiqueta `Owner` sin un valor de etiqueta asociado:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Si la operación de etiquetado se realiza correctamente, Security Lake devuelve una respuesta HTTP 200 vacía. De lo contrario, Security Lake devuelve una respuesta HTTP 4xx o 500 que indica el motivo del error de la operación.

Edición de etiquetas para los recursos de Amazon Security Lake

Para editar las etiquetas (tanto las claves como los valores de las etiquetas) de un recurso de Amazon Security Lake, puede usar la consola de Security Lake o la API de Security Lake.

> **Important**
>
> La edición de etiquetas de un recurso puede afectar al acceso al recurso. Antes de editar la clave o el valor de una etiqueta para un recurso, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizar la etiqueta para controlar el acceso a los recursos.

Console

Siga estos pasos para editar las etiquetas un recurso utilizando la consola de Security Lake.

Para editar las etiquetas de un recurso

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Elija una de las siguientes opciones, en función del tipo de recurso cuyas etiquetas desea editar.
   - Para configurar un lago de datos, elija Regiones en el panel de navegación. A continuación, en la tabla Regiones, seleccione la región.
   - Para un suscriptor, elija Suscriptores en el panel de navegación. A continuación, en la tabla Mis suscriptores, seleccione el suscriptor.

     Si el suscriptor no aparece en la table, use el selector de Región de AWS ubicado en la esquina superior derecha de la página para seleccionar la región en la que lo creó. La tabla muestra una lista de los suscriptores existentes solo para la región actual.
3. Elija Edit (Edición de).
4. Expanda la sección Etiquetas. La sección Etiquetas muestra una lista de todas las etiquetas asignadas actualmente al recurso.
5. Realice uno de los siguientes procedimientos:
   - Para añadir un valor de etiqueta a una clave de etiqueta existente, introduzca el valor en el cuadro Valor situado junto a la clave de etiqueta.

- Para cambiar una clave de etiqueta existente, seleccione Eliminar junto a la etiqueta. Después seleccione Agregar nueva etiqueta. En el cuadro Clave que aparece, introduzca la nueva clave de etiqueta. Opcionalmente, puede introducir un valor de etiqueta asociado en el cuadro Valor.
- Para cambiar el valor de una etiqueta existente, seleccione X en el cuadro Valor que contiene el valor. A continuación, escriba el nuevo valor de la etiqueta en el cuadro Valor.
- Para eliminar el valor de una etiqueta existente, seleccione X en el cuadro Valor que contiene el valor.
- Para eliminar una etiqueta existente (tanto la clave como el valor de la etiqueta), haga clic en Eliminar junto a la etiqueta.

Un recurso puede tener hasta 50 etiquetas. Una clave de etiqueta puede incluir hasta 128 caracteres. Un valor de etiqueta puede incluir hasta 256 caracteres. Los caracteres pueden ser letras, números, espacios o los siguientes símbolos: _ . : / = + - @

6. Cuando termine de editar las etiquetas, elija Guardar.

API

Al editar una etiqueta de un recurso mediante programación, sobrescribe la etiqueta existente con valores nuevos. Por lo tanto, la mejor forma de editar una etiqueta depende de si desea editar una clave de etiqueta, un valor de etiqueta o ambos. Para editar una clave de etiqueta, elimine la etiqueta actual y añada una nueva.

Para editar o eliminar únicamente el valor de etiqueta asociado a una clave de etiqueta, sobrescriba el valor existente mediante la TagResourceoperación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando tag-resource. En su solicitud, especifique el nombre de recurso de Amazon (ARN) del recurso cuyo valor de etiqueta quiere editar o eliminar.

Para editar el valor de una etiqueta, utilice el parámetro `tags` para especificar la clave de etiqueta cuyo valor de etiqueta desea cambiar. Especifique también el nuevo valor de etiqueta para la clave. Por ejemplo, el siguiente AWS CLI comando cambia el valor de la etiqueta de `Cloud` a `On-Premises` para la clave de `Environment` etiqueta asignada al suscriptor especificado. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=On-Premises
```

Donde:

- `resource-arn` especifica el ARN del suscriptor.
- *`Environment`* es la clave de etiqueta asociada al valor de etiqueta que se va a cambiar.
- *`On-Premises`* es el nuevo valor de la etiqueta para la clave especificada (*`Environment`*).

Para eliminar un valor de etiqueta de una clave de etiqueta, no especifique un valor para el argumento `value` de la clave en el parámetro `tags`. Por ejemplo:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Si la operación se realiza correctamente, Security Lake devuelve una respuesta HTTP 200 vacía. De lo contrario, Security Lake devuelve una respuesta HTTP 4xx o 500 que indica el motivo del error de la operación.

Revisión de etiquetas para los recursos de Amazon Security Lake

Puede revisar las etiquetas (tanto las claves como los valores de las etiquetas) de un recurso de Amazon Security Lake mediante la consola de Security Lake o la API de Security Lake.

Console

Siga estos pasos para revisar las etiquetas un recurso utilizando la consola de Security Lake.

Para revisar las etiquetas de un recurso

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Elija una de las siguientes opciones, en función del tipo de recurso cuyas etiquetas desea revisar.

- Para configurar un lago de datos, elija Regiones en el panel de navegación. En la tabla Regiones, seleccione la región y, a continuación, elija Editar. Después expanda la sección Etiquetas.
- Para un suscriptor, elija Suscriptores en el panel de navegación. A continuación, en la tabla Mis suscriptores, seleccione el nombre del suscriptor.

  Si el suscriptor no aparece en la table, use el selector de Región de AWS ubicado en la esquina superior derecha de la página para seleccionar la región en la que lo creó. La tabla muestra una lista de los suscriptores existentes solo para la región actual.

La sección Etiquetas muestra una lista de todas las etiquetas asignadas actualmente al recurso.

API

Para recuperar y revisar las etiquetas de un recurso existente mediante programación, utilice la ListTagsForResourceAPI de Security Lake. En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso.

Si usa AWS Command Line Interface (AWS CLI), ejecute el list-tags-for-resourcecomando y use el `resource-arn` parámetro para especificar el ARN del recurso. Por ejemplo:

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

En el ejemplo anterior, *arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab* es el ARN de un abonado existente.

Si la operación es exitosa, Security Lake devuelve una matriz `tags`. Cada objeto de la matriz especifica una etiqueta (tanto la clave como el valor de la etiqueta) que está asignada actualmente al recurso. Por ejemplo:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
```

```
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Donde `Environment`, `CostCenter` y `Owner` son las claves de etiqueta que se asignan al recurso. `Cloud` es el valor de etiqueta asociado a la clave de etiqueta `Environment`. `12345` es el valor de etiqueta asociado a la clave de etiqueta `CostCenter`. La clave de etiqueta `Owner` no tiene un valor de etiqueta asociado.

Eliminación de etiquetas de los recursos de Amazon Security Lake

Para quitar etiquetas de un recurso de Amazon Security Lake, puede usar la consola de Security Lake o la API de Security Lake.

> **Important**
>
> La eliminación de etiquetas de un recurso puede afectar al acceso al recurso. Antes de eliminar una etiqueta, revise las políticas AWS Identity and Access Management (de IAM) que puedan utilizarla para controlar el acceso a los recursos.

Console

Siga estos pasos para quitar una o más etiquetas un recurso utilizando la consola de Security Lake.

Para eliminar una etiqueta de un recurso

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Elija una de las siguientes opciones, en función del tipo de recurso del que desea eliminar una etiqueta:

   - Para configurar un lago de datos, elija Regiones en el panel de navegación. A continuación, en la tabla Regiones, seleccione la región.

- Para un suscriptor, elija Suscriptores en el panel de navegación. A continuación, en la tabla Mis suscriptores, seleccione el suscriptor.

  Si el suscriptor no aparece en la table, use el selector de Región de AWS ubicado en la esquina superior derecha de la página para seleccionar la región en la que lo creó. La tabla muestra una lista de los suscriptores existentes solo para la región actual.

3. Elija Edit (Edición de).
4. Expanda la sección Etiquetas. La sección Etiquetas muestra una lista de todas las etiquetas asignadas actualmente al recurso.
5. Realice uno de los siguientes procedimientos:

   - Para eliminar solo el valor de la etiqueta de una etiqueta, seleccione X en el cuadro Valor que contiene el valor que quiere eliminar.
   - Para eliminar la clave y el valor de la etiqueta (como un conjunto), haga clic en Eliminar junto a la etiqueta que quiere eliminar.
6. Para eliminar etiquetas adicionales del recurso, repita el paso anterior para cada etiqueta adicional que desee eliminar.
7. Cuando termine de eliminar las etiquetas, elija Guardar.

API

Para eliminar una o más etiquetas de un recurso mediante programación, utilice la UntagResourceoperación de la API de Security Lake. En su solicitud, utilice el parámetro `resourceArn` para especificar el nombre de recurso de Amazon (ARN) del recurso del que quiere eliminar una etiqueta. Utilice el parámetro `tagKeys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Para eliminar varias etiquetas, añada el parámetro `tagKeys` y el argumento de cada etiqueta que desee eliminar, separados por un signo &, por ejemplo, `tagKeys=`*`key1`*`&tagKeys=`*`key2`*. Para quitar solo un valor de etiqueta específico (no una clave de etiqueta) de un recurso, edite la etiqueta en lugar de eliminarla.

Si utilizas AWS Command Line Interface (AWS CLI), ejecuta el comando untag-resource para eliminar una o más etiquetas de un recurso. Para el parámetro `resource-arn`, especifique el ARN del recurso del que se va a eliminar una etiqueta. Utilice el parámetro `tag-keys` para especificar la clave de etiqueta de la etiqueta que se va a eliminar. Por ejemplo, el siguiente comando elimina la etiqueta `Environment` (tanto la clave como el valor de la etiqueta) del suscriptor especificado:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

Donde `resource-arn` especifica el ARN del suscriptor del que se va a eliminar una etiqueta y *`Environment`* es la clave de etiqueta de la etiqueta que se va a eliminar.

Para eliminar varias etiquetas de un recurso, agregue cada clave adicional como argumento para el parámetro `tag-keys`: Por ejemplo:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

Si la operación se realiza correctamente, Security Lake devuelve una respuesta HTTP 200 vacía. De lo contrario, Security Lake devuelve una respuesta HTTP 4xx o 500 que indica el motivo del error de la operación.

Solución de problemas en Security Lake

Si tiene problemas al trabajar con Amazon Security Lake, utilice los siguientes recursos de solución de problemas.

En los siguientes temas se proporcionan consejos para la solución de errores y problemas que puedan surgir relacionados con el estado de los lagos de datos, Lake Formation, las consultas en Amazon Athena AWS Organizations y la IAM. Si encuentra un problema que no aparece aquí, puede utilizar el `Feedback` botón de esta página para informarlo.

Consulte los siguientes temas si tiene problemas al utilizar Security Lake.

Temas

- Solución de problemas del estado del lago de datos
- Solución de problemas de Lake Formation
- Solución de problemas de consultas en Amazon Athena
- Solución de problemas de Organizations
- Solución de problemas de identidad y acceso de Amazon Security Lake

Solución de problemas del estado del lago de datos

La página de problemas de la consola de Security Lake muestra un resumen de los problemas que afectan a su lago de datos. Por ejemplo, Security Lake no puede habilitar la recopilación de registros para los eventos de AWS CloudTrail administración si no ha creado un CloudTrail registro para su organización. La página de problemas cubre los problemas que se han producido en los últimos 14 días. Puedes ver una descripción de cada problema y los pasos de solución sugeridos.

Para acceder mediante programación a un resumen de los problemas, puede utilizar el ListDataLakeExceptionsfuncionamiento de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el list-data-lake-exceptionscomando. Para el `regions` parámetro, puede especificar uno o más códigos de región, por ejemplo, `us-east-1` para la región EE.UU. Este (Virginia del Norte), para ver los problemas que afectan a esas regiones. Si no incluye el `regions` parámetro, se devolverán los problemas que afectan a todas las regiones. Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.

Por ejemplo, el siguiente AWS CLI comando muestra los problemas que afectan a las `eu-west-3` regiones `us-east-1` y. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake list-data-lake-exceptions \
--regions "us-east-1" "eu-west-3"
```

Para notificar a un usuario de Security Lake acerca de un problema o error, CreateDataLakeExceptionSubscriptionutilice la API de Security Lake. El usuario puede recibir notificaciones por correo electrónico, mediante entrega a una cola de Amazon Simple Queue Service (Amazon SQS), entrega a AWS Lambda una función u otro protocolo compatible.

Por ejemplo, el siguiente AWS CLI comando envía notificaciones de las excepciones de Security Lake a la cuenta especificada mediante un envío de SMS. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake create-data-lake-exception-subscription \
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

Para ver los detalles de una suscripción de excepciones, puede utilizar la GetDataLakeExceptionSubscriptionoperación. Para actualizar una suscripción de excepción, puede utilizar la UpdateDataLakeExceptionSubscriptionoperación. Para eliminar una suscripción de excepciones y detener las notificaciones, puede utilizar la DeleteDataLakeExceptionSubscriptionoperación.

Solución de problemas de Lake Formation

Utilice la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Security Lake y AWS Lake Formation bases de datos o tablas. Para obtener más temas de solución de problemas de Lake Formation, consulte la sección Solución de problemas de la Guía para desarrolladores de AWS Lake Formation .

Tabla no encontrada

Es posible que reciba este error al intentar crear un suscriptor.

Para resolver este error, asegúrese de que ya ha agregado orígenes en la región. Si agregó orígenes cuando el servicio Security Lake estaba en versión preliminar, debe volver a agregarlos antes de crear un suscriptor. Para obtener más información sobre cómo agregar orígenes, consulte Administración de fuentes en Security Lake.

400 AccessDenied

Es posible que reciba este error cuando añada un origen personalizado y llame a la API `CreateCustomLogSource`.

Para resolver el error, revise sus permisos de Lake Formation. El rol de IAM que llama a la API debe tener permisos de creación de tablas para la base de datos de Security Lake. Para obtener más información, consulte Granting database permissions using the Lake Formation console and the named resource method en la Guía para desarrolladores de AWS Lake Formation .

SYNTAX_ERROR: line 1:8: SELECT * not allowed from relation that has no columns

Es posible que reciba este error al consultar una tabla de orígenes por primera vez en Lake Formation.

Para resolver el error, conceda `SELECT` permiso a la función de IAM que esté utilizando cuando haya iniciado sesión en su Cuenta de AWS. Para instrucciones sobre cómo conceder el permiso `SELECT`, consulte Granting database permissions using the Lake Formation console and the named resource method en la Guía para desarrolladores de AWS Lake Formation .

Security Lake no pudo agregar el ARN de la entidad principal del intermediario al administrador del lago de datos de Lake Formation. Los administradores actuales del lago de datos pueden incluir entidades principales no válidas que ya no existen.

Es posible que reciba este error al habilitar Security Lake o al agregar uno Servicio de AWS como fuente de registro.

Siga estos pasos para solucionar el problema:

1. Abra la consola de Lake Formation en https://console.aws.amazon.com/lakeformation/.
2. Inicie sesión como usuario administrativo.

3. En el panel de navegación, en Permisos, elija Roles y tareas administrativas.
4. En la sección Administradores de lago de datos, elija Elegir administradores.
5. Borre las entidades principales que estén etiquetadas como No se encuentra en IAM y, a continuación, seleccione Guardar.
6. Vuelva a intentar la operación de Security Lake.

Security Lake CreateSubscriber with Lake Formation no creó una nueva invitación para compartir recursos de RAM para ser aceptada

Es posible que aparezca este error si ha compartido recursos con el uso compartido de datos entre cuentas de Lake Formation versión 2 o versión 3 antes de crear un suscriptor de Lake Formation en Security Lake. Esto se debe a que el uso compartido entre cuentas de Lake Formation, versión 2 y versión 3, optimiza la cantidad de recursos compartidos de AWS RAM al mapear múltiples concesiones de permisos entre cuentas con un recurso compartido de AWS RAM.

Asegúrese de comprobar que el nombre del recurso compartido tiene el ID externo que especificó al crear el suscriptor y que el ARN del recurso compartido coincide con el ARN de la respuesta de `CreateSubscriber`.

Solución de problemas de consultas en Amazon Athena

Utilice la información siguiente para diagnosticar y solucionar los problemas comunes que puedan surgir cuando utilice Athena para consultar los objetos que estén almacenados en el bucket de Security Lake S3. Para obtener más temas de solución de problemas de Athena, consulte la sección Solución de problemas en Athena de la Guía del usuario de Amazon Athena.

Las consultas no devuelven nuevos objetos al lago de datos

Es posible que su consulta de Athena no devuelva nuevos objetos en su lago de datos, incluso cuando el bucket de S3 de Security Lake contenga esos objetos. Esto puede ocurrir si ha desactivado Security Lake y, a continuación, lo ha vuelto a activar. Como resultado, es posible que las AWS Glue particiones no registren correctamente los nuevos objetos.

Siga estos pasos para solucionar el problema:

1. Abra la AWS Lambda consola en https://console.aws.amazon.com/lambda/.

2. En la barra de navegación, en el selector de regiones, seleccione la región en la que Security Lake está activado pero la consulta de Athena no arroja resultados.
3. En el panel de navegación, elija Funciones y seleccione la función de la siguiente lista en función de la versión de origen:

   - `Source version 1 (OCSF 1.0.0-rc.2)` — Función SecurityLake***#region>***_Glue_Partition_Updater_Lambda_.
   - `Source version 2 (OCSF 1.1.0)`AmazonSecurityLakeMetastoreManager— _ función. ***#region>***
4. En la pestaña Configuración, elija Agregar desencadenador.
5. Seleccione la opción situada junto a la función y elija Editar.
6. Seleccione Activar desencadenador y, a continuación, seleccione Guardar. Esto cambiará el estado de la función a Activada.

No se puede acceder a AWS Glue las tablas

Es posible que un suscriptor de acceso a consultas no pueda acceder a AWS Glue las tablas que contienen datos de Security Lake.

En primer lugar, asegúrese de haber seguido los pasos que se describen en Configurar el uso compartido de tablas entre cuentas (paso de suscriptor).

Si el suscriptor sigue sin tener acceso, siga estos pasos:

1. Abra la AWS Glue consola en https://console.aws.amazon.com/glue/.
2. En el panel de navegación, seleccione Catálogo de datos y, a continuación, Configuración del catálogo.
3. Conceda permiso al suscriptor para acceder a las AWS Glue tablas con una política basada en los recursos. Para obtener más información sobre la creación de políticas basadas en recursos, consulte Ejemplos de políticas basadas en recursos de AWS Glue en la Guía para desarrolladores de AWS Glue .

Solución de problemas de Organizations

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Security Lake y AWS Organizations. Para obtener más temas de solución

de problemas de Organizations, consulte la sección Solución de problemas de la Guía del usuario de AWS Organizations .

Se produjo un error de acceso denegado al llamar a la CreateDataLake operación: tu cuenta debe ser la cuenta de administrador delegado de una organización o una cuenta independiente.

Es posible que reciba este error si elimina la organización a la que pertenecía una cuenta de administrador delegado y, a continuación, intenta utilizarla para configurar Security Lake mediante la consola o la API de Security Lake. CreateDataLake

Para resolver el error, utilice una cuenta de administrador delegado de otra organización o una cuenta independiente.

Solución de problemas de identidad y acceso de Amazon Security Lake

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Security Lake e IAM.

No tengo autorización para realizar una acción en Security Lake

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales.

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 *`subscriber`* ficticio, pero no tiene los permisos ficticios `SecurityLake:`*`GetSubscriber`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso a la información del *`subscriber`* mediante la acción `SecurityLake:`*`GetSubscriber`*.

Quiero ampliar los permisos más allá de la política gestionada

Todos los roles de IAM creados por un suscriptor o una fuente de registro personalizada APIs están sujetos a la política `AmazonSecurityLakePermissionsBoundary` administrada. Si desea ampliar los permisos más allá de la política administrada, puede eliminar la política administrada del límite de permisos del rol. Sin embargo, al interactuar con un Security Lake mutante APIs para DataLakes y suscriptores, se debe adjuntar el límite de permisos para que IAM modifique el rol de IAM.

No estoy autorizado a realizar el iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Security Lake.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Security Lake. 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 AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Security Lake

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Security Lake es compatible con estas características, consulte Cómo funciona Security Lake con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte 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.

Cómo se determinan los precios de Security Lake

Los precios de Amazon Security Lake se basan en dos dimensiones: ingesta de datos y conversión de datos. Security Lake también trabaja con otros Servicios de AWS para almacenar y compartir sus datos, y es posible que se le cobren cargos adicionales por estas actividades.

Al activar la recopilación de registros por primera vez Cuenta de AWS en una cuenta compatible con Security Lake, Región de AWS esa cuenta se inscribe automáticamente en una prueba gratuita de 15 días de Security Lake. Es posible que siga incurriendo en cargos por otros servicios durante la prueba gratuita.

> **Note**
>
> Si continúa utilizando Security Lake una vez finalizada la prueba gratuita de 15 días, empezará a incurrir automáticamente en gastos de uso. Para evitar incurrir en cargos una vez finalizada la prueba gratuita, debes desactivar Security Lake.

Para entender la metodología en la que se basan los precios de Security Lake, vea el siguiente vídeo: Precios de Amazon Security Lake -->

Ingesta de datos

Estos costos se derivan del volumen de registros ingeridos y otros AWS CloudTrail registros y eventos (Servicio de AWS registros de consultas de resolución de Amazon Route 53, AWS Security Hub CSPM hallazgos y registros de flujo de Amazon VPC).

Conversión de datos

Estos costos se derivan del volumen de Servicio de AWS registros y eventos que Security Lake normaliza en forma de Marco de esquema de ciberseguridad abierto (OCSF) en Security Lake esquema y convierte al formato Apache Parquet.

Costos de servicios relacionados

Estos son algunos de los costos en los que puede incurrir debido a otros gastos Servicios de AWS por almacenar y compartir los datos de su lago de datos de seguridad:

- Amazon S3: estos costes se derivan del mantenimiento de los buckets de Amazon S3 en su cuenta de Security Lake, del almacenamiento de los datos allí y de la evaluación y supervisión del bucket para garantizar la seguridad y el control de acceso. Para obtener más información, consulte Precios de Amazon S3.
- Amazon SQS: estos costos se derivan de la creación de una cola de Amazon SQS para la entrega de mensajes. Para obtener más información, consulte precios de Amazon SQS.
- Amazon EventBridge : estos costes se derivan del EventBridge envío por parte de Amazon de notificaciones de objetos a los puntos de conexión de las suscripciones. Para obtener más información, consulta los EventBridgeprecios de Amazon.
- AWS Glue — Los costes mensuales se determinan en función del volumen de datos de registros y eventos que se ingieren de AWS los servicios por gigabyte. Sus datos se almacenan en Amazon Simple Storage Service y se aplican los cargos estándar de Amazon S3. Security Lake también organiza otros AWS servicios en su nombre. Se le cobrarán cargos separados por los AWS servicios utilizados y los recursos configurados como parte de su lago de datos de seguridad. Consulte los precios de Amazon AWS Glue EventBridgeAWS Lambda, Amazon SQS y Amazon Simple Notification Service. Usted es responsable de los costes en los que incurra al consultar los datos de Security Lake y almacenar los resultados de las consultas.

Los costos en los que incurra un suscriptor al consultar datos de Security Lake y almacenar los resultados de las consultas son responsabilidad del suscriptor.

Para obtener una lista completa de los costos y los servicios auxiliares, consulte los precios de Security Lake.

Revisar el uso de Security Lake y los costos estimados

La página Uso de la consola de Amazon Security Lake le permite revisar su uso actual de Security Lake, así como el uso futuro y las estimaciones de costos. Si actualmente participa en una prueba gratuita de 15 días, el uso que haga durante la prueba puede ayudarle a calcular los costos de uso de Security Lake una vez que finalice la prueba gratuita. Para obtener una descripción general de los precios de Security Lake, consulte Cómo se determinan los precios de Security Lake. Para obtener información detallada y ejemplos de costos, consulte Precios de Amazon Security Lake.

En Security Lake, los costos de uso estimados se indican en dólares estadounidenses y se aplican únicamente a la Región de AWS actual. Los costos cubren el uso de Security Lake por parte de todas las cuentas de la organización e incluyen la conversión al Open Cybersecurity Schema Framework (OCSF) y al formato Apache Parquet. Sin embargo, los costos previstos no incluyen los costos de otros servicios con los que Security Lake trabaja, como Amazon Simple Storage Service (Amazon S3) y AWS Glue.

En la página Uso, usted elige un período de tiempo para el cual desea ver los datos de uso y costo. El período de tiempo predeterminado es el último día natural. Debe tener al menos 1 día de uso de Security Lake para ver las proyecciones de costos.

En la parte superior de la página se muestra el costo proyectado para todas las cuentas. Este es el costo actual de Security Lake previsto Región de AWS para los próximos 30 días naturales, en función del uso real durante el período de tiempo seleccionado. El uso real y el costo previsto reflejan todas las cuentas de la organización.

En el resto de la página, los datos de uso y el costo se dividen en las dos tablas siguientes:

- Uso y costo por origen: este es su uso actual de Security Lake desglosado por origen de datos, así como el uso y los costos estimados para los próximos 30 días naturales en función de su uso real durante el período de tiempo seleccionado. El uso real, el uso previsto y el costo previsto reflejan todas las cuentas de la organización. Si selecciona un origen, se abre un panel dividido que muestra qué cuentas generaron registros y eventos a partir de ese origen. Para cada cuenta, el panel dividido incluye tanto el uso real de ese origen como el uso y los costos previstos.
- Uso y costo por cuenta: este es su uso actual de Security Lake desglosado por cuenta, así como el uso y los costos estimados para los próximos 30 días naturales en función de su uso real durante el período de tiempo seleccionado. Si selecciona una cuenta, se abre un panel dividido que muestra los orígenes que contribuyeron al uso de esa cuenta. Para cada origen contribuyente, el panel dividido incluye tanto el uso real como el uso y los costos previstos.

Todas las fuentes de AWS datos compatibles aparecen en las tablas anteriores, incluso si no ha agregado ninguna fuente concreta en Security Lake. Le recomendamos que añada todas AWS las fuentes si va a participar en la prueba gratuita para obtener estimaciones de los costes del conjunto completo de registros y eventos. Para obtener instrucciones sobre cómo añadir una AWS fuente, consulteRecopilación de datos de Servicios de AWS en Security Lake. Los orígenes personalizados no se incluyen en los cálculos de uso o costo.

Siga estos pasos para revisar sus datos de uso y costos en la consola de Security Lake.

Para revisar el uso y los costos previstos de Security Lake (consola)

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee revisar el uso y los costes.
3. En el panel de navegación, seleccione Configuración y después Uso.
4. Elija el periodo para el que quiere ver los datos de uso y costos. El valor predeterminado es el último día (es decir, 1 día).
5. Seleccione la pestaña Por origen de datos o Por cuentas para revisar el uso y los costos en detalle.

Regiones y puntos finales de Security Lake

Para obtener una lista de las regiones y puntos de conexión de servicio compatibles con Security Lake, consulte los puntos de conexión de Amazon Security Lake en Referencia general de AWS.

Se recomienda que habilite Security Lake en todas las Regiones de AWS admitidas. Esto le permite usar Security Lake para detectar e investigar actividades no autorizadas o inusuales, incluso en las regiones que no utiliza activamente.

Desactivación de Security Lake

Al deshabilitar Amazon Security Lake, Security Lake deja de recopilar registros y eventos de sus orígenes de AWS . Se conserva la configuración de Security Lake existente y los recursos que se crearon en la Cuenta de AWS se retienen. Además, los datos que almacenó o publicó en otros Servicios de AWS, como los datos confidenciales de AWS Lake Formation tablas y AWS CloudTrail registros, permanecen disponibles. Los datos almacenados en el bucket de Amazon Simple Storage Service (Amazon S3) permanecen disponibles de acuerdo con el ciclo de vida de almacenamiento de Amazon S3.

Si se desactiva Security Lake desde la página de configuración de la consola de Security Lake, se detendrá la recopilación de AWS registros y eventos Regiones de AWS en los que Security Lake esté activado actualmente. Puede utilizar la página Regiones de la consola para detener la recopilación de registros en regiones específicas. La API de Security Lake AWS CLI también detiene la recopilación de registros en las regiones que especifique en su solicitud.

Si utiliza la integración AWS Organizations y su cuenta forma parte de una organización que administra de forma centralizada varias cuentas de Security Lake, solo el administrador delegado de Security Lake puede deshabilitar Security Lake para sí mismo y para las cuentas de los miembros. Sin embargo, al abandonar una organización se detiene la recopilación de registros de una cuenta de miembro.

Al deshabilitar Security Lake para una organización, se conserva la designación de administrador delegado si sigue las instrucciones de desactivación que se proporcionan en esta página. No es necesario volver a designar al administrador delegado para poder volver a activar Security Lake.

Si configuró una o más fuentes personalizadas en Security Lake y deshabilita el servicio, también debe deshabilitar cada fuente independientemente de Security Lake. De lo contrario, la fuente personalizada seguirá enviando registros a Amazon S3. Además, debe desactivar la integración de un suscriptor o el suscriptor podrá seguir consumiendo datos de Security Lake. Para obtener más información sobre cómo eliminar un origen personalizado o la integración de un suscriptor, consulte la documentación del proveedor correspondiente.

> **Important**
>
> Si deshabilita Security Lake, elimine también los AWS Glue recursos existentes para su lago de datos. De lo contrario, las consultas posteriores no funcionarán correctamente si vuelve a habilitar Security Lake más adelante. Si bien la eliminación de AWS Glue recursos es un

requisito principal, las organizaciones tienen flexibilidad a la hora de administrar los recursos adicionales asociados al lago de datos.
Si decide eliminar recursos más allá de los AWS Glue componentes, es fundamental seguir un enfoque de «todo o nada». Si decide eliminar los recursos auxiliares, debe eliminar por completo todos los componentes asociados. Estos recursos adicionales incluyen: colas SQS de Security Lake (`AmazonSecurityLakeManager-xxx`), la función Lambda de Security Lake, las asignaciones de fuentes de eventos y funciones de IAM relacionadas, como la función. `AmazonSecurityLakeMetaStoreManagerV2`
Durante este proceso, no es necesario eliminar los buckets de Amazon S3 que almacenan datos para el lago de datos. Las organizaciones pueden conservar estos depósitos sin que ello afecte al procedimiento de limpieza. La consideración clave es evitar la eliminación parcial de los recursos, lo que podría provocar problemas de configuración en futuras implementaciones.
Cuando planee desmantelar su lago de datos, evalúe detenidamente si desea eliminar solo los AWS Glue recursos o realizar una limpieza completa de los recursos. Si opta por una eliminación completa, asegúrese de seguir un proceso de eliminación sistemático y de eliminar todos los componentes asociados.

Cuando Security Lake se vuelve a activar, se crea un lago de datos nuevo en un nuevo bucket de Amazon S3 y los datos se recopilan en este nuevo bucket de S3. Si ya había eliminado AWS Glue tablas anteriormente, se crea un nuevo conjunto de AWS Glue tablas.

Todos los datos recopilados antes de deshabilitar Security Lake permanecerán en el depósito anterior de Amazon S3. Si desea consultar datos antiguos, debe moverlos al nuevo depósito mediante el `Sync` comando Amazon S3. Para obtener más información, consulte el comando Sync en la Referencia de AWS CLI comandos.

En este tema se explica cómo deshabilitar Security Lake mediante la consola de Security Lake, la API de Security Lake o AWS CLI.

Console

1. Abra la consola de Security Lake en https://console.aws.amazon.com/securitylake/.
2. En el panel de navegación, en Configuración, seleccione General.
3. Seleccione Deshabilitar Security Lake.
4. Cuando se le solicite confirmación, ingrese **`Disable`** y luego, elija Aceptar.

API

Para deshabilitar Security Lake mediante programación, utilice la DeleteDataLakeoperación de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el delete-date-lakecomando. En su solicitud, utilice la `regions` lista para especificar el código de región de cada región en la que desee deshabilitar Security Lake. Para obtener una lista de los códigos de región, consulte los puntos de conexión de Amazon Security Lake en la Referencia general de AWS.

En el caso de una implementación de Security Lake que utilice AWS Organizations, solo el administrador delegado de Security Lake para la organización puede deshabilitar Security Lake para las cuentas de la organización.

Por ejemplo, el siguiente AWS CLI comando desactiva Security Lake en las regiones `ap-northeast-1` y `eu-central-1`. Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

Historial de documentos de la Guía del usuario de Amazon Security Lake

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la última versión de Amazon Security Lake. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Última actualización de la documentación: 24 de abril de 2025

Cambio	Descripción	Fecha
Políticas administrada actualizada	Security Lake ha actualizado la política gestionada `SecurityLakeResourceManagementServiceRolePolicy` para añadir `lambda:DeleteFunction` permisos a Glue_Partition_Updater_Lambda las funciones SecurityLake _ obsoletas. Esto permite a Security Lake eliminar las funciones de Lambda obsoletas como parte de la migración a las fuentes de la versión 2 y al formato iceberg. Para obtener más información, consulte las actualizaciones de las políticas AWS administradas de Security Lake.	18 de noviembre de 2025
Se actualizó el permiso de rol vinculado a un servicio	Security Lake ha actualizado el sustituyéndolo AWSServiceRoleForSecurityLakeResourceManagement `StringLike` por. `ArnLike`	25 de septiembre de 2025

Funcionalidad actualizada: Service-linked rol	Security Lake ahora crea automáticamente la cámara AWSServiceRoleForSecurityLakeResourceManagement réflex durante la creación del lago de datos. Para obtener información, consulte Considerations (Consideraciones).	24 de abril de 2025
Tema reescrito de manera significativa: integraciones AWS	Se actualizó el contenido que especifica la integración de Security Lake con otros específicos. Servicios de AWS Para obtener más información, consulte Servicio de AWS integraciones.	31 de marzo de 2025
Funcionalidad actualizada: administración de varias cuentas	La consola de Security Lake ahora permite administrar la configuración de activación automática de las cuentas cuando se unen a su organización. Para obtener más información, consulte Editar la configuración de una nueva cuenta en la consola.	10 de marzo de 2025
Funcionalidad actualizada: protección de datos en AWS WAF los registros	Se agregó soporte para la protección de datos cuando está habilitada en la ACL web para las cuentas de Security Lake. Para obtener más información, consulte AWS WAF los registros en Security Lake.	17 de febrero de 2025

Nueva característica: compatibilidad agregada con puntos de conexión de VPC	Security Lake ahora está integrado con los puntos finales de VPC AWS PrivateLink y los admite. Para obtener más información sobre la AWS PrivateLink integración, consulte Amazon Security Lake y los puntos de enlace de la VPC de la interfaz ().AWS PrivateLink	4 de febrero de 2025
Nueva característica	Security Lake ahora admite la consulta directa por OpenSearch servicio para analizar los datos en Security Lake. Para obtener más información, consulte Integración con el OpenSearch servicio.	1 de diciembre de 2024
Nuevo rol vinculado a servicio	Hemos agregado un nuevo rol vinculado al servicio. `AWSServiceRoleForSecurityLakeResourceManagement` Esta función vinculada a un servicio otorga permisos a Security Lake para realizar mejoras continuas de monitoreo y rendimiento, lo que puede reducir la latencia y los costos.	14 de noviembre de 2024

Disponibilidad regional	Security Lake ya está disponible en y. AWS GovCloud (US-East) AWS GovCloud (US-West) Regiones de AWS Para obtener una lista completa de las regiones en las que Security Lake está disponible actualmente, consulte Puntos de conexión de Amazon Security Lake en la Referencia general de AWS.	10 de junio de 2024
Actualización de la política administrada existente	Hemos agregado AWS WAF acciones a la política AWS administrada para la `SecurityLakeServiceLinkedRole` política. Las acciones adicionales permiten a Security Lake recopilar AWS WAF registros cuando está habilitada como fuente de registros en Security Lake.	22 de mayo de 2024
Nueva fuente de AWS registro	Security Lake agregó los registros de AWS WAF como fuente de AWS registros. AWS WAF le ayuda a supervisar las solicitudes web que los usuarios finales envían a las aplicaciones.	22 de mayo de 2024
Actualización de la política administrada existente	Hemos agregado acciones de SID a la `AmazonSecurityLakePermissionsBoundary` política.	13 de mayo de 2024

Actualización de la política administrada existente	Hemos actualizado la AmazonSecurityLake MetastoreManager política para añadir una acción de limpieza de metadatos que te permita eliminar los metadatos de tu lago de datos.	27 de marzo de 2024
Nuevas versiones de código fuente	Actualice los permisos de su rol para incorporar datos de las nuevas versiones de la fuente de datos.	29 de febrero de 2024
Nueva fuente de AWS registro	Security Lake agregó los registros de auditoría de EKS como fuente de AWS registros . Los registros de auditoría de EKS le ayudan a detectar actividades potencialmente sospechosas en sus clústeres de EKS dentro de Amazon Elastic Kubernetes Service.	29 de febrero de 2024
Actualización de la política administrada existente	Hemos actualizado la política para permitir `iam:PassRole` el uso del nuevo `AmazonSecurityLakeMetastoreManagerV2` rol y permitir que Security Lake implemente o actualice los componentes del lago de datos.	23 de febrero de 2024

Nueva política administrada	Hemos añadido una nueva AWS política gestionada, la `AmazonSecurityLake MetastoreManager` política. Esta política otorga permisos a Security Lake para administrar los metadatos en su lago de datos.	23 de enero de 2024
Disponibilidad regional	Security Lake ahora está disponible en los siguiente s países Regiones de AWS: Asia Pacífico (Osaka), Canadá (Central), Europa (París) y Europa (Estocolmo). Para obtener una lista completa de las regiones en las que Security Lake está disponible actualmente, consulte Puntos de conexión de Amazon Security Lake en la Referencia general de AWS.	26 de octubre de 2023
Nuevas características	Ahora puede editar algunos ajustes para los suscripto res con acceso a consultas . También puede asignar etiquetas a los recursos de Security Lake para su Cuenta de AWS.	20 de julio de 2023

Nueva política administrada	Security Lake agregó una nueva política AWS administrada, la `AmazonSecurityLakeAdministrator` política. Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Security Lake.	30 de mayo de 2023
Disponibilidad general	El lago de seguridad ahora está disponible con carácter general.	30 de mayo de 2023
Nueva característica	Security Lake ahora envía las métricas a Amazon CloudWatch.	4 de mayo de 2023
Disponibilidad regional	Security Lake ya está disponible en los siguientes países Regiones de AWS: Asia Pacífico (Singapur), Europa (Londres) y Sudamérica (São Paulo).	22 de marzo de 2023
Nueva característica	Security Lake ahora crea funciones AWS Identity and Access Management (IAM) en su nombre cuando usa la consola de Security Lake para habilitar Security Lake y comenzar a usar Security Lake.	15 de febrero de 2023

Versión inicial	Esta es la versión inicial de la guía del usuario de Amazon Security Lake.	29 de noviembre de 2022

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.