aws

Guía del usuario

Amazon Security Lake

Amazon Security Lake: Guía del usuario

Table of Contents

¿Qué es Amazon Security Lake?

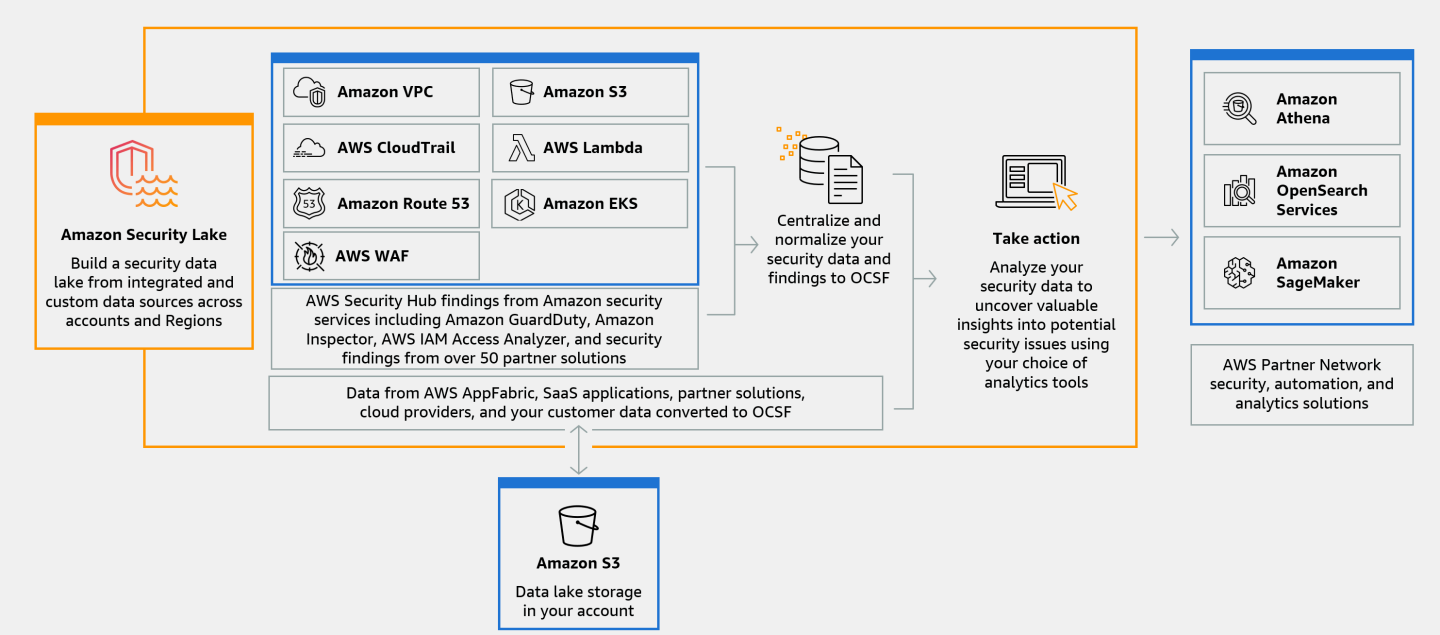
Amazon Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Security Lake para centralizar automáticamente los datos de seguridad de los AWS entornos, los proveedores de SaaS, las instalaciones, las fuentes en la nube y las fuentes de terceros en un lago de datos diseñado específicamente que se almacena en su servidor. 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 procedentes de una amplia gama de AWS fuentes de datos de seguridad empresarial.

Otros servicios Servicios de AWS y los de terceros pueden suscribirse a los datos almacenados en Security Lake para responder a 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 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 Amazon 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 para que pasen de ser compatibles de forma nativa Servicios de AWS al esquema de código abierto Open Cybersecurity Schema Framework (OCSF). Esto hace que los datos sean compatibles con otros proveedores Servicios de AWS y con terceros sin necesidad de procesarlos posteriormente. 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.

Gestión de datos en varias cuentas y regiones

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 de conexión de Amazon 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:

AWS Management Console

AWS Management Console Se trata de una interfaz basada en un navegador que puede utilizar para crear y gestionar 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 de su sistema para realizar 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 de AWS CLI, consulte la AWS Command Line Interface.

AWS SDK

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 otros. 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 basarse. AWS

Servicios relacionados

Los siguientes son otros Servicios de AWS que utiliza Security Lake:

- Amazon EventBridge: Security Lake se 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 de 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.

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 conclusiones
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF v2 Registros

Para obtener más información acerca de estos orígenes, consulte Recopilación de datos de Servicios de AWS. 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 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 acumulativa.

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 tabla de AWS Lake Formation 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 AWS y otros líderes 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

Una Región de AWS que consolida los registros y eventos de seguridad 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 otro Servicio de AWS o un servicio de terceros.

Introducción a Amazon Security Lake

En esta sección se explica cómo habilitar Security Lake y comenzar a utilizarlo. 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 AWS Management Console 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 necesarias AWS Identity and Access Management (IAM) que necesita para crear su lago de datos.

> **Important**
>
> Security Lake no permite rellenar los eventos de origen de registro AWS sin procesar existentes que se generaron antes de activar Security Lake.

Configuración inicial Cuenta de AWS

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

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

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

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

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite IAM Identity Center.

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

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

Iniciar sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos con privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

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.

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 Amazon 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 crea un rol vinculado a servicios para su cuenta denominado `AWSServiceRoleForSecurityLake`. Esta función incluye los permisos para llamar a otras personas Servicios de AWS en su nombre y gestionar el lago de datos de seguridad. Para obtener más información sobre cómo funcionan las funciones vinculadas a servicios, consulte Uso de funciones vinculadas a servicios en la Guía del usuario. IAM 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.
- 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.

Cómo empezar a usar la consola

En este tutorial se explica cómo habilitar y configurar Security Lake a través del AWS Management Console. Como parte de ello AWS Management Console, la consola de Security Lake ofrece un proceso simplificado para empezar y crea todas las funciones necesarias AWS Identity and Access Management (IAM) que necesita 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 orígenes personalizados.

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. Para Seleccionar orígenes de registros y eventos, elija una de las siguientes opciones:

   a. Ingesta AWS las fuentes predeterminadas: si eliges la opción recomendada, CloudTrail los eventos de datos de S3 no se incluyen en la ingesta. Esto se debe a que la ingesta de un gran volumen de CloudTrail eventos de datos de S3 puede afectar significativamente al costo de uso. Para ingerir este origen, seleccione la opción Ingesta de orígenes de AWS específicos.

   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.

   > **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 acceder al servicio, cree un IAM rol nuevo o utilice uno existente IAM 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.
8. Elija Next (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 el acceso al servicio, cree una nueva IAM función o utilice una IAM función existente que dé permiso a Security Lake para replicar datos en varias regiones.
4. Elija Next (Siguiente).

Paso 3: Revisar y crear el 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 de personas y IAM permisos 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 Administración de suscriptores en Amazon Security Lake.

Cómo empezar mediante programación

En este tutorial se explica cómo activar y empezar a utilizar Security Lake mediante programación. Amazon Security Lake API 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 las herramientas para acceder AWS SDKsa Security Lake.

Paso 1: Crear roles IAM

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

> **Important**
>
> No es necesario crear estos IAM roles si usa la consola de Security Lake para habilitar y configurar Security Lake.

Debe crear roles IAM si va a realizar una o más de las siguientes acciones (elija los enlaces para ver más información sobre IAM los roles de 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 esté 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 pueda extraer, transformar y cargar (ETL) trabajos 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 Security Lake. API Si está utilizando el AWS CLI, ejecute el create-data-lakecomando. 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-2` regiones `us-east-1` y. 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 AWS CLI, el update-data-lakecomando. No utilice la `CreateDataLake` operación.

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 orígenes personalizados.

Para definir una o más fuentes de recopilación mediante programación, utilice la CreateAwsLogSourceoperación del Security Lake. API 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 activar Security Lake, utilice el CreateDataLakefuncionamiento del Security Lake. API 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 que se aporten 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 Security Lake API 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 al IAM rol 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 de personas y IAM permisos 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 Administración de suscriptores en Amazon Security Lake.

Administrar varias cuentas con AWS Organizations

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 en toda la organización en todos los Regiones de AWS lugares donde Security Lake esté activado (independientemente del punto de conexión regional que utilice 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

Utilice la RegisterDataLakeDelegatedAdministratorAPI de Security Lake para permitir que Security Lake acceda a su organización y registre al administrador delegado de la organización.
Si utilizas las API de las organizaciones para registrar un administrador delegado, es posible que las funciones vinculadas al servicio para las organizaciones 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 .

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 Administración de suscriptores en Amazon Security Lake.

  Si no utiliza el AWS Control Tower servicio, es posible que no tenga 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.

> Según las mejores prácticas de AWS seguridad y el principio de privilegios mínimos, la cuenta de administración de su 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 (de 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, seleccione la cuenta que ya sirve como administrador delegado para otros servicios de AWS seguridad (recomendado). Como alternativa, introduzca el Cuenta de AWS identificador de 12 dígitos de la cuenta que desee designar como administrador delegado de Security Lake.
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 la RegisterDataLakeDelegatedAdministratoroperación 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-administratorcomando desde la cuenta de administración de la organización. En su solicitud, utilice el `accountId` parámetro para especificar el ID de cuenta de 12 dígitos Cuenta de AWS que desea designar como 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 al agregarlas a la organización. AWS Organizations Como administrador delegado, puede habilitar esta configuración mediante el CreateDataLakeOrganizationConfigurationfuncionamiento de la API de Security Lake o, si utiliza la AWS CLI, ejecutando el create-data-lake-organization-configurationcomando. 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 de Amazon Route 53, AWS Security Hub hallazgos y registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) 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 registros y eventos para las cuentas

individuales de la organización. Para obtener más información, consulte Recopilación de datos de Servicios de AWS.

Puede utilizar la GetDataLakeOrganizationConfigurationoperación para obtener detalles sobre la configuración actual de su organización para las cuentas de los nuevos miembros.

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 el administrador delegado mediante programación, utilice el DeregisterDataLakeDelegatedAdministratorfuncionamiento de la API de Security Lake. Debe invocar la operación desde la cuenta de administración de la organización. Si está utilizando el AWS CLI, ejecute el deregister-data-lake-delegated-administratorcomando 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 conservar la designación de administrador delegado pero cambiar los ajustes de configuración automática de las nuevas cuentas de los DeleteDataLakeOrganizationConfigurationmiembros, utilice la API de Security Lake o, si la utiliza AWS CLI, el delete-data-lake-organization-configurationcomando. Solo el administrador delegado puede cambiar estos ajustes para la organización.

Por ejemplo, el siguiente AWS CLI comando detiene la recopilación automática de los hallazgos de Security Hub de las cuentas de los nuevos miembros que se unen a la organización. Las cuentas de los nuevos miembros no contribuirán a las conclusiones del Security Hub al lago de datos después de 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 de confianza si el administrador delegado Cuenta de AWS está suspendido, aislado o cerrado.

Administración de regiones de

Amazon Security Lake puede recopilar registros de seguridad y eventos Regiones de AWS en los que haya activado 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 obtener el estado de la recopilación de registros en la región actual, utilice la GetDataLakeSourcesoperación Security LakeAPI. Si está utilizando el AWS CLI, ejecute el get-data-lake-sourcescomando. Para el `accounts` parámetro, especifique uno o más en Cuenta de AWS IDs forma de lista. Si su solicitud es correcta, Security Lake devolverá una instantánea de las cuentas de la región actual, incluidas 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 la 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 la 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 activado Security Lake para una región, utilice la ListDataLakesoperación. Si está utilizando el AWS CLI, ejecute el list-data-lakescomando. 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 el estado y los ajustes de 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 recursos de Amazon 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 la UpdateDataLakeoperación Security Lake. API Si está utilizando el AWS CLI, ejecute el update-data-lakecomando. 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 las clases de almacenamiento de 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

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.

> **Important**
>
> Si ha creado una fuente personalizada, para garantizar que los datos de la fuente personalizada se repliquen correctamente en el destino, Security Lake recomienda seguir las prácticas recomendadas descritas 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 particiones S3, tal como se describe en la página.

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

- IAMfunción para la replicación de datos
- IAMfunción para registrar AWS Glue particiones

> **Note**
>
> Security Lake crea estos IAM roles o usa los roles existentes en su nombre cuando usa la consola de Security Lake. Sin embargo, debe crear estos roles cuando utilice Security Lake API o AWS CLI.

IAMfunción para la replicación de datos

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

Para conceder estos permisos, cree un IAM rol 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 cuando cree una región acumulativa en Security Lake. En esta política, `sourceRegions` son regiones contribuyentes y `destinationRegions` son regiones acumulativas.

```
{
  "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:

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

Si utiliza una clave gestionada por el cliente de 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 Configuración de permisos en la Guía del usuario de Amazon Simple Storage Service.

IAMfunción para registrar AWS Glue particiones

Este IAM rol otorga permisos para una AWS Lambda función de actualización de particiones utilizada por Security Lake para registrar AWS Glue las particiones de 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 roles 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 IAM los usuarios y roles, elija el AmazonSecurityLakeMetaStoreManagerIAMrol 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 acceder al servicio, cree una nueva IAM función o utilice una IAM función existente que dé permiso a Security Lake para replicar datos en varias regiones.
6. Cuando termine, elija Save (Guardar).

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

API

Para añadir una región acumulativa mediante programación, utilice la operación de Security Lake. UpdateDataLakeAPI Si está utilizando el 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 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 365 días para los objetos que se agreguen 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 CreateDataLakeoperación (o, si utiliza el AWS CLI, el create-data-lakecomando). Para obtener más información sobre la configuración de las regiones acumulables 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 Save (Guardar).

API

Para configurar las regiones acumulativas mediante programación, utilice la UpdateDataLakeoperación de Security Lake. API Si está utilizando el 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 `us-east-2` como regiones colaboradoras. Ambas regiones aportarán 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 Amazon Security Lake

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

Security Lake ejecuta trabajos de extracción, transformación y carga (ETL) en datos de origen sin procesar y convierte datos al formato de Apache Parquet y al esquema OCSF. Tras procesarlos, Security Lake almacena los datos de origen en un bucket de Amazon Simple Storage Service (Amazon S3) en el lugar en Cuenta de AWS en la Región de AWS en la 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 tablas de AWS Lake Formation independiente.

Temas

Recopilación de datos de Servicios de AWS

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 conclusiones
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF registros v2

Security Lake transforma automáticamente estos datos a Open Cybersecurity Schema Framework (OCSF) 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 registro de estos servicios por separado, excepto en 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 añadir un Servicio de AWS como fuente en Security Lake, debe tener los permisos necesarios. Compruebe que la política AWS Identity and Access Management (IAM) asociada a la función que utilice para añadir 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.

```
{
    "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 de la an Servicio de AWS y enviarlos a la AWS Glue base de datos y tabla correctas.

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

CloudTrail registros de eventos

AWS CloudTrail te proporciona un historial de las llamadas a la AWS API de tu cuenta, incluidas las llamadas a la AWS Management Console API realizadas con los AWS SDK, las herramientas de línea de comandos y determinados AWS servicios. CloudTrail también te 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 registros asociados a eventos CloudTrail de administración y eventos de CloudTrail 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 llevan a cabo con 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 sus recursos o dentro de ellos 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 gestionado a través de la CloudTrail consola o AWS Control Tower, no es necesario realizar ninguna otra acción.

- Para obtener información sobre la creación y la gestión de un recorrido CloudTrail, consulte Creación de un sendero para una organización en la Guía del AWS CloudTrail usuario.
- Para obtener información sobre la creación y la gestión de un recorrido AWS Control Tower, consulte Registrar AWS Control Tower acciones con él AWS CloudTrail en la Guía del AWS Control Tower usuario.

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 sus 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 eventos con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

La siguiente lista proporciona enlaces de GitHub repositorios 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)

Registros de auditoría de Amazon EKS

Cuando agrega Amazon EKS Audit Logs como fuente, Security Lake comienza a recopilar información detallada sobre las actividades realizadas en los recursos de Kubernetes que se

ejecutan en sus clústeres de Elastic Kubernetes Service (EKS). Los registros de auditoría de EKS le ayudan a detectar actividades potencialmente sospechosas en sus clústeres de EKS dentro de 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 independiente y duplicado de registros de auditoría. Este proceso está diseñado para no requerir una configuración adicional ni afectar a las configuraciones de registro del plano de control de Amazon EKS existentes 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 OCSF v1.1.0. Para obtener información sobre cómo Security Lake normaliza los eventos de registros de auditoría de EKS a OCSF, consulte la referencia de mapeo en el repositorio de GitHub OCSF para los eventos de registros de auditoría de Amazon EKS (v1.1.0).

Registros de consultas de Route 53 Resolver

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 de mapeo sobre cómo Security Lake normaliza los registros de Route 53 a OCSF.

GitHub Repositorio de OCSF para los registros de Route 53

- Versión de origen 1 (v1.0.0-rc.2)
- Versión de origen 2 (v1.1.0)

Resultados de Security Hub

Las conclusiones de Security Hub le ayudan a entender su postura de seguridad AWS y le permiten comparar su entorno con los estándares y las mejores prácticas del sector de la seguridad. Security Hub recopila las conclusiones de diversas fuentes, incluidas las integraciones con otras integraciones de productos de terceros Servicios de AWS, y las compara con los controles de Security Hub. Security Hub procesa las conclusiones en un formato estándar denominado AWS Security Finding Format (ASFF).

Cuando agrega los resultados de Security Hub como origen en Security Lake, Security Lake comienza inmediatamente a recopilar sus resultados directamente desde Security Hub a través de un flujo de eventos independiente y duplicado. Security Lake también transforma los resultados de ASFF a Open Cybersecurity Schema Framework (OCSF) (OCSF).

Security Lake no gestiona los resultados de Security Hub ni afecta a la configuración de Security Hub. Para gestionar las conclusiones de Security Hub, debe utilizar la consola del servicio Security Hub, la API o AWS CLI. Para obtener más información, consulte Resultados en AWS Security Hub en la Guía del usuario de AWS Security Hub .

La siguiente lista proporciona enlaces de GitHub repositorios a la referencia de mapeo sobre cómo Security Lake normaliza los hallazgos de Security Hub a OCSF.

GitHub Repositorio OCSF para los hallazgos de Security Hub

- Versión de origen 1 (v1.0.0-rc.2)
- Versión de origen 2 (v1.1.0)

Logs de flujo de VPC

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 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 de mapeo sobre cómo Security Lake normaliza los registros de flujo de 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)

AWS WAF registros

Cuando se agrega AWS WAF como fuente de registros en Security Lake, Security Lake comienza a recopilar los registros inmediatamente. 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. La información registrada incluye la hora en que se AWS WAF recibió una solicitud web de su AWS recurso, información detallada sobre la solicitud y detalles sobre las reglas con las que coincidió 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 AWS WAF las configuraciones existentes que pueda tener. Para obtener más información sobre cómo AWS WAF proteger los recursos de la aplicación, consulte Cómo AWS WAF funciona en la Guía para AWS WAF desarrolladores.

> **Important**
>
> Si utilizas la CloudFront distribución de Amazon como tipo de recurso AWS WAF, debes seleccionar US East (Virginia del Norte) para ingerir los registros globales de Security Lake.

AWS WAF Los registros solo se admiten en OCSF v1.1.0. 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

Añadir un como fuente Servicio de AWS

Después de agregar una Servicio de AWS como fuente, Security Lake comienza a recopilar automáticamente los registros de seguridad y los eventos de esa fuente. 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 orígenes personalizados.

Console

Para agregar una fuente de AWS 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 la Servicio de AWS fuente de la que desee 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 desee usar para la ingesta de datos. De forma predeterminada, Security Lake ingiere la última versión 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 el administrador de Security Lake. Para obtener más información, consulte Actualizar los permisos de los roles.

   Para que sus suscriptores ingieran la versión seleccionada de la fuente de datos, también debe 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 ingerir solo la versión más reciente y deshabilitar todas las versiones de origen anteriores utilizadas para la ingesta de datos.
5. En la sección Regiones, seleccione las regiones en las que desee recopilar datos para la fuente. Security Lake recopilará datos del origen de todas las cuentas de las regiones seleccionadas.
6. Elija Habilitar.

API

Para añadir una fuente de AWS registro (API)

Para añadir una fuente Servicio de AWS como fuente mediante programación, utilice la CreateAwsLogSourceoperación de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando create-aws-log-source. Los parámetros `sourceName` y `regions` son obligatorios. Si lo desea, puede limitar el alcance de la fuente a algo específico o a uno específico. `accounts` `sourceVersion`

> **Important**
>
> Si 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 la organización.

En el siguiente ejemplo, se agregan registros de flujo de 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 activado Security Lake, recibirás un error. Puede resolver el error habilitando Security Lake en esa región o utilizando el `regions` parámetro para especificar solo las regiones en las que ha activado Security Lake.

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

Actualización de los permisos de los roles

Si no tiene los permisos o recursos de rol necesarios (nueva AWS Lambda función y cola de Amazon Simple Queue Service (Amazon SQS)) para ingerir datos de una nueva versión de la fuente de

datos, debe actualizar los permisos de `AmazonSecurityLakeMetaStoreManagerV2` su 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. Se trata de una acción que se realiza una sola vez, ya que los permisos y los recursos se aplican automáticamente a futuras versiones de 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. Seleccione Actualizar permisos de rol.
4. En la sección Acceso al servicio, realice una de las siguientes acciones:
   - Crear y usar un nuevo rol de servicio: puede usar el rol AmazonSecurityLakeMetaStoreManagerV2 creado por Security Lake.
   - Use un rol de servicio existente: puede elegir un rol de servicio existente de la lista de nombres del rol de servicio.
5. Seleccione Apply.

API

Para actualizar los permisos del rol (API)

Para actualizar los permisos mediante programación, utilice la UpdateDataLakeoperación de la API de Security Lake. Para actualizar los permisos mediante el AWS CLI, ejecute el update-data-lakecomando.

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

Eliminar el AmazonSecurityLakeMetaStoreManager rol

> **Important**
>
> Tras actualizar los permisos del 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. Inicie sesión en la AWS Management Console consola de Lake Formation y ábrala 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

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 puedes usar estas instrucciones para eliminar como fuente una fuente compatible de forma nativa. Servicio de AWS Para obtener información acerca de cómo eliminar un origen personalizado, consulte Recopilación de datos de orígenes personalizados.

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 un Servicio de AWS como fuente mediante programación, utilice el DeleteAwsLogSourcefuncionamiento de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando delete-aws-log-source. Los parámetros `sourceName` y `regions` son obligatorios. Si lo desea, puede limitar el alcance de la eliminación a algo específico o a uno específico. `accounts` `sourceVersion`

> **Important**
>
> Si 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 la organización.

En el siguiente ejemplo, se eliminan los registros de flujo de 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 el carácter de continuación de línea con barra invertida (\) para mejorar la legibilidad.

Obtener el estado de la colección de fuentes

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

Console

Para obtener 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 obtener el estado de la recopilación de registros en la región actual, utilice el GetDataLakeSourcesfuncionamiento de la API de Security Lake. Si está utilizando el AWS CLI, ejecute el comando get-data-lake-sources. Para el `accounts` parámetro, puede especificar uno o más Cuenta de AWS ID en forma de lista. Si su solicitud es correcta, Security Lake devolverá una instantánea de las cuentas de la región actual, incluidas 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 la 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"
```

Recopilación de datos de orígenes personalizados

Amazon Security Lake puede recopilar registros y eventos de orígenes de terceros personalizados. 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 de este rol lo establece una política AWS administrada llamada `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 rellena el campo AWS Glue Data Catalog con la tabla. También descubre automáticamente nuevos datos de origen y extrae las definiciones de los esquemas.

Para agregar un origen personalizado a Security Lake, debe cumplir con los siguientes requisitos:

1. 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 las fuentes que contienen varias categorías de datos, debe entregar cada clase de evento única de Open Cybersecurity Schema Framework (OCSF) como una fuente independiente. Security Lake crea una IAM función que permite a la fuente personalizada escribir en la ubicación especificada del bucket de S3.

   > **Note**
   >
   > Utilice la herramienta de OCSF validación para comprobar si la fuente personalizada es compatible con`OCSF Schema 1.1`.

2. Formato: cada objeto de S3 que se recopile del origen personalizado debe tener el formato de un archivo de Apache Parquet.
3. Esquema: se debe aplicar la misma clase de OCSF evento a cada registro de un objeto con formato Parquet.

Prácticas recomendadas de ingestión de orígenes personalizados

Para facilitar el procesamiento y las consultas de datos de forma eficiente, recomendamos seguir estas prácticas recomendadas al añadir un origen personalizado a Security Lake:

Particiones

Los objetos deben dividirse por ubicación de origen, Región de AWS y fecha. Cuenta de AWS

- La ruta de datos de la partición tiene el siguiente formato

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

Un ejemplo de partición es aws-security-data-lake-*us-west-2-lake-uid*/ext/*custom-source-name*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/.

- Si ha añadido una versión de origen a una fuente personalizada, la ruta de datos de la partición se formatea como

  bucket-name/ext/*custom-source-name*/*custom-source-version*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/

  Un ejemplo de partición que incluye la versión fuente esaws-security-data-lake-*us-west-2-lake-uid*/ext/*custom-source-name*/*custom-source-version*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/.

La siguiente lista describe los parámetros utilizados en la partición.

- bucket-name: nombre del bucket de Amazon S3 en el que Security Lake almacena los 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.
- source-version— Versión fuente de la fuente personalizada.
- region— Región de AWS en la que se escriben los datos.
- accountId— Cuenta de AWS ID al que pertenecen los registros de la partición de origen.
- eventDay: fecha en la que ocurrió el evento, formateada como una cadena de ocho caracteres (YYYYMMDD).

Tamaño y velocidad del objeto

Los archivos enviados a Security Lake deben enviarse en incrementos de entre 5 minutos y un día de evento. Los clientes pueden enviar archivos con una frecuencia superior a 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.

Ajustes de Parquet

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.

Ordenar

Dentro de cada objeto con formato Parquet, los registros deben ordenarse por tiempo para reducir el costo de la consulta de datos.

Requisitos previos para añadir un origen personalizado

Al agregar una fuente personalizada, Security Lake crea una IAM función que permite a la fuente 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}`, `region` es decir, el formato Región de AWS en el que se agrega la fuente personalizada. 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 al rol. El límite de permisos de este rol lo establece una política AWS administrada llamada `AmazonSecurityLakePermissionsBoundary`.

Temas

- Verificar permisos
- Cree un IAM rol que permita el acceso de escritura a la ubicación del depósito de Security Lake (APIy AWS CLI solo 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 esta opción para revisar las IAM políticas asociadas a su IAM identidad. 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 en el servidor, también necesitará permiso para `kms:CreateGrant``kms:DescribeKey`, y. `kms:GenerateDataKey`

> **Important**
>
> Si planea usar la consola de Security Lake para agregar una fuente personalizada, puede omitir el siguiente paso y continuar con. Adición de un origen personalizado La consola de Security Lake ofrece un proceso simplificado para empezar y crea todos los IAM roles necesarios o utiliza los roles existentes en su nombre.
> Si planea usar Security Lake API o AWS CLI agregar una fuente personalizada, continúe con el siguiente paso: crear un IAM rol que permita el acceso de escritura a la ubicación del bucket de Security Lake.

Cree un IAM rol que permita el acceso de escritura a la ubicación del depósito de Security Lake (APIy AWS CLI solo paso)

Si utiliza Security Lake API o va AWS CLI a añadir una fuente personalizada, añada esta IAM función para conceder AWS Glue permiso para rastrear los datos de origen personalizados e identificar las particiones de los datos. Estas particiones son necesarias para organizar los datos y crear y actualizar tablas en el catálogo de datos.

Tras crear este IAM rol, necesitará el nombre de recurso de Amazon (ARN) del rol para añadir una fuente personalizada.

Debe 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 en línea en su función para poder leer los archivos de datos de la fuente personalizada y crear o actualizar las tablas del catálogo de datos. Rastreador de AWS Glue AWS Glue

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

Adjunte la siguiente política de confianza para permitir que un Cuenta de AWS usuario pueda asumir el rol en función del identificador externo:

```
{
    "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 paquete administrado por el cliente AWS KMS key, también debes adjuntar la siguiente política a la función y a tu política KMS clave:

```
{
    "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}}"
    ]
}
```

Adición de un origen personalizado

Tras crear el IAM rol para invocar el AWS Glue rastreador, sigue estos pasos para añadir 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 situado en la esquina superior derecha de la página, seleccione la región en la que desee 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 OCSF evento que describa el tipo de datos que la fuente personalizada 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 CreateCustomLogSourceoperación de Security Lake. API Utilice la operación en el Región de AWS lugar en el que desee crear la fuente personalizada. Si está utilizando el AWS Command Line Interface (AWS CLI), ejecute el create-custom-log-sourcecomando.

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 OCSF eventos para describir el tipo de datos que la fuente enviará a Security Lake. Para obtener una lista de las clases de OCSF eventos compatibles 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 del recurso de Amazon (ARN) del IAM rol que creó para invocar el AWS Glue rastreador. Para ver los pasos detallados para crear un IAM rol, consulte Requisitos previos para añadir una fuente personalizada
- `providerIdentity`— Especifique la AWS identidad y el ID externo que utilizará la fuente para escribir registros y 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 los datos de origen personalizados actualizados en AWS Glue

Tras añadir 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.

Eliminación de un origen personalizado

Elimine un origen personalizado para dejar de enviar datos desde el origen a Security Lake.

Console

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 de la que desee 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 DeleteCustomLogSourceoperación de Security Lake. API Si está utilizando AWS Command Line Interface (AWS CLI), ejecute el delete-custom-log-sourcecomando. 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
```

Administración de suscriptores en Amazon 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 Amazon Security Lake.

Security Lake admite dos tipos de acceso de suscriptores:

- Acceso a los datos: los suscriptores reciben una notificación de 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 de nuevos objetos a través de un punto de conexión de suscripción o sondeando una cola de Amazon Simple Queue Service (Amazon SQS). Este tipo de suscripción se identifica `S3` en el `accessTypes` parámetro de la API. CreateSubscriber
- Acceso a consultas: 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 CreateSubscriberAPI.

Los suscriptores solo tienen acceso a los datos de origen Región de AWS que seleccionaste 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 de

> **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
- Administrar el acceso a las consultas para los suscriptores de Security Lake

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

Los suscriptores con acceso a los 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).

Requisitos previos para crear un suscriptor con acceso a los datos

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

Temas

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 necesita 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 ID externo del suscriptor

Para crear un suscriptor, además del Cuenta de AWS ID del suscriptor, también necesitarás su ID externa. El ID externo es un identificador único que te proporciona el suscriptor. Security Lake agrega el ID externo a la función de IAM del suscriptor que crea. El ID externo se utiliza al crear 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 al 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 los datos. 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 piensa utilizar la API de Security Lake o AWS CLI añadir un suscriptor, continúe con el siguiente paso: crear un rol de IAM para EventBridge invocar los destinos de la API.

Cree una función de IAM para invocar los destinos de la EventBridge API (paso único y de API) AWS CLI

Si utilizas Security Lake a través de la API o AWS CLI, crea un rol en AWS Identity and Access Management (IAM) que conceda EventBridge permisos a Amazon 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. Esta función de IAM no es necesaria si el suscriptor sondea datos de una cola de Amazon Simple Queue Service (Amazon SQS) o consulta datos directamente desde ella. AWS Lake Formation Para obtener más información sobre este tipo de método de acceso a los datos (tipo de acceso), consulte. Administrar el acceso a las consultas para los suscriptores de Security Lake

Adjunte la siguiente política a su función de IAM:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInvokeApiDestination",
            "Effect": "Allow",
            "Action": [
                "events:InvokeApiDestination"
            ],
            "Resource": [
                "arn:aws:events:{us-west-2}:{123456789012}:api-destination/
AmazonSecurityLake*/*"
            ]
        }
    ]
```

```
}
```

Adjunta la siguiente política de confianza a tu función de IAM EventBridge para poder asumirla:

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

Security Lake crea automáticamente una función 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 está protegido con una política AWS administrada llamada. `AmazonSecurityLakePermissionsBoundary`

Crear un suscriptor con acceso a los datos

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, selecciona la región en la que quieres 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 tal y como la has seleccionado actualmente Región de AWS y no se puede modificar.

6. En el caso de las fuentes de registro y eventos, elige qué fuentes está autorizado a consumir el suscriptor.
7. Como 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 ver los detalles de las notificaciones, si desea que Security Lake cree una cola de Amazon SQS que el suscriptor pueda sondear en busca de notificaciones de objetos, seleccione la cola de SQS. Si desea que Security Lake envíe notificaciones a un punto de conexión HTTPS, EventBridge seleccione el punto de conexión de suscripción.

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

   a. Introduzca el punto de conexión de la suscripción. Entre los ejemplos de formatos de punto de conexión 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 al servicio, 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 una nueva función de IAM, consulte Crear una función de IAM para invocar los destinos de la API. EventBridge
10. (Opcional) En el caso de las etiquetas, introduzca hasta 50 etiquetas para asignarlas al suscriptor.

    Una etiqueta es una etiqueta que 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 ayudarle a identificar, clasificar y administrar los recursos de diferentes maneras. Para obtener más información, consulte Etiquetado de recursos de Amazon Security Lake.
11. Seleccione Crear.

API

Para crear un suscriptor con acceso a los datos mediante programación, utilice el CreateSubscriberfuncionamiento de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando 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 desee que acceda el suscriptor.
- Para`subscriberIdentity`, especifique el identificador de AWS cuenta y el identificador 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

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 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 el carácter de continuación de línea con barra invertida (\) para mejorar la legibilidad.

(Opcional) Tras crear un suscriptor, utilice la operación de CreateSubscribernotificación para especificar cómo notificar al suscriptor cuando se escriban nuevos datos en el lago de datos de las fuentes a las que desea que acceda el suscriptor. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando create-subscriber-notification.

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

```
$ 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 obtenerlos`subscriberID`, utilice la ListSubscribersoperación 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 Amazon SQS o punto de enlace HTTPS) del suscriptor, utilice la operación UpdateSubscriberNotification o, si la utiliza AWS CLI, ejecute el comando update-subscriber-notification. 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

```
{
  "source": "aws.s3",
  "time": "2021-11-12T00:00:00Z",
  "account": "123456789012",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::example-bucket"
  ],
  "detail": {
    "bucket": {
```

```
      "name": "example-bucket"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b57f9512698f4b09e608f4f2a65852e5"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "securitylake.amazonaws.com"
  }
}
```

Actualización de un suscriptor de datos

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

Elija uno de los métodos de acceso y siga 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. Selecciona el suscriptor.
4. Seleccione Editar y, a continuación, realice una de las siguientes acciones:
   - Para actualizar las fuentes del suscriptor, introduzca la nueva configuración en la sección Fuentes de registros y eventos.
   - Para asignar o editar etiquetas para el suscriptor, cámbielas según sea necesario en la sección Etiquetas.
5. Cuando termine, elija Save (Guardar).

API

Para actualizar las fuentes de acceso a los datos de un suscriptor mediante programación, utilice el UpdateSubscriberfuncionamiento de la API de Security Lake. Si utilizas AWS Command Line

Interface (AWS CLI), ejecuta el comando 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 o a una determinada organización, utilice la ListSubscribersoperación. Si estás usando 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 GetSubscriberoperación. 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 AWS Command Line Interface (AWS CLI), ejecute el comando get-subscriber.

Para actualizar el método de notificación de un suscriptor, usa la operación de UpdateSubscribernotificación. Si utilizas AWS Command Line Interface (AWS CLI), ejecuta el comando update-subscriber-notification. Por ejemplo, puede especificar un nuevo punto de enlace HTTPS para el suscriptor o cambiar de un punto de enlace HTTPS a una cola de Amazon SQS.

Eliminar un suscriptor de datos

Si ya no desea que un suscriptor consuma datos de Security Lake, puede eliminarlo 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 desee eliminar.
4. Elija Eliminar y confirme la acción. Esto eliminará al suscriptor y todos los ajustes de notificación asociados.

API

Según su situación, realice una de las siguientes acciones:

- Para eliminar el suscriptor y todos los ajustes de notificación asociados, utilice el DeleteSubscriberfuncionamiento 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 operación de DeleteSubscriberNotification de la API de Security Lake. Si utilizas AWS Command Line Interface (AWS CLI), ejecuta el comando run the delete-subscriber-notification.

Administrar el acceso a las consultas para los suscriptores de Security Lake

Los suscriptores con acceso a 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

> **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.

Requisitos previos para crear un suscriptor con acceso a consultas

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

Temas

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

Verificar permisos

Antes de crear un suscriptor con acceso de consulta, 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 de consulta.

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

> **Important**
>
> Una vez que haya verificado los permisos:
>
> - Si piensa utilizar la consola de Security Lake para añadir un suscriptor con acceso de consulta, puede omitir el siguiente paso y continuar conOtorgue permisos de administrador de Lake Formation. Security Lake crea todas las funciones de IAM necesarias o utiliza las funciones 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 solo paso AWS CLI)

Cuando utilice la API de Security Lake o AWS CLI conceda acceso a una 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 al crear los roles de IAM necesarios.

Otorgue permisos de administrador de Lake Formation

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

Puede conceder permisos de administrador de Lake Formation para su función 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 data lake, para los usuarios y roles de IAM, elija el rol de administrador que se usa al acceder a la consola de Security Lake 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.

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

Crear un suscriptor con acceso a consultas

Elige el método que prefieras para crear un suscriptor con acceso de consulta en el actual Región de AWS. Un suscriptor solo puede consultar datos desde el Región de AWS lugar en el 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 identificadores externos, consulte Cómo utilizar un identificador externo al 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 conocer 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, selecciona la región en la que quieres 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 tal y como la has seleccionado actualmente Región de AWS y no se puede modificar.
6. En el caso de las fuentes de registros y eventos, elija las fuentes que desee que Security Lake incluya al devolver los resultados de la consulta.
7. En Método de acceso a 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 asignarlas al suscriptor.

   Una etiqueta es una etiqueta que 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 ayudarle a identificar, clasificar y administrar los recursos de diferentes maneras. Para obtener más información, consulte Etiquetado de recursos de Amazon Security Lake.
10. Seleccione Crear.

API

Para crear un suscriptor con acceso a consultas mediante programación, utilice el CreateSubscriberfuncionamiento de la API de Security Lake. Si utilizas AWS Command Line Interface (AWS CLI), ejecuta el comando 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 el suscriptor utiliza para consultar los datos de origen.

En el siguiente ejemplo, se 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 intercambio de tablas entre cuentas de Lake Formation para facilitar el acceso a las consultas de los suscriptores. Al crear un suscriptor con acceso de consulta en la consola, API o 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).

Al realizar determinados tipos de modificaciones en un suscriptor con acceso a consultas, Security Lake crea un nuevo recurso compartido. Para obtener más información, consulte Edición de un suscriptor con acceso a consultas.

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

1. Aceptar el recurso compartido: el suscriptor debe aceptar el recurso compartido que contiene `resourceShareArn` y `resourceShareName` que se genera al crear o editar el suscriptor. Elija uno de los siguientes métodos de acceso:
   - Para la consola y AWS CLI, consulte Aceptar una invitación para compartir recursos de AWS RAM.
   - Para la API, invoque la GetResourceShareInvitationsAPI. Filtra por `resourceShareArn` y `resourceShareName` para encontrar el recurso compartido correcto. Acepta la invitación con la AcceptResourceShareInvitationAPI.

   La invitación para compartir recursos vence en 12 horas, por lo que debes 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 transcurrido más de 12 horas, elimina al suscriptor de Lake Formation y vuelve a crearlo para recibir una nueva invitación para compartir recursos.
2. Crear un enlace de recursos a las tablas compartidas: el suscriptor debe crear un enlace de recursos a las tablas compartidas de Lake Formation en AWS Lake Formation (si usa la consola) o AWS Glue (si usa API/AWS CLI). Este enlace de recursos dirige la cuenta del suscriptor a las tablas compartidas. Elija uno de los siguientes métodos de acceso:
   - Para la consola y AWS CLI, consulte Crear un enlace de recurso a una tabla de catálogo de datos compartido en la Guía para AWS Lake Formation desarrolladores.
   - Para la API, invoque la AWS Glue CreateTableAPI. Recomendamos que los suscriptores también creen una base de datos única con la CreateDatabaseAPI 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 Security Lake recopila están disponibles automáticamente para consultarlos. Las consultas se ejecutan en el Cuenta de AWS suscriptor y los costos incurridos por 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 Uso compartido de datos entre cuentas en Lake Formation en la Guía para AWS Lake Formation desarrolladores.

Edición de un suscriptor con acceso a consultas

Security Lake permite realizar modificaciones en un suscriptor con acceso a consultas. Puede editar el nombre, la descripción, el identificador externo, el director (Cuenta de AWS ID) y las fuentes de registro que el suscriptor puede utilizar. 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 conocer 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

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, selecciona la región en la que deseas 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, selecciona la región en la que quieres 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, selecciona la región en la que quieres 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, selecciona la región en la que deseas 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 ID de cuenta, se elimina automáticamente el AWS RAM recurso compartido anterior para que el principal anterior no pueda consumir las fuentes de registro 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, selecciona la región en la que deseas 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 Guardar.

API

Para editar un suscriptor con acceso a consultas mediante programación, utilice el UpdateSubscriberfuncionamiento de la API de Security Lake. Si usa AWS Command Line Interface (AWS CLI), ejecute el comando 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 `subscriberIdentity` ello, especifique el (Cuenta de AWS ID) principal y el ID 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 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 Administrar el acceso a las consultas para los suscriptores de Security Lake.

Temas

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

La siguiente sección proporciona orientación sobre cómo consultar datos de Security Lake e incluye algunos ejemplos de consultas de fuentes compatibles de forma nativa. 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.

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 hallazgos
- `vpc_flow_1_0`: registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)

Ejemplo: todos los resultados de Security Hub de la tabla **`sh_findings_1_0`** de la región 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 de 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 toda la actividad desde la IP de origen a partir del 1 de marzo de 2023 en la tabla CloudTrail **`192.0.2.1`** **`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

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:

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
```

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 Route 53 Resolver:

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
```

Ejemplos de consultas de resultados de Security Hub

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

Estos son algunos ejemplos de consultas de los resultados 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 = 'AwsS3Bucket')
   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 resultados desde Security Hub 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
```

Consultas de ejemplo de registros de flujo de Amazon VPC

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 registros de flujo de Amazon VPC:

Tráfico específico Regiones de AWS 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 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)

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 Administrar el acceso a las consultas para los suscriptores de Security Lake.

La siguiente sección proporciona orientación sobre cómo consultar datos de Security Lake e incluye algunos ejemplos de consultas de fuentes compatibles de forma nativa. 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.

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 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 v2 AWS WAF

Ejemplo: todos los resultados de Security Hub de la tabla **`sh_findings_2_0`** de la región 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 de la IP de origen 192.0.2.1 que se registraron después de 20230301 (1 de marzo de 2023), en la tabla vpc_flow_2_0 de 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 cosas como nombres de usuario específicos, UID de recursos, IP, 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
```

Consultas de datos CloudTrail

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:

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
```

Consultas 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 para los registros de consultas de resolución de Route 53:

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
```

Consultas sobre los resultados de Security Hub

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

Estos son algunos ejemplos de consultas sobre los resultados de Security Hub:

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 = 'AwsS3Bucket')
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 resultados desde Security Hub 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
```

Consultas de registros de flujo de Amazon VPC

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 para Amazon VPC Flow Logs:

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
```

Consultas 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 para los registros de auditoría de Amazon EKS:

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» en 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
```

AWS WAF Consultas para registros de la 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 para los registros de la AWS WAF versión 2:

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 sus datos de manera que se almacenen de forma rentable, puede configurar los ajustes de retención de los datos. Dado que Security Lake almacena sus datos como objetos en bucket de Amazon Simple Storage Service (Amazon S3), la configuración de retención corresponde a una configuración de ciclo de vida de Amazon S3. Al configurar estos ajustes, puede especificar la clase de almacenamiento de Amazon S3 que prefiera y el período de tiempo para que los objetos de S3 permanezcan en esa clase de almacenamiento antes de que pasen a una clase de almacenamiento diferente o caduquen. Para obtener más información acerca de las configuraciones del ciclo de vida de Amazon S3, consulte Administración del ciclo de vida de almacenamiento en la Guía del usuario de Amazon Simple Storage Service.

En Security Lake, puede especificar la configuración de retención a nivel de región. Por ejemplo, puede optar por hacer la transición de todos los objetos de S3 de una clase de almacenamiento específica Región de AWS a la clase S3 Standard-IA 30 días después de haberlos escrito en el lago de datos. La clase de almacenamiento predeterminada de Amazon S3 es S3 Standard.

> **Important**
>
> 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 S3 Object Lock con el modo de retención predeterminado, se interrumpe la entrega de datos de registro normalizados al lago de datos.

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. Si no configura los ajustes de retención, Security Lake utiliza los ajustes predeterminados para una configuración del ciclo de vida de Amazon S3, es decir, almacenar los datos de forma indefinida mediante la clase de almacenamiento S3 Standard.

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 cuando se incorpore a Security Lake, utilice el CreateDataLakefuncionamiento de la API de Security Lake. Si está utilizando el 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 Save (Guardar).

API

Para actualizar la configuración de retención mediante programación, utilice UpdateDataLakela API de Security Lake. Si la está utilizando AWS CLI, ejecute el comando. update-data-lake 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`.

Por ejemplo, el siguiente AWS CLI comando actualiza la configuración de caducidad de los datos y la configuración de transición de 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

Open Cybersecurity Schema Framework (OCSF)

¿Qué es OCSF?

El Open Cybersecurity Schema Framework (OCSF) es un esfuerzo colaborativo AWS y de código abierto realizado por socios líderes en 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
Security Hub	Security Hub	AWS	Coincide con el valor ProductName de 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
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

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 Open Cybersecurity Schema Framework (OCSF)
- Los datos llegan en formato Apache Parquet

Las integraciones de suscriptores tienen las siguientes propiedades: pueden leer los datos fuente de Security Lake en un HTTPS punto final o en una cola de Amazon Simple Queue Service SQS (Amazon), o consultando directamente los datos fuente de AWS Lake Formation

En la siguiente sección, se explica con qué se integra Servicios de AWS Security Lake y cómo funciona cada integración.

Integración con AWS AppFabric

Tipo de integración: origen

AWS AppFabrices un servicio sin código que conecta las aplicaciones de software como servicio (SaaS) en toda la organización, de modo que los equipos de TI y seguridad puedan gestionar y proteger las aplicaciones 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 OCSF entregar los datos en formato de esquema y 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 OCSF normalizados 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 AppFabric conclusiones a Security Lake

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 orígenes personalizados.

Deje de recibir AppFabric registros en Security Lake

Para dejar de recibir registros de AppFabric auditoría, puede usar la consola de Security LakeAPI, Security Lake o AWS CLI eliminarlos AppFabric como fuente personalizada. Para obtener instrucciones, consulte Eliminación de un origen personalizado.

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 AWS recursos. 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 Service, puede obtener información más rápidamente para investigaciones de seguridad urgentes. Puede responder con rapidez a los incidentes de seguridad, lo que le ayudará 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 dominio de OpenSearch Service Service. Para visualizar los datos mediante los paneles prediseñados, navegue hasta los paneles y elija cualquiera de los paneles instalados.

Integración con Amazon QuickSight

Tipo de integración: suscriptor

Amazon QuickSight es un servicio de inteligencia empresarial (BI) a escala de nube que puedes utilizar para ofrecer easy-to-understand información a las personas con las que trabajas, estén donde estén. Amazon QuickSight se conecta a tus datos en la nube y combina datos de muchas fuentes diferentes. Amazon QuickSight 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.

QuickSight Panel de control de Amazon

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

Integración con Amazon SageMaker

Tipo de integración: suscriptor

Amazon SageMaker 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 que las herramientas de SageMaker aprendizaje automático estén disponibles en varios entornos de desarrollo integrados (). IDEs

SageMaker información

Puede generar información de aprendizaje automático para Security Lake con SageMaker Studio. SageMaker Studio 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 los 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.

Integración con Amazon Bedrock

Amazon Bedrock es un servicio totalmente gestionado que pone a su disposición modelos básicos de alto rendimiento (FMs) de las principales empresas emergentes de IA y Amazon para su uso de forma unificada. API 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 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 SQL consultas y visualizando los datos de su investigación. Para obtener más información, consulte Generar información basada en IA para Amazon Security Lake con Amazon SageMaker Studio y Amazon Bedrock.

Integración con AWS Security Hub

Tipo de integración: origen

AWS Security Hublе proporciona una visión completa del estado de su seguridad AWS y le ayuda a comprobar su entorno según los estándares y las mejores prácticas del sector de la seguridad. Security Hub 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 y agrega los hallazgos del Security Hub como origen en Security Lake, Security Hub comienza a enviar nuevos resultados y actualizaciones de los resultados existentes a Security Lake.

Cómo recibe Security Lake los resultados de Security Hub

En Security Hub, los problemas de seguridad se rastrean como resultados. Algunos resultados provienen de problemas detectados por otros AWS servicios o por socios externos. Security Hub también genera sus propios resultados mediante la ejecución continua y automática de controles de seguridad de conformidad con las normas. Las reglas están representadas por controles de seguridad.

Todos los resultados de Security Hub utilizan un JSON formato estándar denominado AWS Security Finding Format (ASFF).

Security Lake recibe los hallazgos de Security Hub y los transforma en Open Cybersecurity Schema Framework (OCSF).

Envío de los resultados de Security Hub a Security Lake

Para enviar los resultados del Security Hub a Security Lake, debe habilitar ambos servicios y añadir los resultados del Security Hub como origen en Security Lake. Para obtener instrucciones sobre cómo agregar una AWS fuente, consulteAñadir un como fuente Servicio de AWS.

Si desea que Security Hub genere resultados 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 .

Dejar de recibir resultados de Security Hub en Security Lake

Para dejar de recibir los resultados de Security Hub, puede usar la consola de Security Hub, Security Hub API o AWS CLI.

Consulte Deshabilitar y habilitar el flujo de hallazgos desde una integración (consola) o Inhabilitar el flujo de hallazgos desde una integración (Security Hub API AWSCLI) en la Guía del AWS Security Hub usuario.

Integraciones de terceros 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 Open Cybersecurity Schema Framework (OCSF)

Las integraciones de suscriptor tienen las siguientes propiedades:

- Lea los datos de origen de Security Lake en un HTTPS punto final o en una cola de Amazon Simple Queue Service (AmazonSQS), o consulte directamente los datos de origen de AWS Lake Formation
- Puede leer datos en formato Apache Parquet
- Capaz de leer los datos en un esquema OCSF

Las integraciones de servicios pueden ayudarlo a implementar Security Lake y otros Servicios de AWS en su organización. 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, visita AWSMarketplace.

Para solicitar que lo agreguen como una 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 los resultados a AWS Security Hub, también puedes revisarlos en Security Lake si la integración del Security Hub para Security Lake está habilitada. Para obtener información acerca de cómo activar la integración, consulte Integración con AWS Security Hub. Para obtener una lista de integraciones de terceros que envían resultados a Security Hub, consulte las Integraciones de productos de socios de terceros disponibles en la Guía del usuario de AWS Security Hub .

Antes de configurar tus suscriptores, verifica la compatibilidad con el OCSF registro de suscriptores. 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 de Security LakeAPI, o AWS Command Line Interface.

El administrador del lago de datos de Lake Formation debe conceder `SELECT` permisos en las bases de datos y tablas pertinentes a la IAM identidad 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 Administrar el 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
- Palo Alto Networks – XSOAR
- IBM – QRadar
- Query.AI – Query Federated Search
- SOC Prime

- 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 facilita el análisis y gestiona la detección y la respuesta (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 OCSF esquema y al formato Parquet.

Documentación de integración

Barracuda – Email Protection

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

Bosch Software and Digital Solutions – 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

ChaosSearchofrece acceso a datos multimodelo a los usuarios con sistemas abiertosAPIs, como Elasticsearch o con Kibana y SQL Superset incluidos de forma nativa. UIs 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

Cisco Security – Secure Firewall

Tipo de integración: origen

Al integrar Cisco Secure Firewall con Security Lake, puede almacenar los registros del firewall de forma estructurada y escalable. El eNcore cliente de Cisco transmite los registros del firewall desde el Firewall Management Center, realiza la conversión de un OCSF esquema a otro y los almacena en Security Lake.

Documentación de integración

Claroty – xDome

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 proteger los activos extendidos de Internet de las cosas (IoTXIoT) (que incluyen IoT y BMS activos) dentro de la redIIoT, a la vez que detectan automáticamente los primeros indicadores de amenazas.

Documentación de integración

CMD Solutions

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 – Amazon S3 Sink Connector

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

Contrast Security

Tipo de integración: Origen

Producto asociado para la integración: Contrast Assess

Contrast Security Assesses una IAST herramienta que ofrece detección de vulnerabilidades en tiempo real en aplicaciones web y microservicios. APIs 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 – Stream

Tipo de integración: origen

Puede utilizarla Cribl Stream para enviar datos desde cualquier fuente de terceros Cribl compatible a Security Lake de forma OCSF esquemática.

Documentación de integración

CrowdStrike – Falcon Data Replicator

Tipo de integración: origen

Esta integración extrae los datos de forma continua, los transforma CrowdStrike Falcon Data Replicator en un OCSF esquema y los envía a Security Lake.

Documentación de integración

CyberArk – Unified Identify Security Platform

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 forma de OCSF esquema.

Documentación de integración

Cyber Security Cloud – 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 and AI Engine (CAE)

Tipo de integración: suscriptor, servicio

Deloitte MXDR CAE le ayuda a almacenar, analizar y visualizar rápidamente sus datos de seguridad estandarizados. El CAE conjunto de funciones personalizadas de análisis, inteligencia artificial y aprendizaje automático proporciona automáticamente información útil basada en modelos que se utilizan con los datos OCSF formateados 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 recopilador para AWS apoyar la ingesta desde 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 — AIsaac (anteriormente Atos)

Tipo de integración: suscriptor

La AIsaac MDR plataforma consume los registros de VPC flujo introducidos en el OCSF esquema 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 en el esquema los datos de la red, incluidas las detecciones de IOCsExtraHop Reveal(x) 360, desde y hacia Security Lake OCSF

Documentación de integración

Falcosidekick

Tipo de integración: Origen

Falcosidekick recopila y envía los eventos de Falco a Security Lake. Esta integración exporta los eventos de seguridad mediante el OCSF esquema.

Documentación de integración

Fortinet - Cloud Native Firewall

Tipo de integración: origen

Al crear FortiGate CNF instancias en AWS, puede especificar Amazon Security Lake como destino de salida de registros.

Documentación de integración

Gigamon – Application Metadata Intelligence

Tipo de integración: origen

Gigamon Application Metadata Intelligence (AMI)potencia sus herramientas de supervisión de la observabilidad y el rendimiento de la red con atributos de metadatos fundamentales. SIEM 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

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

Insbuilt

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

Kyndryl se integra con Security Lake para proporcionar interoperabilidad de datos cibernéticos, inteligencia sobre amenazas y análisis basados en inteligencia artificial. Como suscriptor de acceso a datos, Kyndryl ingiere los eventos de AWS CloudTrail 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

Lacework – Polygraph

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

Laminarenvía los eventos de seguridad de los datos a Security Lake en OCSF forma esquemática, de forma que estén disponibles 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 ISV soluciones integradas para crear tareas personalizadas y generar información personalizada relacionada con las necesidades de los clientes.

Documentación de integración

Monad

Tipo de integración: origen

Monadtransforma automáticamente sus datos en un OCSF esquema y los envía a su lago de datos de Security Lake.

Documentación de integración

NETSCOUT – Omnis Cyber Intelligence

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. Estos resultados se generan en la cuenta del cliente NETSCOUT CyberStreams yOmnis Cyber

Intelligence, a continuación, se envían a Security Lake en forma de OCSF esquema. 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 los registros relacionados con la seguridad y la 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 ONE es una aplicación de suscriptor basada en Lambda. Se implementa en tu cuenta, lo activa AmazonSQS, y envía datos a New Relic través de claves New Relic de licencia

Documentación de integración

Okta – Workforce Identity Cloud

Tipo de integración: origen

Oktaenvía registros de identidad a Security Lake en un OCSF esquema a través de una EventBridge integración de Amazon. Okta System Logsin OCSF schema 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 OCSF registros 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 – Cloud Security Platform

Tipo de integración: origen

La plataforma de seguridad en la nube Orca sin agentes que AWS se integra con Security Lake al enviar los eventos de Cloud Detection and Response (CDR) en OCSF un esquema.

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 Cloudagrega los datos de detección de vulnerabilidades de sus VMs entornos nativos de la nube y los envía a Security Lake.

Documentación de integración

Palo Alto Networks – XSOAR

Tipo de integración: Suscriptor

Palo Alto Networks XSOARha creado una integración de suscriptores con XSOAR Security Lake.

Documentación de integración

Panther

Tipo de integración: suscriptor

Pantheradmite la ingesta de registros de Security Lake para su uso en búsquedas y detecciones.

Documentación de integración

Ping Identity – PingOne

Tipo de integración: origen

PingOneenvía alertas de modificación de cuentas a Security Lake en formato de OCSF esquema y Parquet, lo que le permite detectar los cambios en la cuenta y actuar en consecuencia.

Documentación de integración

PwC – Fusion center

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 – Query Federated Search

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. OCSF

Documentación de integración

Rapid7 – InsightIDR

Tipo de integración: suscriptor

InsightIDR, la XDR solución Rapid7SIEM/, puede ingerir los registros de Security Lake para detectar amenazas e investigar actividades sospechosas.

Documentación de integración

RipJar – Labyrinth for Threat Investigations

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 SentinelOne Singularity™ XDR plataforma amplía la detección y la respuesta en tiempo real a las cargas de trabajo de punto final, identidad y nube que se ejecutan en infraestructuras locales y de nube pública, incluidas Amazon Elastic Compute Cloud EC2 (Amazon), Amazon Elastic Container Service (AmazonECS) y Amazon Elastic Kubernetes Service (Amazon). EKS

Documentación de integración (inicie sesión en el portal de SentinelOne para revisar la documentación)

Sentra – Data Lifecyle Security Platform

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 se Sentra almacenan y, posteriormente, se transmiten a Security Lake en un esquema para su consulta. OCSF

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 OCSF esquema.

Documentación de integración

Splunk

Tipo de integración: suscriptor

El Splunk AWS complemento para Amazon Web Services (AWS) admite la ingesta 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 OCSF esquema 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 un OCSF esquema.

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 – Turbine

Tipo de integración: suscriptor

Swimlanerecopila los datos de Security Lake en un OCSF esquema 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

Talon

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

Tanium Unified Cloud Endpoint Detection, Management, and SecurityLa plataforma proporciona datos de inventario a Security Lake en forma de OCSF esquema.

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 security automation

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 – Enterprise Security Automation Platform

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 XDR plataforma abierta, Trellix XDR es compatible con la integración de Security Lake. Trellix XDRpuede aprovechar los datos OCSF del esquema 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 Securityenvía la siguiente información a Security Lake desde sus instancias de Amazon Elastic Compute Cloud (EC2):

- DNSActividad de consulta
- 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

Uptycsenvía una gran cantidad de datos en un OCSF esquema desde los activos locales 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 for AWS

Tipo de integración: origen

Al usarloVectra Detect for AWS, puede enviar alertas de alta fidelidad a Security Lake como una fuente personalizada mediante una plantilla dedicada AWS CloudFormation .

Documentación de integración

VMware Aria Automation for Secure Clouds

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 Security Lake 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 OCSF esquema, 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 – Zscaler Posture Control

Tipo de integración: Origen

Zscaler Posture Control™, una plataforma de protección de aplicaciones nativa de la nube, envía los resultados de seguridad a Security Lake en forma esquemática. OCSF

Documentación de integración

Seguridad en Amazon Security Lake

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS en 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 AWSProgramas de conformidad de . Para obtener información sobre los programas de conformidad que se aplican a Amazon Security Lake, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Security Lake. En los siguientes temas, se le mostrará cómo configurar Security Lake para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a monitorear y proteger los recursos de Security Lake.

Temas

Administración de identidades y accesos para Amazon Security Lake

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Security Lake. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Security Lake.

Usuario de servicio: si utiliza el servicio de Security Lake para realizar el trabajo, el administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Security Lake para realizar el trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Security Lake, consulte Solución de problemas de identidad y acceso de Amazon Security Lake.

Administrador de servicio: si está a cargo de los recursos de Security Lake en la empresa, probablemente tenga acceso completo a Security Lake. Su trabajo consiste en determinar a qué características y recursos de Security Lake deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Security Lake, consulteCómo funciona Amazon Security Lake con IAM.

IAMadministrador: si es IAM administrador, puede que desee obtener más información sobre cómo escribir políticas para administrar el acceso a Security Lake. Para ver ejemplos de políticas basadas en la identidad de Security Lake que puede utilizarIAM, consulte. Ejemplos de políticas basadas en identidades para Amazon Security Lake

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS API las solicitudes en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del AWS IAM Identity Center usuario y Uso de la autenticación multifactorial (MFA) AWS en la Guía del IAM usuario.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el

usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, 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 de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS . Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en la Guía AWS IAM Identity Center del usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

Un IAMrol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a una AWS API operación AWS CLI o o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio

haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos Servicios de AWS o para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
- Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.
- Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada 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 IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso dentro de la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos.

AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte Descripción general de JSON las políticas en la Guía del IAM usuario.

Los administradores pueden usar AWS JSON las políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos,

los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del IAMusuario.
- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada

una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

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 IAM usuario.

Cómo funciona Amazon Security Lake con IAM

Antes de administrar el IAM acceso a Security Lake, averigüe qué IAM funciones están disponibles para usar con Security Lake.

IAMfunciones que puedes usar con Amazon Security Lake

IAMcaracterística	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 las políticas)	Sí

IAMcaracterística	Compatibilidad con Security Lake
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 IAM funciones, consulte AWS los servicios con los que funcionan IAM en la Guía del IAM usuario.

Políticas basadas en identidad para Security Lake

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Security Lake es compatible con las políticas basadas en identidad. Para obtener más información, consulte Ejemplos de políticas basadas en identidades para Amazon Security Lake.

Políticas basadas en recursos de Security Lake

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos JSON de política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y

las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

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) `dearn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`. En este ejemplo, `region` es un Región de AWS lugar específico en el que ha activado Security Lake y `bucket-identifier` es una cadena alfanumérica única a nivel regional que Security Lake asigna al depósito. 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:

```
{
    "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:{DA-AccountID}:*"
                }
            }
        }
    ]
}
```

Para obtener más información sobre las políticas basadas en recursos, consulte Políticas basadas en identidad y políticas basadas en recursos en la Guía del usuario. IAM

Acciones de política para Security Lake

Compatibilidad con las acciones de política: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de 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 identidades para Amazon Security Lake.

Recursos de políticas para Security Lake

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

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 medianteARNs.

Para obtener una lista de los tipos de recursos de Security Lake y la ARN sintaxis de cada uno de ellos, consulte Tipos de recursos definidos por Amazon Security Lake en la Referencia de autorización 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 identidades para Amazon 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 AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios

valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del IAMusuario.

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 identidades para Amazon Security Lake.

Listas de control de acceso (ACLs) en Security Lake

SoportaACLs: 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. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Security Lake no es compatibleACLs, lo que significa que no se puede adjuntar ningún recurso ACL a un recurso de Security Lake.

Control de acceso basado en atributos (ABAC) con Security Lake

Soportes ABAC (etiquetas en las políticas): Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

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 recursos de Amazon 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 identidades para Amazon Security Lake.

Uso de credenciales temporales con Security Lake

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Servicios de AWS la guía del IAM usuario sobre cómo trabajar con IAM ellas.

Está utilizando credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte Cambiar a un rol (consola) en la Guía del IAMusuario.

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. 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.

Security Lake admite el uso de credenciales temporales.

Sesiones de acceso directo para Security Lake

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a una Servicio de AWS, junto con los que solicita, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos Servicios de AWS o para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

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

Una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

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

Admite 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 IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Security Lake usa un rol vinculado a un IAM servicio 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. Esta función vinculada a un servicio es una IAM función que está vinculada directamente a Security Lake. Security Lake lo 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 Función vinculada al servicio para Amazon Security Lake.

Ejemplos de políticas basadas en identidades para Amazon Security Lake

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Security Lake. Tampoco pueden realizar tareas con AWS Management Console, AWS Command Line Interface (AWS CLI) o. AWS API Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

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

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. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. 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 AWS

CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.

- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

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 realicen llamadas al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando realizar.

Para garantizar que los usuarios y los roles puedan usar la consola de Security Lake, cree IAM políticas que les proporcionen acceso a la consola. Para obtener más información, consulte IAMlas identidades en la Guía IAM del usuario.

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 se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
    "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.

```
{
    "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 se puede crear una política que permita a un usuario revisar los suscriptores mediante la consola de Security Lake o Security Lake. API 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.

```
{
    "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 sobre el uso de las claves de condición, consulte los elementos de la IAM JSON política: Condición en la Guía del IAM usuario. Para obtener información acerca del etiquetado de recursos de Security Lake, consulte Etiquetado de recursos de Amazon Security Lake.

AWS políticas gestionadas para Amazon 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 estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AmazonSecurityLakeMetastoreManager

Amazon Security Lake utiliza una AWS Lambda función para gestionar los metadatos de su lago de datos. Mediante el uso de esta función, Security Lake puede indexar las particiones del Amazon Simple Storage Service (Amazon S3) que contienen sus datos y archivos de datos en las tablas AWS Glue del catálogo de datos. Esta política gestionada 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 el resultado de la función Lambda en Amazon CloudWatch Logs.

- `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 o actualizan objetos en su lago de datos.
- `s3`— Permite a los directores realizar acciones específicas de lectura y escritura para el bucket de Amazon S3 que contiene sus datos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowWriteLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowGlueManage",
      "Effect": "Allow",
      "Action": [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
```

```
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowToReadFromSqs",
      "Effect": "Allow",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource": [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowMetaDataReadWrite",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid": "AllowMetaDataCleanup",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

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 tome ninguna medida para utilizar esta política. Si el lago de datos está cifrado con una AWS KMS clave gestionada por el cliente `kms:Decrypt` y se añaden `kms:GenerateDataKey` permisos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsForSecurityLake",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
```

```
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsForSecurityLake",
      "Effect": "Deny",
      "NotAction": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeBucket",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource": [
```

```
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeSQS",
      "Effect": "Deny",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "kms:ViaService": [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
```

```
          "kms:EncryptionContext:aws:s3:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:s3:arn": [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:sqs:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:sqs:arn": [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

AWS política gestionada: AmazonSecurityLakeAdministrator

Puedes adjuntar la `AmazonSecurityLakeAdministrator` política a un mandante 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. Luego, el principal 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 gestionar la replicación entre regiones de Amazon S3, el registro de nuevas particiones de datos, la ejecución de un rastreador de Glue con los datos añadidos a fuentes personalizadas o la notificación de nuevos datos a los suscriptores de puntos de conexión 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` gestionada, Security Lake requiere `lakeformation:PutDataLakeSettings` permisos para las funciones de incorporación y configuración. `PutDataLakeSettings`permite establecer un director de IAM como administrador de todos los recursos regionales de Lake Formation de la cuenta. Esta función debe `iam:CreateRole permission` ir acompañada de una `AmazonSecurityLakeAdministrator` política.

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 a Security Lake y el `AmazonSecurityLakeMetaStoreManager` rol (u otro rol específico) como 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 rol o usuario administrador de Security Lake:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutLakeFormationSettings",
            "Effect": "Allow",
            "Action": "lakeformation:PutDatalakeSettings",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "securitylake.amazonaws.com"
                }
            }
        }
    ]
}
```

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `securitylake`— Permite a los directores el acceso total a todas las acciones de Security Lake.
- `organizations`— Permite a los directores recuperar información de AWS Organizations 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 cuenta.
- `iam`— Permite a los directores crear funciones vinculadas a servicios para Security Lake y AWS Lake Formation Amazon EventBridge, como paso obligatorio a la hora de habilitar esos servicios. También permite crear y editar políticas para 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 de los suscriptores a las fuentes de Security Lake.
- `s3`— Permite a los directores crear y administrar depósitos de Security Lake y leer el contenido de esos depósitos.
- `lambda`— Permite a los directores gestionar las particiones de la AWS Glue tabla Lambda utilizadas para actualizar tras la entrega en AWS origen 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 utilizadas para notificar a los suscriptores los nuevos datos en las fuentes de Security Lake.
- `sqs`— Permite a los directores crear y administrar 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 gestionar los secretos que se utilizan para notificar a los suscriptores los nuevos datos en las fuentes de Security Lake a través de puntos de conexión HTTPS.

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

```
  {
    "Sid": "AllowActionsWithAnyResource",
    "Effect": "Allow",
    "Action": [
      "securitylake:*",
      "organizations:DescribeOrganization",
      "organizations:ListDelegatedServicesForAccount",
      "organizations:ListAccounts",
      "iam:ListRoles",
      "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
    "Effect": "Allow",
    "Action": [
      "glue:CreateCrawler",
      "glue:StopCrawlerSchedule",
      "lambda:CreateEventSourceMapping",
      "lakeformation:GrantPermissions",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "lakeformation:GetDatalakeSettings",
      "events:ListConnections",
      "events:ListApiDestinations",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowManagingSecurityLakeS3Buckets",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
```

```
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketNotification",
      "s3:PutBucketTagging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetBucketNotification"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaCreateFunction",
    "Effect": "Allow",
    "Action": [
      "lambda:CreateFunction"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaAddPermission",
    "Effect": "Allow",
    "Action": [
      "lambda:AddPermission"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
```

```
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringEquals": {
        "lambda:Principal": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "glue:CreateTable",
      "glue:GetTable"
    ],
    "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"
      }
    }
  },
  {
    "Sid": "AllowEventBridgeActions",
    "Effect": "Allow",
    "Action": [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
      "events:DeleteConnection",
      "events:DeleteApiDestination",
      "events:ListTargetsByRule",
      "events:RemoveTargets",
```

```
      "events:DeleteRule"
    ],
    "Resource": [
      "arn:aws:events:*:*:rule/AmazonSecurityLake*",
      "arn:aws:events:*:*:rule/SecurityLake*",
      "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
      "arn:aws:events:*:*:connection/AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowSQSActions",
    "Effect": "Allow",
    "Action": [
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes",
      "sqs:GetQueueURL",
      "sqs:AddPermission",
      "sqs:GetQueueAttributes",
      "sqs:DeleteQueue"
    ],
    "Resource": [
      "arn:aws:sqs:*:*:SecurityLake*",
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowKmsCmkGrantForSecurityLake",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
```

```
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "GenerateDataKey",
          "RetireGrant",
          "Decrypt"
        ]
      }
    }
  },
  {
    "Sid": "AllowEnablingQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "ram:ResourceArn": [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
      "ram:DeleteResourceShare"
    ],
    "Resource": "*",
    "Condition": {
```

```
      "StringLike": {
        "ram:ResourceShareName": "LakeFormation*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringCredentialsForSubscriberNotification",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect": "Allow",
```

```
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": [
          "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
          "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
```

```
        "iam:AssociatedResourceARN": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
```

```
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:subscriber/*"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:events:*:*:rule/AmazonSecurityLake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowOnboardingToSecurityLakeDependencies",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": [
      "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
      "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
          "apidestinations.events.amazonaws.com"
```

```
        ]
      }
    }
  },
  {
    "Sid": "AllowRolePolicyActionsforSubscibersandSources",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "StringEquals": {
        "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowRegisterS3LocationInLakeFormation",
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam:GetRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowIAMActionsByResource",
    "Effect": "Allow",
    "Action": [
      "iam:ListRolePolicies",
      "iam:DeleteRole"
```

```
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "S3ReadAccessToSecurityLakes",
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid": "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid": "S3ResourcelessReadOnly",
    "Effect": "Allow",
    "Action": [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  }
]
}
```

AWS política gestionada: SecurityLakeServiceLinkedRole

No puede adjuntar la política `SecurityLakeServiceLinkedRole` gestionada a sus entidades de IAM. Esta política está asociada a una función vinculada al servicio que permite a Security Lake

realizar acciones en su nombre. Para obtener más información, consulte Función vinculada al servicio para Amazon Security Lake.

AWS política gestionada: función AWS GlueService

La política `AWS GlueServiceRole` administrada invoca el AWS Glue rastreador y permite AWS Glue rastrear los datos de origen personalizados e identificar los metadatos de las particiones. Estos metadatos son necesarios para crear y actualizar tablas en el catálogo de datos.

Para obtener más información, consulte Recopilación de datos de orígenes personalizados.

Security Lake actualiza las políticas AWS administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas de 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
Función vinculada a servicios para Amazon Security Lake: actualización de los permisos de funciones vinculadas a servicios existentes	Hemos añadido AWS WAF acciones a la política AWS gestionada de la política. `SecurityLakeServiceLinkedRole` 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 las acciones del SID a la política.	13 de mayo de 2024

Cambio	Descripción	Fecha
AmazonSecurityLake MetastoreManager: actualización de una política actual	Security Lake actualizó la política para añadir una acción de limpieza de metadatos que le permite eliminar los metadatos de su lago de datos.	27 de marzo de 2024
AmazonSecurityLakeAdministrator: actualización de una política actual	Security Lake actualizó la política para permitir `iam:PassRole` el nuevo `AmazonSecurityLakeMetastoreManagerV2` rol y permitir a Security Lake implementar o actualizar los componentes del lago de datos.	23 de febrero de 2024
AmazonSecurityLake MetastoreManager: política nueva	Security Lake agregó una nueva política administrada que otorga permisos a Security Lake para administrar los metadatos de 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 rastrear los cambios en sus políticas AWS administradas.	29 de noviembre de 2022

Función vinculada al servicio para Amazon Security Lake

Security Lake usa un rol vinculado a un servicio AWS Identity and Access Management (IAM) denominado. `AWSServiceRoleForSecurityLake` Este rol vinculado a servicios es un rol de IAM que está vinculado directamente a Security Lake. Security Lake lo predefine 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 al servicio en todos los lugares en los Regiones de AWS que Security Lake está disponible.

La función vinculada al servicio elimina la necesidad de añadir manualmente los permisos necesarios al configurar Security Lake. Security Lake define los permisos de este rol vinculado al 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 adjuntar 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 Permisos de roles vinculados a servicios 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 de , ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para revisar la documentación acerca del rol vinculado al servicio en cuestión.

Temas

Permisos de rol vinculados al servicio para Security Lake

Security Lake usa el rol vinculado al 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 gestionadas de Amazon Security Lake, consulte AWS gestionar las políticas de Amazon Security Lake.

La política de permisos del rol, denominada política AWS administrada`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:

- Utilice 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
- Utilice AWS CloudTrail acciones para recuperar información sobre el rol vinculado al servicio
- Utilice AWS WAF acciones para recopilar AWS WAF registros cuando esté habilitada como fuente de registros en Security Lake
- Utilice `LogDelivery` esta acción para crear o eliminar una suscripción de entrega de AWS WAF registros.

El rol se configura con la siguiente política de permisos:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "OrganizationsPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DescribeOrgAccounts",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:DescribeAccount"
            ],
            "Resource": [
                "arn:aws:organizations::*:account/o-*/*"
            ]
        },
        {
            "Sid": "AllowManagementOfServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateServiceLinkedChannel",
                "cloudtrail:DeleteServiceLinkedChannel",
                "cloudtrail:GetServiceLinkedChannel",
                "cloudtrail:UpdateServiceLinkedChannel"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
        },
        {
            "Sid": "AllowListServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:ListServiceLinkedChannels"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DescribeAnyVpc",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListDelegatedAdmins",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "organizations:ServicePrincipal": "securitylake.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowWafLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration",
                "wafv2:GetLoggingConfiguration",
                "wafv2:ListLoggingConfigurations",
                "wafv2:DeleteLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "wafv2:LogScope": "SecurityLake"
                }
            }
        },
        {
            "Sid": "AllowPutLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-
security-lake-*"
                }
            }
        },
        {
            "Sid": "ListWebACLs",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LogDelivery",
```

```
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "wafv2.amazonaws.com"
                    ]
                }
            }
        }

    ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación 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.

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 al 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 al servicio, primero debe confirmar que el rol no tiene sesiones activas y eliminar todos los recursos que esté utilizando. `AWSServiceRoleForSecurityLake`

> **Note**
>
> Si Security Lake utiliza el `AWSServiceRoleForSecurityLake` rol al intentar eliminar los recursos, es posible que no se pueda eliminar. 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 en su cuenta. Cuando vuelva a activar Security Lake, Security Lake volverá a crear automáticamente el rol vinculado al servicio.

Compatible con el Regiones de AWS rol vinculado al servicio de Security Lake

Security Lake admite el uso del rol `AWSServiceRoleForSecurityLake` vinculado al servicio en todos los Regiones de AWS lugares donde Security Lake esté disponible. Para obtener una lista de las regiones en las que Security Lake está disponible actualmente, consulte Regiones y puntos de conexión de Amazon Security Lake.

Protección de los datos en Amazon Security Lake

El modelo de se aplica a protección de datos en Amazon Security Lake. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

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:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma federal de procesamiento de información () 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 dispositivo Servicios de AWS mediante la consola, API AWS CLI, o. AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar la solicitud a ese servidor.

Cifrado en reposo

Amazon Security Lake almacena de forma segura sus datos en reposo mediante soluciones de AWS cifrado. El registro de seguridad sin procesar y los datos de eventos se almacenan en un bucket de Amazon Simple Storage Service (Amazon S3) de varios usuarios en una cuenta que administra Security Lake. 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 tareas de extracción, transformación y carga (ETL) sobre datos sin procesar de registros y eventos. Los datos procesados permanecen cifrados en la cuenta de servicio de Security Lake.

Una vez finalizados los ETL trabajos, Security Lake crea depósitos de S3 de un solo usuario en su cuenta (un depósito por cada depósito en el Región de AWS que haya activado Security Lake). Los

datos se almacenan en el bucket de S3 multiinquilino solo de forma temporal hasta que Security Lake pueda entregarlos de forma fiable a los buckets de 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 depósito de S3, puede elegir una clave de cifrado gestionada por S3 o una clave gestionada por el cliente (de). AWS KMS Ambas opciones utilizan el cifrado simétrico.

Uso de una KMS clave para cifrar sus 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 claves de cifrado administradas por Amazon S3 (-S3). SSE Para proporcionar una capa de seguridad que administre 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 usarloSSE: KMS con el Security Lake API oCLI, primero se crea una KMS clave o se usa 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 AWS KMS se utilizan para dar a Security Lake acceso a una KMS clave de la cuenta de un 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 por su clave gestionada por el cliente.
- Envíe `RetireGrant` las solicitudes a AWS KMS. Al actualizar su lago de datos, esta operación permite retirar la subvención que se agregó a la AWS KMS clave para su ETL procesamiento.

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 utilizar una KMS clave existente para cifrar los datos de Security Lake, debe modificar la política de claves de la KMS clave. La política clave debe permitir que la IAM función asociada a la ubicación del lago de datos de Lake Formation utilice la KMS clave para descifrar los datos. Para obtener instrucciones sobre cómo cambiar la política de claves de una KMS clave, consulte Cambiar una política de claves en la Guía para AWS Key Management Service desarrolladores.

Su KMS clave puede aceptar solicitudes de concesión, lo que permite a Security Lake acceder a la clave, cuando crea una política de claves o utiliza 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 su KMS clave:

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleRole"}
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

IAMPermisos necesarios cuando se utiliza una clave gestionada por el cliente

Consulte la sección Primeros pasos: requisitos previos para obtener una descripción general de las IAM funciones que debe crear para usar Security Lake.

Al añadir una fuente personalizada o un suscriptor, Security Lake crea IAM roles en su cuenta. Estos roles están pensados para compartirse con otras IAM identidades. 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 gestionada denominada `AmazonSecurityLakePermissionsBoundary` establece los límites de los permisos para estas funciones.

Cifrar las colas de Amazon SQS

Al crear su lago de datos, Security Lake crea dos colas de Amazon Simple Queue Service SQS (Amazon) sin cifrar en la cuenta de administrador de Security Lake delegada. Debe cifrar estas colas

para proteger los datos. El cifrado predeterminado del lado del servidor (SSE) 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 servicio Amazon S3 los permisos principales para trabajar con las colas cifradas. Para obtener instrucciones sobre cómo conceder estos permisos, consulte ¿Por qué no se envían las notificaciones de eventos de Amazon S3 a una SQS cola de Amazon que utiliza cifrado del lado del servidor? en el Centro de conocimiento AWS .

Dado que Security Lake AWS Lambda admite tareas de extracción, transferencia y carga (ETL) en sus datos, también debe conceder permisos a Lambda para gestionar los mensajes de sus colas de AmazonSQS. 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 Transport Layer Security (TLS) 1.2. HTTPSLas solicitudes directas que se envían al Security Lake APIs se firman mediante el algoritmo AWS Signature versión 4 para establecer una conexión segura.

Optar por no utilizar sus 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. 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 Security Lake y las funcionalidades de otros servicios de AWS seguridad, Security Lake puede recopilar dichos datos en el futuro, incluidos los datos que 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 estar gestionadas de forma centralizada por AWS Organizations. Si aún no ha creado una organización para sus AWS cuentas, consulte Creación y administración de 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

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

> **Note**
>
> No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

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

Para seguir el principio de privilegios mínimos, conceda el conjunto mínimo de permisos de la política de acceso para los roles, grupos de usuarios y usuarios de AWS Identity and Access Management (IAM). Por ejemplo, puede permitir que un usuario de IAM vea una lista de fuentes de registro en Security Lake, pero no cree fuentes ni suscriptores. Para obtener más información, consulte Ejemplos de políticas basadas en identidades para Amazon Security Lake

También puede utilizar AWS CloudTrail para realizar un seguimiento del uso de la API en Security Lake. CloudTrail proporciona un registro de las acciones de la API que realiza un usuario, un rol o un grupo en Security Lake. Para obtener más información, consulte Registro de llamadas a la API de Amazon Security Lake mediante AWS 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.

Integración con Security Hub

Integre Security Lake y AWS Security Hub pare recibir resultados de Security Hub en Security Lake. Security Hub genera resultados a partir de múltiples Servicios de AWS diferentes e integraciones de terceros. Recibir los resultados de Security Hub le ayuda a obtener una visión general de su postura de cumplimiento y de si está cumpliendo con las prácticas recomendadas de seguridad de AWS.

Para obtener más información, consulte Integración con AWS Security Hub.

Supervisión de los eventos de Security Lake

Puede supervisar Security Lake mediante las métricas de Amazon CloudWatch. CloudWatch recopila los 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 Métricas de CloudWatch para Amazon Security Lake.

Resiliencia de Amazon Security Lake

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. 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 Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, Security Lake, que ofrece los datos con Amazon Simple Storage Service (Amazon S3), ofrece varias características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los 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.

APILas llamadas 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). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta asociada a un director. IAM También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Configuración y análisis de vulnerabilidades en Security Lake

La configuración y los controles de TI son una responsabilidad compartida entre AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad compartida de AWS.

Supervisión de Amazon Security Lake

Security Lake está integrado con AWS CloudTrail, que es un servicio que proporciona un registro de las acciones realizadas en Security Lake por un usuario, un rol u otro servicio de 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. Mediante el uso de la información recopilada por CloudTrail, puede determinar qué solicitudes se realizaron en 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 Amazon Security Lake mediante AWS CloudTrail.

Security Lake y Amazon CloudWatch están integrados, por lo que puede recopilar, ver y analizar métricas de los registros que Security Lake recopila. Las métricas de CloudWatch para su lago de datos de Security Lake se recopilan automáticamente y se insertan en CloudWatch a 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 que Security Lake envía a CloudWatch, consulte Métricas y dimensiones de Security Lake.

Métricas de CloudWatch para Amazon Security Lake

Puede supervisar Security Lake con Amazon CloudWatch, que recopila y procesa los datos sin procesar cada minuto y los convierte en métricas legibles casi 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
- Ver métricas de CloudWatch para Amazon Security Lake
- Configuración de alarmas de CloudWatch para las métricas de Security Lake

Métricas y dimensiones de Security Lake

El espacio de nombres de `AWS/SecurityLake` incluye las siguientes métricas.

Métrica	Descripción
`ProcessedSize`	El volumen de datos de Servicios de AWS compatibles de forma nativa que se encuentra actualmente almacenado en su lago de datos. Unidades: bytes

Las siguientes dimensiones están disponibles para métricas de Security Lake.

Dimensión	Descripción
`Account`	Métrica de `ProcessedSize` para una Cuenta de AWS específica. Esta dimensión solo está disponible cuando ve las `Per-Account Source Version Metrics` en CloudWatch.
`Region`	Métrica de `ProcessedSize` para una Región de AWS específica.
`Source`	Métrica de `ProcessedSize` para un origen de registro de AWS específico.
`SourceVersion`	Métrica de `ProcessedSize` para una versión específica de un origen de registro de AWS.

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`).

Ver métricas de CloudWatch para Amazon Security Lake

Puede monitorear las métricas de Amazon Security Lake mediante la consola de CloudWatch, la interfaz de la línea de comandos (CLI) propia de CloudWatch o mediante programación con la API de

CloudWatch. Elija el método que prefiera y siga estos pasos para acceder a las métricas de Security Lake.

CloudWatch console

1. Abra la consola de CloudWatch 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 API de CloudWatch, utilice la acción `GetMetricStatistics`.

AWS CLI

Para acceder a las métricas de Security Lake utilizando la AWS CLI, ejecute el comando `get-metric-statistics`.

Para obtener más información sobre la supervisión mediante métricas, consulte Uso de métricas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Configuración de alarmas de CloudWatch para las métricas de Security Lake

Con CloudWatch, también puede establecer alarmas cuando se llega al umbral de una métrica. Por ejemplo, puede configurar una alarma para la métrica ProcessedSize, de modo que reciba una notificación cuando el volumen de datos de un origen específico supere un umbral determinado.

Para obtener instrucciones sobre cómo configurar alarmas, consulte Uso de alarmas de Amazon CloudWatch en la Guía del usuario de CloudWatch.

Registro de llamadas a la API de Amazon Security Lake mediante AWS CloudTrail

Amazon Security Lake está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas en Security Lake por un usuario, un rol un servicio de AWS. 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 un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para Security Lake. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información que recopila CloudTrail, puede determinar la solicitud que se hizo a Security Lake, la dirección IP desde la que se hizo dicha solicitud, quién la hizo y cuándo, además de información adicional.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información sobre Security Lake en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad en Security Lake, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la Cuenta de AWS, incluidos los eventos de Security Lake, cree una traza. Un registro de seguimiento permite a CloudTrail enviar eventos como archivos de registro a un bucket de Amazon S3 que 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. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail

- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Security Lake las registra CloudTrail y se documentan en la Referencia de la API de Security Lake. Por ejemplo, las llamadas a las acciones `UpdateDataLake`, `ListLogSources` y `CreateSubscriber` generan entradas en los archivos de log de CloudTrail.

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 las credenciales raíz o del usuario de AWS Identity and Access Management.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de Security Lake

Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para la acción `GetSubscriber` 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 recursos de Amazon 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

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 parte AWS de. 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 AWS Resource Groups 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 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. AWS Billing and Cost Management 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:

```
{
    "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 Editar.
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 incluye 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.

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 el ListTagsForResourcefuncionamiento de la API 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 suscriptor 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": ""
        }
    ]
}
```

Dónde `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.

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, revisa cualquier política AWS Identity

and Access Management (de IAM) que pueda usar 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 Editar.
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 incluye 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 solo 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.

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, revisa 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 Editar.
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 API UntagResourcede 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 de Amazon Security Lake

Consulte los siguientes temas si tiene problemas al utilizar 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 del Security Lake. API 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, utilice la CreateDataLakeExceptionSubscriptionoperación de Security LakeAPI. Se puede notificar al usuario por correo electrónico, mediante entrega a una cola de Amazon Simple Queue Service (AmazonSQS), entrega a una AWS Lambda función u otro protocolo compatible.

Por ejemplo, el siguiente AWS CLI comando envía las notificaciones de las excepciones de Security Lake a la cuenta especificada mediante SMS entrega. 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 Amazon Security Lake.

400 AccessDenied

Es posible que reciba este error cuando añada una fuente personalizada y llame al `CreateCustomLogSource`API.

Para resolver el error, revise sus permisos de Lake Formation. El IAM rol al que se llama 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: línea 1:8: SELECT * no está permitida en una relación que no tiene columnas

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 al IAM rol que está utilizando al iniciar 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 al director de la persona que llamó ARN 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. Borra los principios que estén etiquetados como No se encuentra en yIAM, a continuación, selecciona Guardar.
6. Vuelva a intentar la operación de Security Lake.

Security Lake CreateSubscriber with Lake Formation no creó una nueva invitación para compartir RAM recursos 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, versiones

2 y 3, optimiza la cantidad de AWS RAM recursos compartidos al mapear varias concesiones de permisos entre cuentas con un AWS RAM recurso compartido.

Asegúrese de comprobar que el nombre del recurso compartido tiene el identificador externo que especificó al crear el suscriptor y que el recurso compartido ARN coincide con el de la respuestaARN. `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)` — SecurityLake _Glue_Partition_Update_Lambda_***#region>***función.
   - `Source version 2 (OCSF 1.1.0)` – AmazonSecurityLakeMetastoreManager_***#region>***función.
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 de Security Lake o la. CreateDataLakeAPI

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 ayudarle a diagnosticar y solucionar los problemas comunes que pueden surgir al trabajar con Security Lake yIAM.

No tengo autorización para realizar una acción en Security Lake

Si AWS Management Console 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.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver los detalles de una imagen ficticia*`subscriber`*, pero no tiene los `SecurityLake:`*`GetSubscriber`* permisos ficticios.

```
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`*.

No estoy autorizado a realizar 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 el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta usar 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 AWS el 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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Security Lake es compatible con estas características, consulte Cómo funciona Amazon Security Lake con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un IAM usuario en otro de tu Cuenta de AWS propiedad en la Guía del IAMusuario.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. 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.

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 hallazgos y Amazon VPC Flow Logs).

Conversión de datos

Estos costos se derivan del volumen de Servicio de AWS registros y eventos que Security Lake normaliza en forma de Open Cybersecurity Schema Framework (OCSF) 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.
- AmazonSQS: estos costes se derivan de la creación de una SQS cola de Amazon para la entrega de mensajes. Para obtener más información, consulta los SQSprecios de Amazon.

- 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.

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 ver una lista completa de los servicios auxiliares, consulta 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 costes cubren el uso de Security Lake por parte de todas las cuentas de la organización e incluyen la conversión al formato Open Cybersecurity Schema Framework (OCSF) y 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 coste actual previsto de Security Lake Región de AWS para los próximos 30 días naturales, en función del uso real durante el período 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. 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 de conexión de Amazon 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 Amazon 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.

Para los orígenes personalizados, al desactivar Security Lake, debe desactivar todos los orígenes fuera de la consola de Security Lake. Si no se desactiva una integración, las integraciones de origen seguirán 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.

Recomendamos eliminar AWS Glue las tablas antes de volver a activar Security Lake para garantizar que el acceso a las consultas de los suscriptores funcione correctamente. Cuando Security Lake se vuelve a activar, se crea un nuevo lago de datos (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 antiguo bucket de Amazon S3. Si desea consultar datos antiguos, debe moverlos al nuevo bucket 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 el DeleteDataLakefuncionamiento 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"
```

Preguntas frecuentes

Actualización de Security Lake a la última versión de parquet

El 20 de mayo de 2024, Amazon Security Lake se actualizará a la última versión de parquet.

¿Por qué Security Lake realiza esta actualización?

Como parte de los esfuerzos continuos de Amazon para ofrecer a nuestros clientes servicios seguros y eficientes, Security Lake actualiza periódicamente las dependencias, las bibliotecas, las API y las herramientas de terceros. Security Lake también se asegura de que los clientes utilicen las últimas extensiones de todos los estándares, incluida la especificación general.

En raras ocasiones, esto puede provocar cambios menores en la forma en que se almacenan o procesan los datos. Los cambios siempre son compatibles con versiones anteriores dentro de los estándares comunitarios establecidos.

Security Lake normaliza los archivos de registro de seguridad de los clientes al formato OCSF y los expone en un formato de parqué eficiente desde el punto de vista de las consultas. Security Lake está realizando este cambio para garantizar la adopción sin problemas del último formato de parquet. Para obtener más información, consulte Formato de parquet.

¿Dónde puedo obtener más información sobre el cambio en las especificaciones del parquet?

Para obtener más información, consulte Marca de tiempo obsoleta ConvertedType en el repositorio de formato parquet. GitHub

¿Esta actualización afecta a mis integraciones de Security Lake?

Si solo usa las herramientas de Amazon Athena o Apache (Spark, Hive, Impala, Hadoop) para acceder a las tablas de Security Lake, no habrá cambios. Las API y las herramientas del cliente gestionarán automáticamente los cambios relacionados con la actualización de forma transparente.

Si utiliza otras herramientas de cliente, Security Lake recomienda comprender las nuevas formas de almacenar y gestionar los campos de fecha y hora. En la siguiente tabla se enumeran las pequeñas diferencias que puede observar entre los datos sintéticos antiguos y los nuevos.

Cambios en los datos sintéticos

AWS Servicios	Tipo	Actuales	New
Amazon Athena	Fecha/hora	1970-01-20 03:04:05.399 000	Sin cambios
Chispa Apache	Fecha/hora	1970-01-20T 00:04:05.000 -03:00	Sin cambios
PyArrow	Fecha/hora	1970-01-20 03:04:05	1970-01-20 03:04:05 + 00:00 La introducción del marcador de zona horaria UTC ha cambiado.

¿Cómo puedo identificar los cambios en el procesamiento del formato parquet?

Descargue el archivo zip parquet_format.zip. El archivo zip se compone de dos archivos.

- Datos de pruebas sintéticas generados por el marco anterior: `parquet_format_old.parquet`
- Datos de pruebas sintéticas generados por el nuevo marco: `parquet_format_new.parquet`

Pruebe las herramientas de su cliente y compare los datos de prueba sintéticos generados por el marco anterior con los datos generados por el nuevo marco.

Si observa cambios notables, utilice las recomendaciones de la `Changes in synthetic data` tabla. Si necesitas más ayuda, ponte en contacto con el servicio de AWS asistencia.

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: 10 de junio de 2024

Cambio	Descripción	Fecha
Disponibilidad regional	Security Lake ya está disponible en (EE. UU. este) y AWS GovCloud AWS GovCloud (EE. UU., oeste). 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 gestionada existente	Security Lake agregó AWS WAF acciones a la política AWS administrada de 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 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 gestionada existente	Security Lake agregó acciones de SID a la `AmazonSecurityLakePermissionsBoundary` política.	13 de mayo de 2024
Actualización de la política gestionada existente	Security Lake actualizó la política del AmazonSecurityLakeMetastoreManager para añadir una acción de limpieza de metadatos que le permite eliminar los metadatos de su lago de datos.	27 de marzo de 2024
Nuevas versiones fuente	Actualice los permisos de su rol para ingerir datos de las nuevas versiones de las fuentes 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 registro. 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 gestionada existente	Security Lake actualizó la política para permitir `iam:PassRole` el nuevo `AmazonSecurityLakeMetastoreManagerV2` rol y permitir a Security Lake implementar o actualizar los componentes del lago de datos.	23 de febrero de 2024
Nueva política gestionada	Security Lake agregó una nueva política AWS administrada, la `AmazonSecurityLakeMetastoreManager` política. Esta política otorga permisos para que Security Lake administre los metadatos de su lago de datos.	23 de enero de 2024
Disponibilidad regional	Security Lake ya está disponible en las siguientes Regiones de AWS regiones: 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 suscriptores 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 gestionada	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 las siguientes Regiones de AWS regiones: 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 utiliza la consola de Security Lake para activar y empezar a utilizar 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.