Manual do usuário

Amazon Security Lake

Amazon Security Lake: Manual do usuário

Table of Contents

O que é o Amazon Security Lake?

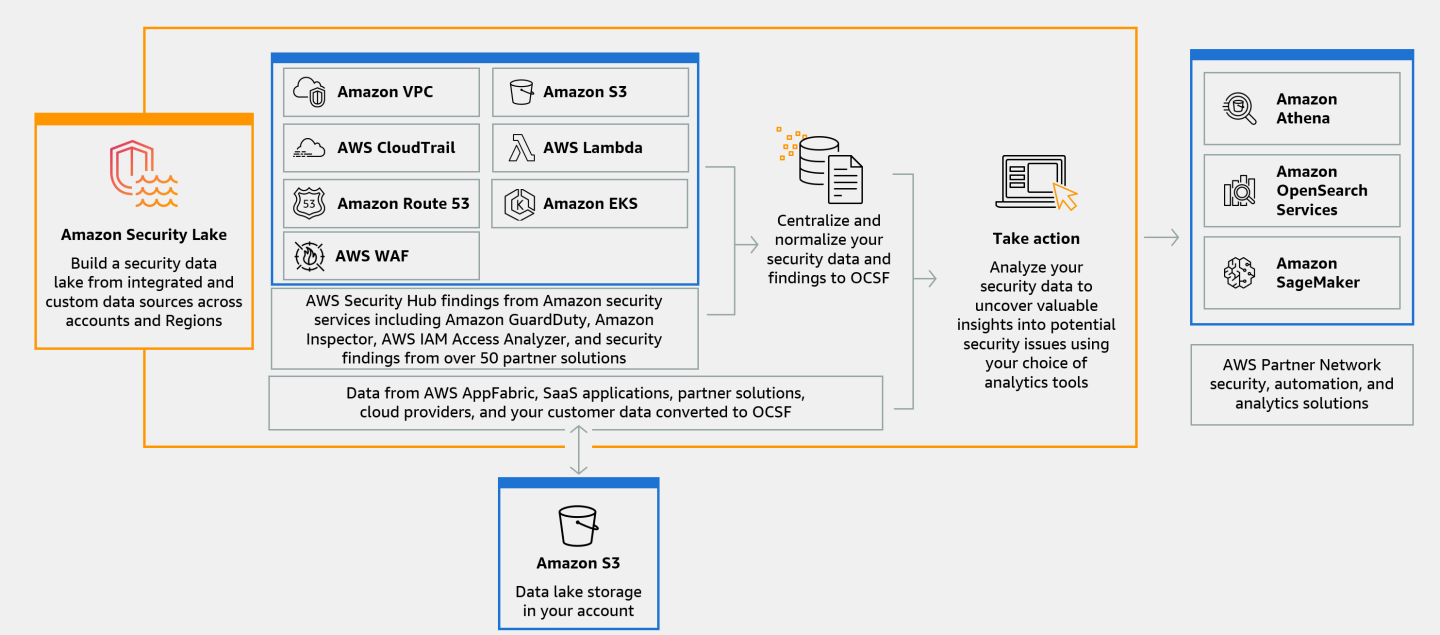
O Amazon Security Lake é um serviço de data lake de segurança totalmente gerenciado. Você pode usar o Security Lake para centralizar automaticamente os dados de segurança de AWS ambientes, provedores de SaaS, locais, fontes de nuvem e fontes de terceiros em um data lake específico que é armazenado em seu. Conta da AWS O Security Lake ajuda você a analisar dados de segurança, para que você tenha uma compreensão mais integral das posturas de segurança de toda a organização. Com o Security Lake, você também pode melhorar a proteção das suas workloads, aplicações e dados.

O data lake é respaldado pelos buckets do Amazon Simple Storage Service (Amazon S3). Você é o proprietário dos seus dados.

O Security Lake automatiza a coleta de logs e de dados de eventos relacionados à segurança a partir de serviços integrados da Serviços da AWS e de terceiros. Também ajuda você a gerenciar o ciclo de vida dos dados com configurações personalizáveis de retenção e replicação. O Security Lake converte dados ingeridos ao formato Apache Parquet e a um esquema padrão de código aberto chamado Open Cybersecurity Schema Framework (OCSF). Com o suporte do OCSF, o Security Lake normaliza e combina dados de segurança de AWS uma ampla variedade de fontes de dados de segurança corporativa.

Outros serviços Serviços da AWS e serviços de terceiros podem assinar os dados armazenados no Security Lake para resposta a incidentes e análise de dados de segurança.

Visão geral do Security Lake



Atributos do Security Lake

Veja como o Security Lake ajuda você a centralizar, gerenciar e assinar logs e dados de eventos relacionados à segurança.

Agregação de dados na sua conta

O Security Lake cria um data lake de segurança específico na sua conta. O Security Lake de logs e de eventos a partir de fontes de dados da nuvem, on-premises e personalizadas em todas as contas e Regiões. O data lake é respaldado pelos buckets do Amazon Simple Storage Service (Amazon S3). Você é o proprietário dos seus dados.

Variedade de fontes de log e eventos compatíveis

O Security Lake coleta registros e eventos de segurança de várias fontes, incluindo serviços locais e de terceiros. Serviços da AWS Depois de ingerir os logs, independentemente da fonte, você pode acessá-los centralmente e gerenciar seu ciclo de vida. Para obter detalhes sobre as fontes de onde logs e eventos são coletados pelo Security Lake, consulte Gerenciamento de fontes no Security Lake

Transformação e normalização de dados

O Security Lake particiona automaticamente os dados recebidos de serviços da Serviços da AWS com suporte nativo e os converte para o formato Parquet, eficiente em termos de armazenamento e consulta. Ele também transforma dados do suporte nativo Serviços da AWS para o esquema de código aberto Open Cybersecurity Schema Framework (OCSF). Isso torna os dados compatíveis com outros fornecedores Serviços da AWS e fornecedores terceirizados sem a necessidade de pós-processamento. Como o Security Lake normaliza os dados, muitas soluções de segurança podem consumir esses dados em paralelo.

Vários níveis de acesso para assinantes

Assinantes consomem dados armazenados no Security Lake. Você pode escolher o nível de acesso de um assinante aos seus dados. Assim, eles podem consumir dados somente das fontes e nas Regiões da AWS que você especificar. Os assinantes podem ser notificados automaticamente sobre novos objetos à medida que são gravados no data lake. Eles também podem consultar dados do data lake. O Security Lake cria e troca automaticamente as credenciais necessárias entre o Security Lake e o assinante.

Gerenciamento de dados de várias contas e várias Regiões

Você pode ativar centralmente o Security Lake em todas as Regiões em que ele estiver disponível e em várias Contas da AWS. No Security Lake, também é possível designar Regiões cumulativas para consolidar logs de segurança e dados de eventos de várias Regiões. Isso pode ajudar você a cumprir os requisitos de conformidade de residência de dados.

Configurável e personalizável

O Security Lake é um serviço configurável e personalizável. É possível especificar para quais fontes, contas e Regiões você deseja configurar a coleta de logs. Você também pode especificar o nível de acesso de um assinante ao data lake.

Gerenciamento e otimização do ciclo de vida dos dados

O Security Lake gerencia o ciclo de vida de seus dados com configurações de retenção personalizáveis e custos de armazenamento com nivelamento automatizado. Ele automaticamente particiona e converte dados de segurança recebidos para o formato Parquet, eficiente em termos de armazenamento e consulta.

Como acessar o Security Lake

Para ver uma lista das Regiões em que o Security Lake está disponível atualmente, consulte Regiões e endpoints do Security Lake. Para saber mais sobre Regiões, consulte Endpoints de serviço da AWS no Referência geral da AWS.

Em cada Região, você pode acessar o Security Lake de qualquer uma das maneiras a seguir:

Console de gerenciamento da AWS

Console de gerenciamento da AWS É uma interface baseada em navegador que você pode usar para criar e gerenciar AWS recursos. O console do Security Lake fornece acesso à sua conta e aos recursos do serviço. Você pode realizar a maioria das tarefas usando o console.

API Security Lake

Para acessar o Security Lake programaticamente, use a API e emita solicitações HTTPS diretamente ao serviço. Para mais informações, consulte a Referência da API do Security Lake.

AWS Command Line Interface (AWS CLI)

Com o AWS CLI, você pode emitir comandos na linha de comando do seu sistema para realizar tarefas e AWS tarefas do Security Lake. Usar a linha de comando pode ser mais rápido e mais conveniente do que usar o console. As ferramentas da linha de comando também são úteis se você quiser criar scripts que realizem tarefas. Para obter informações sobre como instalar e usar o AWS CLI, consulte AWS Command Line Interfaceo.

AWS SDKs

AWS fornece SDKs bibliotecas e exemplos de código para várias linguagens e plataformas de programação, como Java, Go, Python, C++ e .NET. Eles SDKs fornecem acesso conveniente e programático ao Security Lake e outros Serviços da AWS. Eles também incluem tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter informações sobre como instalar e usar o AWS SDKs, consulte Ferramentas para construir AWS.

Serviços relacionados

A seguir estão outros Serviços da AWS que o Security Lake usa:

- Amazon EventBridge — O Security Lake é usado EventBridge para notificar os assinantes quando objetos são gravados no data lake.
- AWS Glue— O Security Lake usa AWS Glue rastreadores para criar as AWS Glue Data Catalog tabelas e enviar dados recém-gravados para o Catálogo de Dados. O Security Lake também armazena metadados de partição para AWS Lake Formation tabelas no Catálogo de Dados.
- AWS Lake Formation — O Security Lake cria uma tabela do Lake Formation separada para cada fonte que contribui com dados ao Security Lake. As tabelas do Lake Formation contêm informações sobre os dados de cada fonte, incluindo informações sobre esquema, partição e localização dos dados. Os assinantes têm a opção de consumir dados consultando as tabelas do Lake Formation.
- AWS Lambda — O Security Lake usa funções do Lambda para oferecer suporte a trabalhos de extração, transformação e carregamento (ETL) em dados brutos e para registrar partições para dados de fontes do AWS Glue.
- Amazon S3 — O Security Lake armazena seus dados como objetos do Amazon S3. As classes de armazenamento e as configurações de retenção são baseadas nas ofertas do Amazon S3. O Security Lake não é compatível com o Amazon S3 Select.
- Amazon Simple Queue Service — O Security Lake usa o Amazon SQS para permitir o processamento orientado por eventos e gerenciar notificações.

O Security Lake coleta dados de fontes personalizadas, além do seguinte: Serviços da AWS

- AWS CloudTrail eventos de gerenciamento e dados (S3, Lambda)
- Registros de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS)
- Logs de consulta do Amazon Route 53 Resolver
- AWS Security Hub CSPM descobertas
- Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF Registros v2

Para obter mais informações sobre essas fontes, consulte Coletando dados Serviços da AWS do Security Lake. Você pode consumir os objetos do Amazon S3 no seu data lake de segurança criando um assinante que possa ler dados no esquema do OCSF. Você também pode consultar dados usando o Amazon Athena, o Amazon Redshift e serviços de assinatura de terceiros que se integram com o. AWS Glue

Conceitos e terminologia

Esta seção descreve os principais conceitos e termos para ajudar você a usar o Amazon Security Lake.

Região contribuinte

Um ou mais Regiões da AWS que contribuem com dados para uma região cumulativa.

Data lake

Seus dados persistentes, armazenados no Amazon Simple Storage Service (Amazon S3) e gerenciados pelo Security Lake. O Security Lake usa AWS Glue para enviar dados recém-gravados para o Catálogo de Dados. O Security Lake também cria uma AWS Lake Formation tabela para cada fonte que contribui com dados para o data lake. Um data lake normalmente armazena o seguinte:

- Dados estruturados e não estruturados
- Dados brutos e transformados

O Security Lake é um serviço de data lake projetado para coletar logs e eventos relacionados à segurança.

Open Cybersecurity Schema Framework (OCSF)

Um esquema padronizado de código aberto para logs e eventos relacionados à segurança. Ele foi desenvolvido por AWS outros líderes do setor de segurança em vários domínios de segurança. O Security Lake converte automaticamente os registros e eventos que ele coleta Serviços da AWS no esquema OCSF. Fontes personalizadas convertem seus logs e eventos em OCSF antes de enviá-los para o Security Lake.

Região cumulativa

E Região da AWS que consolida registros e eventos de segurança de uma ou mais regiões contribuintes. A especificação de uma ou mais Regiões cumulativas pode ajudar você a cumprir os requisitos de conformidade regionais.

Origem

Um conjunto de logs e eventos gerados a partir de um único sistema correspondente a uma classe de evento específica no OCSF. O Security Lake pode coletar dados de uma fonte. Uma fonte pode ser outro AWS service (Serviço da AWS) ou um serviço de terceiros. Para fontes

terceirizadas, você deve converter os dados ao esquema do OCSF antes de enviá-los para o Security Lake.

Assinante

Um serviço que consome logs e eventos do Security Lake. Um assinante pode ser outro serviço AWS service (Serviço da AWS) ou um serviço de terceiros.

Conceitos básicos do Amazon Security Lake

Os tópicos desta seção explicam como ativar e começar a usar o Security Lake. Você aprenderá como definir suas configurações de data lake e configurar a coleta de registros. Você pode ativar e usar o Security Lake por meio do Console de gerenciamento da AWS ou programaticamente. Seja qual for o método usado, você deve primeiro configurar um Conta da AWS e um usuário administrativo. As etapas posteriores diferem com base no método de acesso.

O console do Security Lake oferece um processo simplificado para começar e cria todas as funções AWS Identity and Access Management (IAM) necessárias para criar seu data lake.

Se você acessar o Security Lake programaticamente, é necessário criar algumas funções AWS Identity and Access Management (IAM) para configurar seu data lake.

> **Important**
>
> O Security Lake não oferece suporte ao preenchimento de eventos de origem de log AWS bruta existentes que foram gerados antes da ativação do Security Lake.

Tópicos

Configurando seu Conta da AWS

Antes de habilitar o Amazon Security Lake, você deve ter um Conta da AWS. Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS Centro de Identidade do AWS IAM, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte Habilitar o Centro de Identidade do AWS IAM no Guia do usuário do Centro de Identidade do AWS IAM .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia Centro de Identidade do AWS IAM do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Identifique a conta que você usará para ativar o Security Lake

O Security Lake se integra AWS Organizations para gerenciar a coleta de registros em várias contas em uma organização. Se deseja usar o Security Lake em uma organização, a conta de gerenciamento do Organizations deve designar um administrador delegado do Security Lake. Em seguida, você deve usar as credenciais do administrador delegado para ativar o Security Lake, adicionar contas de membros e ativar o Security Lake para elas. Para obter mais informações, consulte Gerenciando várias contas com o AWS Organizations Security Lake.

Como alternativa, você pode usar o Security Lake sem a integração do Organizations para uma conta autônoma que não faz parte de uma organização.

Considerações ao ativar o Security Lake

Antes de habilitar o Security Lake, considere o seguinte:

- O Security Lake fornece recursos de gerenciamento entre regiões, o que significa que você pode criar seu data lake e configurar a coleta de registros nas Regiões da AWS. Para habilitar o Security Lake em todas as regiões suportadas, você pode escolher qualquer endpoint regional compatível. Você também pode adicionar Regiões de rollup para agregar dados de várias regiões em uma única região.
- Recomendamos habilitar o Security Lake em todas as Regiões da AWS suportadas. Se você fizer isso, o Security Lake poderá coletar dados conectados a atividades não autorizadas ou incomuns, mesmo em regiões que você não usa ativamente. Se o Security Lake não estiver ativado em todas as regiões suportadas, sua capacidade de coletar dados de outros serviços que você usa em várias regiões será reduzida.
- Quando você ativa o Security Lake pela primeira vez em qualquer região, ele cria as seguintes funções vinculadas ao serviço para sua conta:
  - AWSServiceRoleForSecurityLake: essa função inclui as permissões para ligar para outras Serviços da AWS pessoas em seu nome e operar o data lake de segurança. Se você habilitar o Security Lake como administrador delegado do Security Lake, o Security Lake criará a função vinculada a serviços em cada conta membro da organização.
  - AWSServiceRoleForSecurityLakeResourceManagement: O Security Lake usa essa função para realizar melhorias contínuas de monitoramento e desempenho, o que pode reduzir potencialmente a latência e os custos. Essa função vinculada a serviços confia no serviço `resource-management.securitylake.amazonaws.com` para assumir a função. Habilitar essa função de serviço também concederá a ela acesso ao Lake Formation.

    Para obter informações sobre como isso afeta as contas existentes que ativaram o Security Lake antes de 17 de abril de 2025, consulteUpdate for existing accounts.

  Para obter informações sobre como as funções vinculadas ao serviço funcionam, consulte Como usar permissões de funções vinculadas ao serviço no Guia do usuário do IAM.
- O Security Lake não oferece suporte ao bloqueio de objetos do Amazon S3. Quando os buckets do data lake são criados, o bloqueio de objetos do S3 é desabilitado por padrão. Habilitar o bloqueio de objetos em um bucket interrompe a entrega de dados de log normalizados para o data lake.

- Se você estiver reativando o Security Lake em uma região, deverá excluir o AWS Glue banco de dados correspondente da região do seu uso anterior do Security Lake.

Ativando o Security Lake usando o console

Este tutorial explica como habilitar e configurar o Security Lake por meio do Console de gerenciamento da AWS. Como parte do Console de gerenciamento da AWS, o console do Security Lake oferece um processo simplificado para começar e cria todas as funções AWS Identity and Access Management (IAM) necessárias para criar seu data lake.

Etapa 1: Configurar fontes

O Security Lake coleta dados de logs e de eventos de várias fontes e de todas as suas Contas da AWS e Regiões da AWS. Siga estas instruções para identificar quais dados você deseja que o Security Lake colete. Você só pode usar essas instruções para adicionar um AWS service (Serviço da AWS) com suporte nativo como fonte. Para obter mais informações sobre como adicionar uma fonte personalizada, consulte Coletando dados de fontes personalizadas no Security Lake.

Para configurar a coleta de fontes de log

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione uma região. Você pode habilitar o Security Lake na região atual e em outras regiões durante a integração.
3. Escolha Começar.
4. Em Selecionar fontes de registro e eventos, escolha uma das seguintes opções para Seleção de origem:

    a. AWS Fontes padrão de ingestão — Quando você escolhe a opção recomendada, CloudTrail - eventos de dados do S3 e não AWS WAF são incluídos para ingestão por padrão. Isso ocorre porque a ingestão de alto volume de ambos os tipos de fonte pode afetar significativamente os custos de uso. Para ingerir essas fontes, primeiro selecione a opção Ingerir AWS fontes específicas e, em seguida, selecione essas fontes na lista Fontes de registros e eventos.

    b. Ingerir AWS fontes específicas — Com essa opção, você pode selecionar uma ou mais fontes de registro e eventos que deseja ingerir.

> **Note**
>
> Quando você habilita o Security Lake em uma conta pela primeira vez, todas as origens de log e eventos selecionadas farão parte de um período de teste gratuito de 15 dias. Para saber mais sobre estatísticas de uso, consulte Como analisar o uso e os custos estimados.

5. Em Versões, escolha a versão da fonte de dados da qual você deseja ingerir fontes de registro e eventos. Para obter mais informações sobre versões, consulte Identificação da fonte do OCSF.

> **Important**
>
> Se você não tiver as permissões de função necessárias para habilitar a nova versão da fonte de AWS log na região especificada, entre em contato com o administrador do Security Lake. Para obter mais informações, consulte Atualizar permissões de função.

6. Em Selecionar regiões, escolha se deseja ingerir fontes de logs e eventos de todas as regiões suportadas ou regiões específicas. Se você escolher Regiões específicas, selecione de quais regiões ingerir dados.
7. Para selecionar contas, execute as seguintes etapas:

    1. Escolha se o Security Lake ingerirá dados de todas as contas ou contas específicas em sua organização. O Security Lake será ativado para essas contas com as configurações que você escolher durante essa configuração.
    2. A caixa de seleção Ativar automaticamente o Security Lake para novas contas da organização está marcada por padrão. Essas configurações de ativação automática serão aplicadas Contas da AWS quando eles ingressarem na sua organização. Você pode editar as configurações de ativação automática a qualquer momento.

    > **Note**
    >
    > As configurações de ativação automática só se aplicarão às contas quando elas ingressarem na sua organização, não às contas existentes. Para obter mais informações, consulte Editando a configuração da nova conta no console.

8. Para Acesso ao serviço, crie um novo perfil do IAM ou use um perfil do IAM existente que dê permissão ao Security Lake para coletar dados de suas fontes e adicioná-los ao seu data lake. Uma função é usada em todas as regiões nas quais você habilitar o Security Lake.
9. Escolha Próximo.

Etapa 2: definir configurações de armazenamento e regiões cumulativas (opcional)

Você pode especificar a classe de armazenamento do Amazon S3 na qual deseja que o Security Lake armazene seus dados e por quanto tempo. Você também pode especificar uma região de rollup para consolidar dados de várias regiões. Essas são etapas opcionais. Para obter mais informações, consulte Gerenciamento do ciclo de vida no Security Lake.

Para definir as configurações de armazenamento e de rollup

1. Se você quiser consolidar dados de várias regiões contribuintes em uma região de rollup, em Selecionar regiões de rollup, escolha Adicionar região de rollup. Especifique a região de rollup e as regiões que contribuirão com ela. Você pode configurar uma ou mais regiões de rollup.
2. Em Selecionar classes de armazenamento, escolha uma classe de armazenamento do Amazon S3. A classe de armazenamento padrão é S3 Standard. Forneça um período de retenção (em dias) se quiser que os dados sejam transferidos para outra classe de armazenamento após esse período e escolha Adicionar transição. Após o término desse período de retenção, os objetos expiram e o Amazon S3 os exclui. Para obter mais informações sobre classes de armazenamento e retenção do Amazon S3, consulte Gerenciamento de retenção.
3. Se você selecionou uma região de rollup na primeira etapa, para Acesso ao serviço, crie um novo perfil do IAM ou use um perfil do IAM existente que dê permissão ao Security Lake para replicar dados em várias regiões.
4. Escolha Próximo.

Etapa 3: revisar e criar um data lake

Analise as fontes das quais o Security Lake coletará dados, suas regiões de rollup e suas configurações de retenção. Em seguida, crie seu data lake.

Para revisar e criar o data lake

1. Ao habilitar o Security Lake, revise Fontes de logs e eventos, Regiões, Regiões de rollup e Classes de armazenamento.
2. Escolha Criar.

Depois de criar seu data lake, você verá a página Resumo no console do Security Lake. Esta página fornece uma visão geral do número de regiões e regiões cumulativas, informações sobre assinantes e problemas.

O menu Problemas mostra um resumo dos problemas dos últimos 14 dias que estão afetando o serviço Security Lake ou seus buckets do Amazon S3. Para obter detalhes adicionais sobre cada problema, acesse a página Problemas do console do Security Lake.

Etapa 4: visualizar e consultar seus próprios dados

Depois de criar seu data lake, você pode usar o Amazon Athena ou serviços similares para visualizar e consultar seus dados em AWS Lake Formation bancos de dados e tabelas. Quando você usa o console, o Security Lake concede automaticamente permissões de visualização do banco de dados ao perfil que você usa para habilitar o Security Lake. No mínimo, a função deve ter permissões de Analista de dados. Para obter mais informações sobre os níveis de permissão, consulte Referência de permissões do IAM e personas do Lake Formation. Para obter instruções sobre como conceder permissões `SELECT`, consulte Como conceder permissões no catálogo de dados usando o método de recurso nomeado no Guia do desenvolvedor do AWS Lake Formation .

Etapa 5: criar assinantes

Depois de criar seu data lake, você pode adicionar assinantes para consumir seus dados. Os assinantes podem consumir dados acessando diretamente os objetos nos seus buckets do Amazon S3 ou consultando o data lake. Para obter mais informações sobre assinantes, consulte Gerenciamento de assinantes no Security Lake.

Ativando o Security Lake programaticamente

Este tutorial explica como ativar e começar a usar o Security Lake programaticamente. A API do Amazon Security Lake oferece acesso abrangente e programático à sua conta, dados e recursos do Security Lake. Como alternativa, você pode usar ferramentas de linha de AWS comando — AWS

Command Line Interfaceou as AWS Ferramentas para PowerShell — ou a AWS SDKspara acessar o Security Lake.

Etapa 1: criar funções do IAM

Se você acessar o Security Lake programaticamente, é necessário criar algumas funções AWS Identity and Access Management (IAM) para configurar seu data lake.

> **Important**
>
> Não é necessário criar essas funções do IAM se você usar o console do Security Lake para habilitar e configurar o Security Lake.

Crie funções no IAM se você estiver realizando uma ou mais dessas ações (escolha os links para ver mais informações sobre os perfis do IAM para cada ação):

- Como criar uma fonte personalizada: fontes personalizadas são fontes sem suporte nativo nos Serviços da AWS que enviam dados para o Security Lake.
- Como criar um assinante com acesso a dados: os assinantes com permissões podem acessar diretamente os objetos do S3 do seu data lake.
- Como criar um assinante com acesso de consulta: assinantes com permissões podem consultar dados do Security Lake usando serviços como o Amazon Athena.
- Como configurar uma região de rollup: uma região de rollup consolida dados de várias Regiões da AWS.

Depois de criar as funções mencionadas anteriormente, anexe a política AmazonSecurityLakeAdministrator AWS gerenciada à função que você está usando para ativar o Security Lake. Essa política concede permissões administrativas que permitem à entidade principal acesso ao Security Lake e acesso total a todas as ações do Security Lake.

Anexe a política AmazonSecurityLakeMetaStoreManager AWS gerenciada para criar seu data lake ou consultar dados do Security Lake. Essa política é necessária para que o Security Lake ofereça suporte a trabalhos de extração, transformação e carregamento (ETL) em dados brutos de log e eventos recebidos das fontes.

Etapa 2: habilitar o Amazon Security Lake

Para habilitar o Security Lake programaticamente, use a CreateDataLakeoperação da API do Security Lake. Se você estiver usando o AWS CLI, execute o create-data-lakecomando. Em sua solicitação, use o campo `region` do objeto `configurations` para especificar o código da região na qual o Security Lake será habilitado. Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.

Exemplo 1

O comando de exemplo a seguir ativa o Security Lake nas `us-east-2` regiões `us-east-1` e. Em ambas as regiões, esse data lake é criptografado com chaves gerenciadas do Amazon S3. Os objetos expiram após 365 dias, e os objetos fazem a transição para a classe de armazenamento `ONEZONE_IA` S3 após 60 dias. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ 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"
```

Exemplo 2

O comando de exemplo a seguir ativa o Security Lake na `us-east-2` região. Esse data lake é criptografado com uma chave gerenciada pelo cliente que foi criada em AWS Key Management Service (AWS KMS). Os objetos expiram após 500 dias, e os objetos fazem a transição para a classe de armazenamento `GLACIER` S3 após 30 dias. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ 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**
>
> Se você já habilitou o Security Lake e deseja atualizar as configurações de uma região ou fonte, use a UpdateDataLakeoperação ou, se estiver usando o AWS CLI, o update-data-lakecomando. Não use a `CreateDataLake` operação.

Etapa 3: Configurar fontes

O Security Lake coleta dados de logs e de eventos de várias fontes e de todas as suas Contas da AWS e Regiões da AWS. Siga estas instruções para identificar quais dados você deseja que o Security Lake colete. Você só pode usar essas instruções para adicionar um AWS service (Serviço da AWS) com suporte nativo como fonte. Para obter mais informações sobre como adicionar uma fonte personalizada, consulte Coletando dados de fontes personalizadas no Security Lake.

Para definir uma ou mais fontes de coleta programaticamente, use a CreateAwsLogSourceoperação da API Security Lake. Para cada fonte, especifique um valor regionalmente exclusivo para o parâmetro `sourceName`. Opcionalmente, use parâmetros adicionais para limitar o escopo da fonte a contas específicas (`accounts`) ou a uma versão específica (`sourceVersion`).

> **Note**
>
> Se você não incluir um parâmetro opcional em sua solicitação, o Security Lake aplicará sua solicitação a todas as contas ou a todas as versões da fonte especificada, dependendo do parâmetro que você excluir. Por exemplo, se você for o administrador delegado do Security Lake de uma organização e excluir o parâmetro `accounts`, o Security Lake aplicará sua solicitação a todas as contas da sua organização. Da mesma forma, se você excluir o parâmetro `sourceVersion`, o Security Lake aplicará sua solicitação a todas as versões da fonte especificada.

Se sua solicitação especificar uma região na qual você não habilitou o Security Lake, ocorrerá um erro. Para resolver esse erro, certifique-se de que a matriz `regions` especifique somente as regiões nas quais você habilitou o Security Lake. Como alternativa, você pode habilitar o Security Lake na região e enviar sua solicitação novamente.

Quando você habilita o Security Lake em uma conta pela primeira vez, todas as origens de log e eventos selecionadas farão parte de um período de teste gratuito de 15 dias. Para saber mais sobre estatísticas de uso, consulte Como analisar o uso e os custos estimados.

Etapa 4: definir as configurações de armazenamento e as regiões cumulativas (opcional)

Você pode especificar a classe de armazenamento do Amazon S3 na qual deseja que o Security Lake armazene seus dados e por quanto tempo. Você também pode especificar uma região de rollup para consolidar dados de várias regiões. Essas são etapas opcionais. Para obter mais informações, consulte Gerenciamento do ciclo de vida no Security Lake.

Para definir um objetivo alvo programaticamente ao ativar o Security Lake, use a CreateDataLakeoperação da API do Security Lake. Se você já habilitou o Security Lake e deseja definir um objetivo alvo, use a UpdateDataLakeoperação, não a `CreateDataLake` operação.

Para qualquer operação, use os parâmetros suportados para especificar as configurações desejadas:

- Para especificar uma região cumulativa, use o `region` campo para especificar a região na qual você deseja contribuir com dados para as regiões cumulativas. Na `regions` matriz do `replicationConfiguration` objeto, especifique o código da região para cada região de rollup. Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.
- Para especificar as configurações de retenção dos seus dados, use os parâmetros `lifecycleConfiguration`:
  - Para `transitions`, especifique o número total de dias (`days`) pelo qual você deseja armazenar objetos do S3 em uma determinada classe de armazenamento do Amazon S3 (`storageClass`).
  - Para `expiration`, especifique o número total de dias pelo qual você deseja armazenar objetos no Amazon S3, usando qualquer classe de armazenamento, após a criação dos objetos. Quando esse período de retenção termina, os objetos expiram e o Amazon S3 os exclui.

  O Security Lake aplica as configurações de retenção especificadas à Região que você especifica no campo `region` do objeto `configurations`.

Por exemplo, o comando a seguir cria um data lake com `ap-northeast-2` uma região cumulativa. A `us-east-1` Região contribuirá com dados para a `ap-northeast-2` Região. Esse exemplo também estabelece um período de expiração de 10 dias para objetos adicionados ao data lake.

```
$ 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"
```

Agora você criou seu data lake. Use a ListDataLakesoperação da API Security Lake para verificar a ativação do Security Lake e suas configurações de data lake em cada região.

Se surgirem problemas ou erros na criação do seu data lake, você poderá visualizar uma lista de exceções usando a ListDataLakeExceptionsoperação e notificar os usuários sobre exceções com a CreateDataLakeExceptionSubscriptionoperação. Para obter mais informações, consulte Solução de problemas do status do data lake.

Etapa 5: visualizar e consultar seus próprios dados

Depois de criar seu data lake, você pode usar o Amazon Athena ou serviços similares para visualizar e consultar seus dados em AWS Lake Formation bancos de dados e tabelas. Quando você ativa programaticamente o Security Lake, as permissões de visualização do banco de dados não são concedidas automaticamente. A conta de administrador do data lake AWS Lake Formation deve conceder `SELECT` permissões para a função do IAM que você deseja usar para consultar os bancos de dados e tabelas relevantes. No mínimo, a função deve ter permissões de Analista de dados. Para obter mais informações sobre os níveis de permissão, consulte Referência de permissões do IAM e personas do Lake Formation. Para obter instruções sobre como conceder permissões `SELECT`, consulte Como conceder permissões no catálogo de dados usando o método de recurso nomeado no Guia do desenvolvedor do AWS Lake Formation .

Etapa 6: criar assinantes

Depois de criar seu data lake, você pode adicionar assinantes para consumir seus dados. Os assinantes podem consumir dados acessando diretamente os objetos nos seus buckets do Amazon S3 ou consultando o data lake. Para obter mais informações sobre assinantes, consulte Gerenciamento de assinantes no Security Lake.

Gerenciando várias contas com o AWS Organizations Security Lake

Você pode usar o Amazon Security Lake para coletar registros e eventos de segurança de várias Contas da AWS. Para ajudar a automatizar e simplificar o gerenciamento de várias contas, é altamente recomendável que você integre o Security Lake com o AWS Organizations.

Em Organizações, a conta que você usa para criar a organização é chamada conta de gerenciamento. Para integrar o Security Lake com o Organizations, a conta de gerenciamento deve designar uma conta delegada de administrador do Security Lake para a organização.

O administrador delegado do Security Lake pode ativar o Security Lake e definir as configurações do Security Lake para as contas-membro. O administrador delegado pode coletar registros e eventos em toda a organização em todos os Regiões da AWS lugares onde o Security Lake está ativado (independentemente do endpoint regional que ele esteja usando atualmente). O administrador delegado também pode configurar o Security Lake para coletar automaticamente dados de log e eventos para novas contas da organização.

O administrador delegado do Security Lake tem acesso ao log e dados de eventos das contas-membros associadas. Assim, eles podem configurar o Security Lake para coletar dados pertencentes às contas-membro associadas. Eles também podem conceder aos assinantes permissão para consumir dados pertencentes às contas-membro associadas.

Para habilitar o Security Lake para várias contas em uma organização, a conta de gerenciamento da organização deve primeiro designar uma conta delegada de administrador do Security Lake para a organização. O administrador delegado pode então ativar e configurar o Security Lake para a organização.

> **Important**
>
> Use a RegisterDataLakeDelegatedAdministratorAPI do Security Lake para permitir que o Security Lake acesse sua organização e registre o administrador delegado da organização. Se você usar 'Organizations' APIs para registrar um administrador delegado, as funções vinculadas ao serviço das Organizations podem não ser criadas com êxito. Para garantir a funcionalidade total, use o Security Lake APIs.

Para obter mais informações sobre como configurar organizações, consulte Criar e gerenciar uma organização no Guia do usuário do AWS Organizations.

> **Para contas existentes do Security Lake**
>
> Se você ativou o Security Lake antes de 17 de abril de 2025, recomendamos que você habilite Permissões de função vinculada ao serviço (SLR) para gerenciamento de recursos o. Ao usar essa SLR, você pode continuar realizando melhorias contínuas de monitoramento e desempenho, o que pode reduzir potencialmente a latência e os custos. Para obter informações sobre as permissões associadas a essa SLR, consultePermissões de função vinculada ao serviço (SLR) para gerenciamento de recursos.
> Se você usa o console Security Lake, você receberá uma notificação solicitando que você habilite o. AWSServiceRoleForSecurityLakeResourceManagement Se você usa AWS CLI, consulte Criação da função vinculada ao serviço Security Lake.

Considerações importantes para administradores delegados do Security Lake

Observe os seguintes fatores que definem como um administrador delegado se comporta no Security Lake:

O administrador delegado é o mesmo em todas as regiões.

Quando você cria o administrador delegado, ele se torna o administrador delegado de cada região na qual você ativa o Security Lake.

Recomendamos definir a conta Log Archive como administrador delegado do Security Lake.

A conta Log Archive é dedicada à ingestão e arquivamento de todos os registros relacionados à segurança.Conta da AWS O acesso a essa conta geralmente é limitado a alguns usuários, como auditores e equipes de segurança para investigações de conformidade. Recomendamos definir a conta Log Archive como administrador delegado do Security Lake para que você possa visualizar logs e eventos relacionados à segurança com o mínimo de alternância de contexto.

Além disso, recomendamos que apenas um conjunto mínimo de usuários tenha acesso direto à conta Log Archive. Fora desse grupo seleto, se um usuário precisar acessar os dados que o Security Lake coleta, você poderá adicioná-lo como assinante do Security Lake. Para obter

mais informações sobre como adicionar um assinante, consulte Gerenciamento de assinantes no Security Lake.

Se você não usa o AWS Control Tower serviço, talvez não tenha uma conta do Log Archive. Para obter mais informações sobre a conta Log Archive, consulte Security OU — Conta Log Archive na Arquitetura de referência de segurança da AWS.

Uma organização pode ter apenas um administrador delegado.

Você pode ter somente um administrador delegado do Security Lake para cada organização.

A conta de gerenciamento da organização não pode ser o administrador delegado.

Com base nas melhores práticas de AWS segurança e no princípio do menor privilégio, a conta de gerenciamento da sua organização não pode ser o administrador delegado.

O administrador delegado deve fazer parte de uma organização ativa.

Quando você exclui uma organização, a conta de administrador delegado não pode mais gerenciar o Security Lake. Você deve designar um administrador delegado de uma organização diferente ou usar o Security Lake com uma conta independente que não faça parte de uma organização.

Permissões do IAM necessárias para designar um administrador delegado

Ao designar o administrador delegado do Security Lake, você deve ter permissões para habilitar o Security Lake e usar determinadas operações de AWS Organizations API listadas na declaração de política a seguir.

Você pode adicionar a seguinte declaração ao final de uma política AWS Identity and Access Management(IAM) para conceder essas permissões.

```
{
    "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": "*"
}
```

Com designar o administrador delegado do Security Lake e adicionar contas de membros

Escolha seu método de acesso para designar uma conta de administrador do delegada do Security Lake para a sua organização. Somente a conta de gerenciamento da organização pode designar a conta do administrador delegado para sua organização. A conta de gerenciamento da organização não pode ser a conta do administrador delegado da própria organização.

> **Note**
>
> - A conta de gerenciamento da organização deve usar a operação `RegisterDataLakeDelegatedAdministrator` do Security Lake para designar a conta delegada do administrador do Security Lake. Não há suporte para designar o administrador delegado do Security Lake por meio do Organizations.
> - Se você quiser alterar o administrador delegado da organização, primeiro remova o administrador delegado atual. Em seguida, você pode designar um novo administrador delegado.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login usando as credenciais da conta de gerenciamento da sua organização.

2. - Se o Security Lake ainda não estiver ativado, selecione Começar e, em seguida, designe o administrador delegado do Security Lake na página Ativar Security Lake.
   - Se o Security Lake já estiver ativado, designe o administrador delegado do Security Lake na página Configurações.

3. Em Delegar administração para outra conta, insira o Conta da AWS ID de 12 dígitos da sua conta do Log Archive.

   Recomendamos usar o Log Archive como administrador delegado do Security Lake. Para obter mais informações, consulte Considerações importantes para administradores delegados do Security Lake.
4. Selecione Delegar. Se o Security Lake ainda não estiver habilitado, designar um administrador delegado habilitará o Security Lake para essa conta na região atual.

API

Para designar programaticamente o administrador delegado, use a RegisterDataLakeDelegatedAdministratoroperação da API Security Lake. Você deve invocar a operação a partir da conta de gerenciamento da organização. Se você estiver usando o AWS CLI, execute o register-data-lake-delegated-administratorcomando na conta de gerenciamento da organização. Em sua solicitação, use o `accountId` parâmetro para especificar o ID da conta de 12 dígitos do Conta da AWS para designar como a conta de administrador delegado da organização.

Por exemplo, o AWS CLI comando a seguir designa o administrador delegado. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

O administrador delegado também pode optar por automatizar a coleta de dados de logs e eventos da AWS de novas contas da organização. Com essa configuração, o Security Lake é habilitado automaticamente em novas contas quando as contas são adicionadas à organização em AWS Organizations. Como administrador delegado, você pode habilitar essa configuração usando a CreateDataLakeOrganizationConfigurationoperação da API Security Lake ou, se estiver usando a AWS CLI, executando create-data-lake-organization-configurationo comando. Em sua solicitação, você também pode especificar determinadas configurações para novas contas.

Por exemplo, o AWS CLI comando a seguir ativa automaticamente o Security Lake e a coleta de registros de consulta,AWS Security Hub CSPM descobertas e registros de fluxo da Amazon Virtual Private Cloud (Amazon VPC) do resolvedor do Amazon Route 53 em novas contas da

organização. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

Após a conta de gerenciamento da organização designar o administrador delegado, o administrador pode ativar e configurar o Security Lake para a organização. Isso inclui habilitar e configurar o Security Lake para coletar dados de AWS registros e eventos para contas individuais na organização. Para obter mais informações, consulte Coletando dados Serviços da AWS do Security Lake.

Você pode usar a GetDataLakeOrganizationConfigurationoperação para obter detalhes sobre a configuração atual da sua organização para novas contas de membros.

Editando a configuração de ativação automática para novas contas da organização

Um administrador delegado do Security Lake pode visualizar e editar as configurações de ativação automática das contas quando elas ingressam na sua organização. O Security Lake ingere dados com base nessas configurações somente para novas contas, não para contas existentes.

Use as etapas a seguir para editar a configuração das novas contas da organização:

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, selecione Contas.
3. Na página Contas, expanda a seção Nova configuração de conta. Você pode ver quais fontes o Security Lake ingere de cada região.
4. Escolha Editar para editar essa configuração.
5. Na página Editar nova configuração da conta, execute as seguintes etapas:
    a. Em Selecionar regiões, selecione uma ou mais regiões para as quais você deseja atualizar as fontes das quais ingerir os dados. Em seguida, escolha Próximo.
    b. Em Selecionar fontes, escolha uma das seguintes opções para Seleção de origem:

i. AWS Fontes padrão de ingestão — Quando você escolhe a opção recomendada, CloudTrail - eventos de dados do S3 e não AWS WAF são incluídos para ingestão por padrão. Isso ocorre porque a ingestão de alto volume de ambos os tipos de fonte pode afetar significativamente os custos de uso. Para ingerir essas fontes, primeiro selecione a opção Ingerir AWS fontes específicas e, em seguida, selecione essas fontes na lista Fontes de registros e eventos.

ii. Ingerir AWS fontes específicas — Com essa opção, você pode selecionar uma ou mais fontes de registro e eventos que deseja ingerir.

iii. Não ingerir nenhuma fonte — Selecione essa opção quando não quiser ingerir nenhuma fonte das regiões que você selecionou na etapa anterior.

iv. Escolha Próximo.

> **Note**
>
> Quando você habilita o Security Lake em uma conta pela primeira vez, todas as origens de log e eventos selecionadas farão parte de um período de teste gratuito de 15 dias. Para saber mais sobre estatísticas de uso, consulte Como analisar o uso e os custos estimados.

c. Depois de revisar as alterações, escolha Aplicar.

Quando um homem Conta da AWS se junta à sua organização, essas configurações se aplicam a essa conta por padrão.

Como remover o administrador delegado do Security Lake

Apenas a conta de gerenciamento da organização pode remover o administrador delegado do Security Lake da organização. Se desejar alterar o administrador delegado da organização, remova o administrador delegado atual e, em seguida, designe o novo administrador delegado.

> **Important**
>
> A remoção do administrador delegado do Security Lake exclui seu data lake e desativa o Security Lake para as contas da sua organização.

Não é possível alterar ou remover o administrador delegado usando o console do Security Lake. Essas tarefas só podem ser executadas por programação.

Para remover programaticamente o administrador delegado, use a DeregisterDataLakeDelegatedAdministratoroperação da API Security Lake. Você deve invocar a operação a partir da conta de gerenciamento da organização. O Se você estiver usando o AWS CLI, execute o deregister-data-lake-delegated-administratorcomando na conta de gerenciamento da organização.

Por exemplo, o AWS CLI comando a seguir remove o administrador delegado do Security Lake.

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

Para manter a designação de administrador delegado, mas alterar as configurações automáticas das novas contas de membros, use a DeleteDataLakeOrganizationConfigurationoperação da API Security Lake ou, se estiver usando o AWS CLI, o delete-data-lake-organization-configurationcomando. Somente o administrador delegado pode alterar essas configurações para a organização.

Por exemplo, o AWS CLI comando a seguir interrompe a coleta automática de descobertas de CSPM do Security Hub de novas contas membros que ingressam na organização. Novas contas de membros não contribuirão com as descobertas do CSPM do Security Hub para o data lake depois que o administrador delegado invocar essa operação. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

Acesso confiável do Security Lake

Depois de configurar o Security Lake para uma organização, a conta AWS Organizations de gerenciamento pode habilitar o acesso confiável com o Security Lake. O acesso confiável permite que o Security Lake crie uma função vinculada a serviços do IAM e execute tarefas na organização e nas contas em seu nome. Para obter mais informações, consulte Usar o AWS Organizations com outro Serviços da AWS no Guia do usuário do AWS Organizations.

Como usuário da conta de gerenciamento da organização, você pode desativar o acesso confiável para o Security Lake no AWS Organizations. Para obter instruções sobre como desativar o acesso confiável, consulte Como ativar ou desativar o acesso confiável no Guia do usuário do AWS Organizations.

Recomendamos desativar o acesso confiável se o do administrador delegado Conta da AWS estiver suspenso, isolado ou fechado.

Gerenciando regiões no Security Lake

O Amazon Security Lake pode coletar registros e eventos de segurança Regiões da AWS nos quais você habilitou o serviço. Para cada região, seus dados são armazenados em um bucket do Amazon S3 diferente. Você pode especificar diferentes configurações de data lake (por exemplo, diferentes fontes e configurações de retenção) para diferentes regiões. Você também pode definir uma ou mais regiões de rollup para consolidar dados de várias regiões.

Verificação do status da região

O Security Lake pode coletar dados em várias Regiões da AWS. Para monitorar o estado do seu data lake, pode ser útil entender como cada região está configurada atualmente. Escolha seu método de acesso preferido e siga estas etapas para obter o status atual de uma região.

Console

Para verificar o status da região

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, escolha Regiões. A página Regiões é exibida, fornecendo uma visão geral das regiões nas quais o Security Lake está atualmente ativado.
3. Selecione uma região e escolha Editar para ver os detalhes dessa região.

API

Para obter o status da coleta de registros na região atual, use a GetDataLakeSourcesoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o get-data-lake-sourcescomando. Para o `accounts` parâmetro, especifique um ou mais Conta da AWS IDs como uma lista. Se sua solicitação for bem-sucedida, o Security Lake retornará um instantâneo dessas contas na região atual, incluindo de quais AWS fontes o Security Lake está coletando dados e o status de cada fonte. Se você não incluir o `accounts` parâmetro, a resposta incluirá o status da coleta de registros para todas as contas nas quais o Security Lake está configurado na região atual.

Por exemplo, o AWS CLI comando a seguir recupera o status da coleta de registros para as contas especificadas na região atual. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

O AWS CLI comando a seguir lista o status da coleta de registros para todas as contas e fontes habilitadas na região especificada. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

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

Para determinar se você ativou o Security Lake para uma região, use a ListDataLakesoperação. Se você estiver usando o AWS CLI, execute o list-data-lakescomando. Para o parâmetro `regions`, especifique o código da região: por exemplo, `us-east-1` para a região Leste dos EUA (Norte da Virgínia). Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS. A operação `ListDataLakes` retorna as configurações do data lake para cada região que você especifica em sua solicitação. Se você não especificar uma região, o Security Lake retornará o status e as configurações do seu data lake em cada região em que o Security Lake está disponível.

Por exemplo, o AWS CLI comando a seguir mostra o status e as configurações do seu data lake na `eu-central-1` região. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

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

Alterando as configurações da região

Escolha seu método preferido e siga estas instruções para atualizar as configurações do seu data lake em uma ou mais Regiões da AWS.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, escolha Regiões.
3. Selecione uma região e escolha Editar.

4. Marque a caixa de seleção Substituir fontes para todas as contas na <Region> para confirmar se suas seleções aqui substituem as seleções anteriores para esta região.
5. Em Selecionar classes de armazenamento, escolha Adicionar transição para adicionar novas classes de armazenamento aos seus dados.
6. Para Tags, opcionalmente atribua ou edite as tags para a Região. Uma tag é um rótulo que você pode definir e atribuir a determinados tipos de AWS recursos, incluindo a configuração do data lake para você Conta da AWS em uma região específica. Para saber mais, consulte Marcando recursos do Security Lake.
7. Para transformar uma região em uma região de rollup, escolha Regiões de rollup (em Configurações) no painel de navegação. Em seguida, escolha Modificar. Na seção Selecionar regiões de rollup, escolha Adicionar região de rollup. Selecione as regiões contribuintes e forneça permissão ao Security Lake para replicar dados em várias regiões. Quando terminar, escolha Salvar para salvar as alterações.

API

Para atualizar programaticamente as configurações de região do seu data lake, use a UpdateDataLakeoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o update-data-lakecomando. Para o parâmetro `region`, especifique o código da região para a qual deseja alterar as configurações: por exemplo, `us-east-1` para a região Leste dos EUA (Norte da Virgínia). Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.

Use parâmetros adicionais para especificar um novo valor para cada configuração que você deseja alterar, por exemplo, a chave de criptografia (`encryptionConfiguration`) e as configurações de retenção (`lifecycleConfiguration`).

Por exemplo, o AWS CLI comando a seguir atualiza as configurações de expiração de dados e transição da classe de armazenamento para a `us-east-1` região. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

Configurando regiões cumulativas no Security Lake

Uma região de rollup consolida dados de uma ou mais regiões contribuintes. Especificar uma região de rollup pode ajudá-lo a cumprir os requisitos de conformidade regionais.

Devido às limitações do Amazon S3, a replicação do data lake regional criptografado com chave gerenciada pelo cliente (CMK) para o data lake regional criptografado (criptografia padrão) gerenciado pelo S3 não é suportada.

> **Important**
>
> Se você criou uma fonte personalizada, para garantir que os dados da fonte personalizada sejam replicados adequadamente no destino, o Security Lake recomenda seguir as melhores práticas descritas em Práticas recomendadas para ingestão de fontes personalizadas. A replicação não pode ser executada em dados que não seguem o formato do caminho de dados da partição S3, conforme descrito na página.

Antes de adicionar uma região de rollup, primeiro você precisa criar dois perfis diferentes no AWS Identity and Access Management (IAM):

- Perfil do IAM para replicação de dados
- Função do IAM para registrar AWS Glue partições

> **Note**
>
> O Security Lake cria esses perfis do IAM ou usa os perfis existentes em seu nome quando você usa o console do Security Lake. No entanto, você deve criar essas funções ao usar a API Security Lake ou AWS CLI.

Perfil do IAM para replicação de dados

Esse perfil do IAM concede permissão ao Amazon S3 para replicar logs e eventos de fonte em várias regiões.

Para conceder essas permissões, crie um perfil do IAM que comece com o prefixo `SecurityLake` e anexe à função o seguinte exemplo de política. Você precisará do nome do recurso da Amazon

(ARN) da função ao criar uma região de rollup no Security Lake. Nesta política, `sourceRegions` são regiões contribuintes e `destinationRegions` são regiões de rollup.

JSON

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

```
        "arn:aws:s3:::aws-security-data-lake-[[destinationRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    }
  ]
}
```

Anexe a política de confiança a seguir à função para permitir que o Amazon S3 assuma a função:

JSON

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

Se você usar uma chave gerenciada pelo cliente de AWS Key Management Service (AWS KMS) para criptografar seu data lake do Security Lake, deverá conceder as seguintes permissões, além das permissões na política de replicação de dados.

```
{
    "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 obter mais informações sobre funções de replicação, consulte Configuração de permissões no Guia do usuário do Amazon Simple Storage Service.

Função do IAM para registrar AWS Glue partições

Essa função do IAM concede permissões para uma AWS Lambda função atualizadora de partições usada pelo Security Lake para registrar AWS Glue partições para os objetos do S3 que foram replicados de outras regiões. Sem criar essa função, os assinantes não podem consultar eventos desses objetos.

Para conceder essas permissões, crie uma função chamada `AmazonSecurityLakeMetaStoreManager` (talvez você já tenha criado essa função na integração ao Security Lake). Para obter mais informações sobre essa função, incluindo um exemplo de política, consulte Etapa 1: criar funções do IAM.

No console do Lake Formation, você também deve conceder permissões `AmazonSecurityLakeMetaStoreManager` como administrador do data lake seguindo estas etapas:

1. Abra o console do Lake Formation em https://console.aws.amazon.com/lakeformation/.
2. Faça login como usuário administrador.
3. Se a janela Bem-vindo ao Lake Formation for exibida, escolha o usuário que você criou ou selecionou na Etapa 1 e, escolha Começar.
4. Se você não vir a janela de Boas-vindas ao Lake Formation, execute as etapas a seguir para configurar um administrador do Lake Formation.
    1. No painel de navegação, em Permissões, selecione Perfis e tarefas administrativas. Na seção Administradores do data Lake da página do console, selecione Escolher administradores.
    2. Na caixa de diálogo Gerenciar administradores do data lake, para usuários e funções do IAM, escolha a função do AmazonSecurityLakeMetaStoreManagerIAM que você criou e, em seguida, escolha Salvar.

Para obter mais informações sobre a alteração de permissões para administradores de data lake, consulte Criar um administrador de data lake no Guia do desenvolvedor do AWS Lake Formation .

Como adicionar regiões de rollup

Escolha seu método de acesso preferido e siga estas etapas para adicionar uma região de rollup.

> **Note**
>
> Uma região pode contribuir com dados para várias regiões de rollup. No entanto, uma região de rollup não pode ser uma região contribuinte para outra região de rollup.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, em Configurações, selecione Regiões de rollup.
3. Escolha Modificar e, em seguida, escolha Adicionar região de rollup.
4. Especifique a região de rollup e as regiões contribuintes. Repita esta etapa se quiser adicionar várias regiões de rollup.
5. Se esta é a primeira vez que você adiciona uma região de rollup, para Acesso ao serviço, crie um novo perfil do IAM ou use um perfil do IAM existente que dê permissão ao Security Lake para replicar dados em várias regiões.
6. Ao concluir, escolha Salvar.

Você também pode adicionar uma região de rollup na integração do Security Lake. Para obter mais informações, consulte Conceitos básicos do Amazon Security Lake.

API

Para adicionar uma região cumulativa de forma programática, use a UpdateDataLakeoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o update-data-lakecomando. Em sua solicitação, use o campo `region` para especificar a região na qual você deseja contribuir com dados para a região de rollup. Na `regions` matriz do `replicationConfiguration` parâmetro, especifique o código da região para cada região cumulativa. Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.

Por exemplo, o comando a seguir é definido `ap-northeast-2` como uma região cumulativa. A `us-east-1` Região contribuirá com dados para a `ap-northeast-2` Região. Esse exemplo também estabelece um período de expiração de 365 dias para objetos adicionados ao data lake. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ 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}}}]'
```

Você também pode adicionar uma região de rollup na integração do Security Lake. Para fazer isso, use a CreateDataLakeoperação (ou, se estiver usando o AWS CLI, o create-data-lakecomando). Para obter mais informações sobre como configurar regiões cumulativas durante a integração, consulte. Conceitos básicos do Amazon Security Lake

Como atualizar ou remover regiões de rollup

Escolha seu método de acesso preferido e siga estas etapas para atualizar ou remover regiões de rollup no Security Lake.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, em Configurações, selecione Regiões de rollup.
3. Escolha Modificar.
4. Para alterar as regiões contribuintes de uma região de rollup, especifique as regiões contribuintes atualizadas na linha da região de rollup.
5. Para remover uma região de rollup, escolha Remover na linha da Região de rollup.
6. Ao concluir, escolha Salvar.

API

Para configurar regiões cumulativas de forma programática, use a UpdateDataLakeoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o update-data-lakecomando. Em sua solicitação, use os parâmetros compatíveis para especificar as configurações de rollup:

- Para adicionar uma região contribuinte, use o campo `region` para especificar o código da região a ser adicionada. Na matriz `regions` do objeto `replicationConfiguration`, especifique o código da região para cada região de rollup para a qual contribuir com dados. Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.

- Para remover uma região contribuinte, use o campo `region` para especificar o código da região a ser removida. Nos parâmetros `replicationConfiguration`, não especifique nenhum valor.

Por exemplo, o comando a seguir configura ambas `us-east-1` e `us-east-2` como regiões contribuintes. Ambas as regiões contribuirão com dados para a região `ap-northeast-3` cumulativa. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

```
$ 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"}]}}]'
```

Gerenciamento de fontes no Security Lake

As fontes são registros e eventos gerados a partir de um único sistema que correspondem a uma classe de evento específica no esquema Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake. O Amazon Security Lake pode coletar registros e eventos de várias fontes, incluindo fontes personalizadas de terceiros Serviços da AWS e com suporte nativo.

O Security Lake executa trabalhos de extração, transformação e carregamento (ETL) em dados de origem bruta e converte os dados no formato Apache Parquet e no esquema do OCSF. Após o processamento, o Security Lake armazena os dados de origem em um bucket do Amazon Simple Storage Service (Amazon S3) no local em Conta da AWS que Região da AWS os dados foram gerados. O Security Lake cria um bucket do Amazon S3 diferente para cada região na qual você habilita o serviço. Cada fonte recebe um prefixo separado em seu bucket do S3, e o Security Lake organiza os dados de cada fonte em um conjunto separado de tabelas. AWS Lake Formation

Tópicos

Coletando dados Serviços da AWS do Security Lake

O Amazon Security Lake pode coletar logs e eventos dos seguintes Serviços da AWS com suporte nativo:

- AWS CloudTrail eventos de gerenciamento e dados (S3, Lambda)
- Registros de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS)
- Logs de consulta do Amazon Route 53 Resolver
- AWS Security Hub CSPM descobertas
- Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF registros v2

O Security Lake transforma automaticamente esses dados no formato Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake e Apache Parquet.

> **Tip**
>
> Para adicionar um ou mais dos serviços anteriores como fonte de log no Security Lake, você não precisa configurar separadamente o registro nesses serviços, exceto nos eventos CloudTrail de gerenciamento. Se você tiver o registro configurado nesses serviços, não precisará alterar sua configuração de registro em log para adicioná-los como fontes de registro no Security Lake. O Security Lake extrai dados diretamente desses serviços por meio de um fluxo de eventos independente e duplicado.

Pré-requisito: verificar permissões

Para adicionar um AWS service (Serviço da AWS) como fonte no Security Lake, você deve ter as permissões necessárias. Verifique se a política AWS Identity and Access Management (IAM) anexada à função que você usa para adicionar uma fonte tem permissão para realizar as seguintes ações:

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

É recomendável que a função tenha as seguintes condições e o escopo do recurso para as `s3:PutObject` permissões `S3:getObject` e.

JSON

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

```
            "Sid": "AllowUpdatingSecurityLakeS3Buckets",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::aws-security-data-lake*",
              "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
    }
    ]
}
```

Essas ações permitem coletar registros e eventos do an AWS service (Serviço da AWS) e enviá-los para o AWS Glue banco de dados e a tabela corretos.

Se você usar uma AWS KMS chave para criptografia do lado do servidor do seu data lake, também precisará de permissão para. `kms:DescribeKey`

Adicionando um AWS service (Serviço da AWS) como fonte

Depois de adicionar um AWS service (Serviço da AWS) como fonte, o Security Lake começa automaticamente a coletar registros e eventos de segurança a partir dele. Essas instruções explicam como adicionar uma fonte com suporte nativo no AWS service (Serviço da AWS) Security Lake. Para obter instruções sobre como adicionar uma fonte personalizada, consulte Coletando dados de fontes personalizadas no Security Lake.

Console

Para adicionar uma fonte de AWS registro (console)

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Escolha Fontes no painel de navegação.
3. Selecione AWS service (Serviço da AWS) aquele do qual você deseja coletar dados e escolha Configurar.

4. Na seção Configurações da fonte, habilite a fonte e selecione a versão da fonte de dados que você deseja usar para ingestão de dados. Por padrão, a versão mais recente da fonte de dados é ingerida pelo Security Lake.

   > **Important**
   >
   > Se você não tiver as permissões de função necessárias para habilitar a nova versão da fonte de AWS log na região especificada, entre em contato com o administrador do Security Lake. Para obter mais informações, consulte Atualizar permissões de função.

   Para que seus assinantes consumam a versão selecionada da fonte de dados, você também deve atualizar suas configurações de assinante. Para obter detalhes sobre como editar um assinante, consulte Gerenciamento de assinantes no Amazon Security Lake.

   Opcionalmente, você pode optar por ingerir somente a versão mais recente e desativar todas as versões de origem anteriores usadas para ingestão de dados.

5. Na seção Regiões, selecione as regiões nas quais você deseja coletar dados para a fonte. O Security Lake coletará dados da fonte de todas as contas nas regiões selecionadas.
6. Escolha Habilitar.

API

Para adicionar uma fonte de AWS registro (API)

Para adicionar um AWS service (Serviço da AWS) como fonte programaticamente, use a CreateAwsLogSourceoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o create-aws-log-sourcecomando. Os parâmetros `sourceName` e `regions` são obrigatórios. Opcionalmente, você pode limitar o escopo da fonte a um específico `accounts` ou específico`sourceVersion`.

> **Important**
>
> Quando você não fornece um parâmetro em seu comando, o Security Lake presume que o parâmetro ausente se refere ao conjunto inteiro. Por exemplo, se você não fornecer

o `accounts` parâmetro, o comando se aplicará a todo o conjunto de contas em sua organização.

O exemplo a seguir adiciona registros de fluxo de VPC como fonte nas contas e regiões designadas. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

> **Note**
>
> Se você aplicar essa solicitação a uma região na qual não ativou o Security Lake, você receberá uma mensagem de erro. Você pode resolver o erro ativando o Security Lake nessa região ou usando o `regions` parâmetro para especificar somente as regiões nas quais você ativou o Security Lake.

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

Obtendo o status da coleção de fontes

Escolha seu método de acesso e siga as etapas para obter uma visão geral das contas e fontes para as quais a coleta de registros está ativada na região atual.

Console

Para obter o status da coleta de registros na região atual

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, escolha Contas.
3. Passe o cursor sobre o número na coluna Fontes para ver quais registros estão habilitados para a conta selecionada.

API

Para obter o status da coleta de registros na região atual, use a GetDataLakeSourcesoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o get-data-lake-sourcescomando. Para o `accounts` parâmetro, você pode especificar um ou mais Conta da AWS IDs como uma lista. Se sua solicitação for bem-sucedida, o Security Lake retornará um instantâneo dessas contas na região atual, incluindo de quais AWS fontes o Security Lake está coletando dados e o status de cada fonte. Se você não incluir o `accounts` parâmetro, a resposta incluirá o status da coleta de registros para todas as contas nas quais o Security Lake está configurado na região atual.

Por exemplo, o AWS CLI comando a seguir recupera o status da coleta de registros para as contas especificadas na região atual. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

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

Atualizando permissões de função no Security Lake

Se você não tiver as permissões de função ou os recursos necessários — nova AWS Lambda função e fila do Amazon Simple Queue Service (Amazon SQS) — para ingerir dados de uma nova versão da fonte de dados, você deve atualizar `AmazonSecurityLakeMetaStoreManagerV2` suas permissões de função e criar um novo conjunto de recursos para processar dados de suas fontes.

Escolha seu método preferido e siga as instruções para atualizar suas permissões de função e criar novos recursos para processar dados de uma nova versão de uma fonte de AWS log em uma região específica. Essa é uma ação única, pois as permissões e os recursos são aplicados automaticamente às futuras versões da fonte de dados.

Console

Para atualizar as permissões da função (console)

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login com as credenciais do administrador delegado do Security Lake.
2. No painel de navegação, em Configurações, selecione Geral.
3. Escolha Atualizar permissões de função.

4. Na seção Acesso ao serviço, faça o seguinte:
   - Crie e use uma nova função de serviço — Você pode usar a função AmazonSecurityLakeMetaStoreManagerV2 criada pelo Security Lake.
   - Usar uma função de serviço existente — Você pode escolher uma função de serviço existente na lista de nomes da função de serviço.
5. Escolha Aplicar.

API

Para atualizar as permissões de função (API)

Para atualizar as permissões programaticamente, use a UpdateDataLakeoperação da API Security Lake. Para atualizar as permissões usando o AWS CLI, execute o update-data-lakecomando.

Para atualizar suas permissões de função, você deve anexar a AmazonSecurityLakeMetastoreManagerpolítica à função.

Excluindo a função AmazonSecurityLakeMetaStoreManager

> **Important**
>
> Depois de atualizar suas permissões de função para`AmazonSecurityLakeMetaStoreManagerV2`, confirme se o data lake funciona corretamente antes de remover a `AmazonSecurityLakeMetaStoreManager` função antiga. Recomenda-se esperar pelo menos 4 horas antes de remover a função.

Se você decidir remover a função, primeiro exclua a `AmazonSecurityLakeMetaStoreManager` função de AWS Lake Formation.

Siga estas etapas para remover a `AmazonSecurityLakeMetaStoreManager` função do console do Lake Formation.

1. Faça login no Console de gerenciamento da AWS, e abra o console do Lake Formation em https://console.aws.amazon.com/lakeformation/.

2. No console do Lake Formation, no painel de navegação, escolha Funções e tarefas administrativas.
3. Remova `AmazonSecurityLakeMetaStoreManager` de cada região.

Removendo uma AWS service (Serviço da AWS) fonte de gás do Security Lake

Escolha seu método de acesso e siga estas etapas para remover uma fonte nativa suportada AWS service (Serviço da AWS) como Security Lake. Você pode remover uma fonte de uma ou mais regiões. Quando você remove a fonte, o Security Lake interrompe a coleta de dados dessa fonte nas regiões e contas especificadas, e os assinantes não podem mais consumir novos dados da fonte. No entanto, os assinantes ainda podem consumir dados que o Security Lake coletou da fonte antes da remoção. Você só pode usar essas instruções para remover um AWS service (Serviço da AWS) com suporte nativo como uma fonte. Para obter informações sobre como remover uma fonte personalizada, consulte Coletando dados de fontes personalizadas no Security Lake.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Escolha Fontes no painel de navegação.
3. Selecione uma fonte e escolha Desabilitar.
4. Selecione uma região ou regiões das quais você deseja parar de coletar dados dessa fonte. O Security Lake deixará de coletar dados da fonte de todas as contas nas regiões selecionadas.

API

Para remover um AWS service (Serviço da AWS) como fonte programaticamente, use a DeleteAwsLogSourceoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o delete-aws-log-sourcecomando. Os parâmetros `sourceName` e `regions` são obrigatórios. Opcionalmente, você pode limitar o escopo da remoção a um específico `accounts` ou específico`sourceVersion`.

> **Important**
>
> Quando você não fornece um parâmetro em seu comando, o Security Lake presume que o parâmetro ausente se refere ao conjunto inteiro. Por exemplo, se você não fornecer o `accounts` parâmetro, o comando se aplicará a todo o conjunto de contas em sua organização.

O exemplo a seguir remove os registros de fluxo da VPC como fonte nas contas e regiões designadas.

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

O exemplo a seguir remove o Route 53 como fonte na conta e nas regiões designadas.

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

Os exemplos anteriores estão formatados para Linux, macOS ou Unix e usam o caractere de continuação de linha com barra invertida (\) para melhorar a legibilidade.

CloudTrail registros de eventos no Security Lake

AWS CloudTrail fornece um histórico de chamadas de AWS API para sua conta, incluindo chamadas de API feitas usando as Console de gerenciamento da AWS AWS SDKs ferramentas de linha de comando e determinados AWS serviços. CloudTrail também permite identificar quais usuários e contas AWS APIs solicitaram serviços compatíveis CloudTrail, o endereço IP de origem a partir do qual as chamadas foram feitas e quando as chamadas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

O Security Lake pode coletar registros associados a eventos CloudTrail de gerenciamento e eventos de CloudTrail dados para S3 e Lambda. CloudTrail eventos de gerenciamento, eventos de dados S3 e eventos de dados Lambda são três fontes distintas no Security Lake. Como resultado, eles

têm valores diferentes para `sourceName` quando você adiciona um deles como uma fonte de logs ingeridos. Os eventos de gerenciamento, também conhecidos como eventos do plano de controle, fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos do seu Conta da AWS. CloudTrail eventos de dados, também conhecidos como operações de plano de dados, mostram as operações de recursos realizadas em ou dentro de recursos em seu Conta da AWS. Essas operações geralmente são atividades de alto volume.

Para coletar eventos CloudTrail de gerenciamento no Security Lake, você deve ter pelo menos uma trilha CloudTrail organizacional multirregional que colete eventos de CloudTrail gerenciamento de leitura e gravação. O registro de log deve estar habilitado para a trilha. Se você tiver o registro em log configurado nesses serviços, não precisará alterar sua configuração de registro em log para adicioná-los como fontes de log no Security Lake. O Security Lake extrai dados diretamente desses serviços por meio de um fluxo de eventos independente e duplicado.

Uma trilha de várias regiões fornece arquivos de log de várias regiões para um único bucket do Amazon Simple Storage Service (Amazon S3) para uma única Conta da AWS. Se você já tem uma trilha multirregional gerenciada por meio CloudTrail do console ou AWS Control Tower, nenhuma outra ação é necessária.

- Para obter informações sobre como criar e gerenciar uma trilha CloudTrail, consulte Criação de uma trilha para uma organização no Guia AWS CloudTrail do usuário.
- Para obter informações sobre como criar e gerenciar uma trilha AWS Control Tower, consulte Registrar AWS Control Tower ações AWS CloudTrail no Guia do AWS Control Tower usuário.

Quando você adiciona CloudTrail eventos como fonte, o Security Lake imediatamente começa a coletar seus registros de CloudTrail eventos. Ele consome eventos CloudTrail de gerenciamento e dados diretamente CloudTrail por meio de um fluxo de eventos independente e duplicado.

O Security Lake não gerencia seus CloudTrail eventos nem afeta suas CloudTrail configurações existentes. Para gerenciar o acesso e a retenção de seus CloudTrail eventos diretamente, você deve usar o console CloudTrail de serviço ou a API. Para obter mais informações, consulte Visualização de CloudTrail eventos com histórico de eventos no Guia AWS CloudTrail do usuário.

A lista a seguir fornece links de GitHub repositório para a referência de mapeamento de como o Security Lake normaliza CloudTrail eventos para OCSF.

GitHub Repositório OCSF para eventos CloudTrail

- Versão de origem 1 (v1.0.0-rc.2)

- Versão de origem 2 (v1.1.0)

Registros de auditoria do Amazon EKS no Security Lake

Quando você adiciona os registros de auditoria do Amazon EKS como fonte, o Security Lake começa a coletar informações detalhadas sobre as atividades realizadas nos recursos do Kubernetes em execução em seus clusters do Elastic Kubernetes Service (EKS). Os registros de auditoria do EKS ajudam você a detectar atividades potencialmente suspeitas em seus clusters do EKS no Amazon Elastic Kubernetes Service.

O Security Lake consome eventos do EKS Audit Log diretamente do recurso de registro do plano de controle do Amazon EKS por meio de um fluxo independente e duplicativo de registros de auditoria. Esse processo foi projetado para não exigir configuração adicional ou afetar as configurações existentes de registro do plano de controle do Amazon EKS que você possa ter. Para obter mais informações, consulte Logs do ambiente de gerenciamento do Amazon EKS no Guia do usuário do Amazon EKS.

Os registros de auditoria do Amazon EKS são compatíveis somente com o OCSF v1.1.0. Para obter informações sobre como o Security Lake normaliza os eventos do EKS Audit Logs para OCSF, consulte a referência de mapeamento no repositório GitHub OCSF para eventos do Amazon EKS Audit Logs (v1.1.0).

Registros de consulta do resolvedor Route 53 no Security Lake

Os logs de consulta do Route 53 Resolver rastreiam consultas ao DNS feitas por recursos dentro da sua Amazon Virtual Private Cloud (Amazon VPC). Isso ajuda você a entender como suas aplicações estão operando e a identificar ameaças à segurança.

Quando você adiciona logs de consulta do Route 53 Resolver como fonte no Security Lake, o Security Lake imediatamente começa a coletar seus logs de consulta do Resolver diretamente do Route 53 por meio de um fluxo de eventos independente e duplicado.

O Security Lake não gerencia seus logs do Route 53 nem afeta suas configurações existentes de log de consulta do resolvedor. Para gerenciar logs de consulta do Resolver, é necessário usar o console do Route 53. Para obter mais informações, consulte Como gerenciar configurações de log de consulta do Resolver no Guia do desenvolvedor do Amazon Route 53.

A lista a seguir fornece links de GitHub repositório para a referência de mapeamento de como o Security Lake normaliza os registros do Route 53 para OCSF.

GitHub Repositório OCSF para registros do Route 53

- Versão de origem 1 (v1.0.0-rc.2)
- Versão de origem 2 (v1.1.0)

Descobertas do CSPM do Security Hub em Security Lake

As descobertas do CSPM do Security Hub ajudam você a entender sua postura de segurança AWS e permitem que você verifique seu ambiente de acordo com os padrões e as melhores práticas de segurança do setor. O Security Hub CSPM coleta descobertas de várias fontes, incluindo integrações com outras integrações de produtos de terceiros e Serviços da AWS verificações em relação aos controles CSPM do Security Hub. O Security Hub CSPM processa as descobertas em um formato padrão chamado AWS Security Finding Format (ASFF).

Quando você adiciona as descobertas do Security Hub CSPM como fonte no Security Lake, o Security Lake imediatamente começa a coletar suas descobertas diretamente do CSPM do Security Hub por meio de um fluxo independente e duplicado de eventos. O Security Lake também transforma as descobertas do ASFF para o Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake (OCSF).

O Security Lake não gerencia suas descobertas de CSPM do Security Hub nem afeta suas configurações de CSPM do Security Hub. Para gerenciar as descobertas do CSPM do Security Hub, você deve usar o console de serviço CSPM do Security Hub, a API ou. AWS CLI Para mais informações, consulte Descobertas no AWS Security Hub CSPM no Guia do usuário do AWS Security Hub .

A lista a seguir fornece links de GitHub repositório para a referência de mapeamento de como o Security Lake normaliza as descobertas do CSPM do Security Hub para OCSF.

GitHub Repositório OCSF para descobertas do CSPM do Security Hub

- Versão de origem 1 (v1.0.0-rc.2)
- Versão de origem 2 (v1.1.0)

Registros de fluxo de VPC no Security Lake

O atributo Logs de fluxo da VPC do Amazon VPC captura informações sobre o tráfego de IP que entra e sai das interfaces de rede do seu ambiente.

Quando você adiciona Logs de fluxo da VPC como fonte no Security Lake, o Security Lake imediatamente começa a coletar seus Logs de fluxo da VPC. Ele consome VPC Flow Logs diretamente da Amazon VPC por meio de um stream independente e duplicado de Flow Logs.

O Security Lake não gerencia seus Logs de fluxo da VPC nem afeta suas configurações da Amazon VPC. Para gerenciar seus Logs de fluxo, você deve usar o console de serviços da Amazon VPC. Para obter mais informações, consulte Trabalhar com Logs de fluxo no Guia do desenvolvedor da Amazon VPC.

A lista a seguir fornece links de GitHub repositório para a referência de mapeamento de como o Security Lake normaliza os registros de fluxo de VPC para OCSF.

GitHub Repositório OCSF para registros de fluxo de VPC

- Versão de origem 1 (v1.0.0-rc.2)
- Versão de origem 2 (v1.1.0)

AWS WAF loga no Security Lake

Quando você adiciona AWS WAF como fonte de registros no Security Lake, o Security Lake imediatamente começa a coletar os registros. AWS WAF é um firewall de aplicativo da web que você pode usar para monitorar as solicitações da web que seus usuários finais enviam aos seus aplicativos e para controlar o acesso ao seu conteúdo. As informações registradas incluem a hora em que AWS WAF recebeu uma solicitação da web do seu AWS recurso, informações detalhadas sobre a solicitação e detalhes sobre as regras às quais a solicitação correspondeu.

O Security Lake consome AWS WAF registros diretamente AWS WAF de um fluxo independente e duplicado de registros. Esse processo foi projetado para não exigir configuração adicional nem afetar AWS WAF as configurações existentes. Os registros do Security Lake recuperam somente dados permitidos pela configuração da lista de controle de acesso à AWS WAF web (Web ACL). Se a proteção de dados estiver ativada para a ACL da web nas contas do Security Lake, os dados gerados serão editados ou codificados com base nas configurações da ACL da web. Para obter informações sobre como usar AWS WAF para proteger os recursos do seu aplicativo, consulte Como AWS WAF funciona no Guia do AWS WAF desenvolvedor.

> **Important**
>
> Se você estiver usando a CloudFront distribuição da Amazon como tipo de recurso AWS WAF, deverá selecionar Leste dos EUA (Norte da Virgínia) para ingerir os registros globais no Security Lake.

AWS WAF os registros são suportados somente no OCSF v1.1.0. Para obter informações sobre como o Security Lake normaliza eventos de AWS WAF log para OCSF, consulte a referência de mapeamento no repositório GitHub OCSF para registros (v1.1.0). AWS WAF

Removendo um AWS service (Serviço da AWS) como fonte

Escolha seu método de acesso e siga estas etapas para remover uma fonte nativa suportada AWS service (Serviço da AWS) como Security Lake. Você pode remover uma fonte de uma ou mais regiões. Quando você remove a fonte, o Security Lake interrompe a coleta de dados dessa fonte nas regiões e contas especificadas, e os assinantes não podem mais consumir novos dados da fonte. No entanto, os assinantes ainda podem consumir dados que o Security Lake coletou da fonte antes da remoção. Você só pode usar essas instruções para remover um AWS service (Serviço da AWS) com suporte nativo como uma fonte. Para obter informações sobre como remover uma fonte personalizada, consulte Coletando dados de fontes personalizadas no Security Lake.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Escolha Fontes no painel de navegação.
3. Selecione uma fonte e escolha Desabilitar.
4. Selecione uma região ou regiões das quais você deseja parar de coletar dados dessa fonte. O Security Lake deixará de coletar dados da fonte de todas as contas nas regiões selecionadas.

API

Para remover um AWS service (Serviço da AWS) como fonte programaticamente, use a DeleteAwsLogSourceoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o delete-aws-log-sourcecomando. Os parâmetros

`sourceName` e `regions` são obrigatórios. Opcionalmente, você pode limitar o escopo da remoção a um específico `accounts` ou específico`sourceVersion`.

> **Important**
>
> Quando você não fornece um parâmetro em seu comando, o Security Lake presume que o parâmetro ausente se refere ao conjunto inteiro. Por exemplo, se você não fornecer o `accounts` parâmetro, o comando se aplicará a todo o conjunto de contas em sua organização.

O exemplo a seguir remove os registros de fluxo da VPC como fonte nas contas e regiões designadas.

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

O exemplo a seguir remove o Route 53 como fonte na conta e nas regiões designadas.

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

Os exemplos anteriores estão formatados para Linux, macOS ou Unix e usam o caractere de continuação de linha com barra invertida (\) para melhorar a legibilidade.

Coletando dados de fontes personalizadas no Security Lake

O Amazon Security Lake pode coletar logs e eventos de fontes personalizadas de terceiros. Uma fonte personalizada do Security Lake é um serviço terceirizado que envia registros e eventos de segurança para o Amazon Security Lake. Antes de enviar os dados, a fonte personalizada deve converter os registros e eventos no Open Cybersecurity Schema Framework (OCSF) e atender aos requisitos de origem do Security Lake, incluindo particionamento, formato de arquivo em parquet e requisitos de tamanho e taxa do objeto.

Para cada fonte personalizada, o Security Lake trata do seguinte:

- Fornece um prefixo exclusivo da fonte do bucket do Amazon S3.
- Cria uma função no AWS Identity and Access Management (IAM) que permite que uma fonte personalizada grave dados no data lake. O limite de permissões para essa função é definido por uma política AWS gerenciada chamada `AmazonSecurityLakePermissionsBoundary`.
- Cria uma AWS Lake Formation tabela para organizar os objetos que a fonte grava no Security Lake.
- Configura um AWS Glue rastreador para particionar seus dados de origem. O rastreador o preenche AWS Glue Data Catalog com a mesa. Ele também descobre automaticamente novos dados da fonte e extrai definições do esquema.

> **Note**
>
> Você pode adicionar no máximo 50 fontes de registro personalizadas em uma conta.

Para adicionar uma fonte personalizada ao Security Lake, ela deve atender aos seguintes requisitos. O não cumprimento desses requisitos pode ter impactos no desempenho e em casos de uso de análises, como consultas.

- Destino: a fonte personalizada deve ser capaz de gravar dados no Security Lake como um conjunto de objetos do S3 sob do prefixo atribuído à fonte. Para fontes que contêm várias categorias de dados, você deve fornecer cada classe de evento exclusiva do Open Cybersecurity Schema Framework (OCSF) como uma fonte separada. O Security Lake cria um perfil do IAM que permite que a fonte personalizada grave no local especificado em seu bucket do S3.
- Formato: cada objeto do S3 coletado da fonte personalizada deve ser formatado como um arquivo do Apache Parquet.
- Esquema: a mesma classe de evento do OCSF deve ser aplicada a cada registro em um objeto formatado em Parquet. O Security Lake oferece suporte às versões 1.x e 2.x do Parquet. O tamanho da página de dados deve ser limitado a 1 MB (descompactado). O tamanho do grupo de linhas não deve ser maior que 256 MB (compactado). Para compressão dentro do objeto Parquet, o padrão é o preferido.
- Particionamento — Os objetos devem ser particionados por região, AWS conta, EventDay. Os objetos devem ser prefixados com`source location`/region=`region`/accountId=`accountID`/eventDay=`yyyyMMdd`/.

- Tamanho e taxa do objeto — Os arquivos enviados para o Security Lake devem ser enviados em incrementos entre 5 minutos e 1 dia de evento. Os clientes podem enviar arquivos com mais de 5 minutos se os arquivos tiverem mais de 256 MB. O requisito de objeto e tamanho é otimizar o Security Lake para desempenho de consultas. Não seguir os requisitos de fonte personalizada pode ter um impacto no desempenho do Security Lake.
- Classificação — Dentro de cada objeto formatado em Parquet, os registros devem ser ordenados por tempo para reduzir o custo da consulta de dados.

> **Note**
>
> Use a ferramenta de validação OCSF para verificar se a fonte personalizada é compatível com o. `OCSF Schema` Para fontes personalizadas, o Security Lake oferece suporte ao OCSF versão 1.3 e anteriores.

Requisitos de particionamento para ingestão de fontes personalizadas no Security Lake

Para facilitar o processamento e a consulta eficientes de dados, precisamos atender aos requisitos de particionamento, objeto e tamanho ao adicionar uma fonte personalizada ao Security Lake:

Particionamento

Os objetos devem ser particionados por local de origem Região da AWS, Conta da AWS, e data.

- O caminho dos dados da partição é formatado como

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

  Um exemplo de partição com o nome de bucket de exemplo é`aws-security-data-lake-`*`us-west-2-lake-uid`*`/ext/`*`custom-source-name`*`/region=`*`us-west-2`*`/accountId=`*`123456789012`*`/eventDay=`*`20230428`*`/`.

A lista a seguir descreve os parâmetros usados na partição de caminho do S3:

- O nome do bucket Amazon S3 no qual o Security Lake armazena seus dados de origem personalizados.

- `source-location`: prefixo da fonte personalizada em seu bucket do S3. O Security Lake armazena todos os objetos do S3 de uma determinada fonte sob esse prefixo, e o prefixo é exclusivo da fonte em questão.
- `region`— Região da AWS para o qual os dados são enviados. Por exemplo, você deve usar `US East (N. Virginia)` para carregar dados em seu bucket do Security Lake na região Leste dos EUA (Norte da Virgínia).
- `accountId`— Conta da AWS ID ao qual os registros na partição de origem pertencem. Para registros pertencentes a contas externas à AWS, recomendamos o uso de uma string como `external` ou`external_externalAccountId`. Ao adotar essa convecção de nomenclatura, você pode evitar ambigüidade ao nomear contas externas IDs para que elas não entrem em conflito com a conta IDs ou a AWS conta externa IDs mantida por outros sistemas de gerenciamento de identidade.
- `eventDay`— Carimbo de data/hora UTC do registro, truncado para hora formatado como uma sequência de oito caracteres (). `YYYYMMDD` Se os registros especificarem um fuso horário diferente no timestamp do evento, você deverá converter o timestamp em UTC para essa chave de partição.

Pré-requisitos para adicionar uma fonte personalizada no Security Lake

Ao adicionar uma fonte personalizada, o Security Lake cria um perfil do IAM que permite que a fonte grave dados no local correto no data lake. O nome da função segue o formato`AmazonSecurityLake-Provider-{name of the custom source}-{region}`, onde `region` é aquele Região da AWS em que você está adicionando a fonte personalizada. O Security Lake atribui uma política à função que permite o acesso ao data lake. Se você criptografou o data lake com uma AWS KMS chave gerenciada pelo cliente, o Security Lake também anexa uma política `kms:Decrypt` e `kms:GenerateDataKey` permissões à função. O limite de permissões para essa função é definido por uma política AWS gerenciada chamada `AmazonSecurityLakePermissionsBoundary`.

Tópicos

- Verificar permissões
- Crie a função do IAM para permitir acesso de gravação à localização do bucket do Security Lake (API e etapa AWS CLI somente)

Verificar permissões

Antes de adicionar uma fonte personalizada, verifique se você tem as permissões para realizar as ações a seguir.

Para verificar suas permissões, use o IAM para revisar as políticas do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações nessas políticas com a seguinte lista de ações que você deve ter permissão para adicionar uma fonte personalizada.

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

Essas ações permitem que você colete logs e eventos de uma fonte personalizada, os envie para o AWS Glue banco de dados e a tabela corretos e os armazene no Amazon S3.

Se você usar uma AWS KMS chave para criptografia do lado do servidor do seu data lake, também precisará de permissão para`kms:CreateGrant`, e. `kms:DescribeKey` `kms:GenerateDataKey`

> **Important**
>
> Se você planeja usar o console do Security Lake para adicionar uma fonte personalizada, você pode pular a próxima etapa e continuarAdicionando uma fonte personalizada no Security Lake. O console do Security Lake oferece um processo simplificado para começar e cria todos os perfis necessários do IAM ou usa os perfis existentes em seu nome.

Se você planeja usar a API Security Lake ou AWS CLI adicionar uma fonte personalizada, continue com a próxima etapa para criar uma função do IAM para permitir o acesso de gravação à localização do bucket do Security Lake.

Crie a função do IAM para permitir acesso de gravação à localização do bucket do Security Lake (API e etapa AWS CLI somente)

Se você estiver usando a API Security Lake ou AWS CLI para adicionar uma fonte personalizada, adicione essa função do IAM para conceder AWS Glue permissão para rastrear seus dados de origem personalizados e identificar partições nos dados. Essas partições são necessárias para organizar seus dados e criar e atualizar tabelas no Catálogo de dados.

Depois de criar esse perfil do IAM, você precisará do nome do recurso da Amazon (ARN) do perfil para adicionar uma fonte personalizada.

Você deve anexar a política `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS gerenciada.

Para conceder as permissões necessárias, você também deve criar e incorporar a seguinte política embutida em sua função Crawler do AWS Glue para permitir a leitura de arquivos de dados da fonte personalizada e das tabelas create/update no Catálogo de AWS Glue Dados.

JSON

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

```
}
```

Anexe a seguinte política de confiança para permitir que uma, Conta da AWS usando a qual, ela possa assumir a função com base na ID externa:

JSON

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

Se o bucket do S3 na região em que você está adicionando a fonte personalizada estiver criptografado com uma política gerenciada pelo cliente AWS KMS key, você também deverá anexar a seguinte política à função e à sua política de chaves do KMS:

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

```
}
```

Adicionando uma fonte personalizada no Security Lake

Depois de criar a função do IAM para invocar o AWS Glue rastreador, siga estas etapas para adicionar uma fonte personalizada no Security Lake.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja criar a fonte personalizada.
3. Escolha Fontes personalizadas no painel de navegação e Criar fonte personalizada.
4. Na seção Detalhes da fonte personalizada, insira um nome globalmente exclusivo para sua fonte personalizada. Em seguida, selecione uma classe de evento do OCSF que descreva o tipo de dados que a fonte personalizada enviará para o Security Lake.
5. Para Conta da AWS com permissão para gravar dados, insira o ID da Conta da AWS e o ID externo da fonte personalizada que gravará logs e eventos no data lake.
6. Para o Acesso ao serviço, crie e use um novo perfil de serviço ou use um perfil de serviço existente que dê permissão ao Security Lake para invocar o AWS Glue.
7. Escolha Criar.

API

Para adicionar uma fonte personalizada programaticamente, use a CreateCustomLogSourceoperação da API Security Lake. Use a operação no Região da AWS local em que você deseja criar a fonte personalizada. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o create-custom-log-sourcecomando.

Em sua solicitação, use os parâmetros compatíveis para especificar as configurações da fonte personalizada:

- `sourceName`— Especifique um nome para a fonte. O nome deve ser um valor regionalmente exclusivo.
- `eventClasses`— Especifique uma ou mais classes de eventos OCSF para descrever o tipo de dados que a fonte enviará ao Security Lake. Para obter uma lista das classes de eventos

do OCSF suportadas como fonte no Security Lake, consulte Open Cybersecurity Schema Framework (OCSF).

- `sourceVersion`— Opcionalmente, especifique um valor para limitar a coleta de registros a uma versão específica dos dados de origem personalizados.
- `crawlerConfiguration`— Especifique o Amazon Resource Name (ARN) da função do IAM que você criou para invocar o rastreador. AWS Glue Para ver as etapas detalhadas para criar uma função do IAM, consulte Pré-requisitos para adicionar uma fonte personalizada
- `providerIdentity`— especifique a AWS identidade e a ID externa que a fonte usará para gravar registros e eventos no data lake.

O exemplo a seguir adiciona uma fonte personalizada como fonte de registro na conta do provedor de registros designado nas regiões designadas. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ 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”]
```

Mantendo os dados de origem personalizados atualizados no AWS Glue

Depois de adicionar uma fonte personalizada no Security Lake, o Security Lake cria um AWS Glue rastreador. O crawler se conecta à sua fonte personalizada, determina as estruturas de dados e preenche o Catálogo de dados do AWS Glue com tabelas.

Recomendamos executar manualmente o crawler para manter seu esquema de fonte personalizado atualizado e manter a funcionalidade de consulta no Athena e em outros serviços de consulta. Especificamente, você deve executar o crawler se alguma das seguintes alterações ocorrer em seu conjunto de dados de entrada de uma fonte personalizada:

- O conjunto de dados tem uma ou mais novas colunas de nível superior.
- O conjunto de dados tem um ou mais campos novos em uma coluna com um tipo de dados `struct`.

Para obter instruções sobre como executar um rastreador, consulte Como programar um AWS Glue rastreador no Guia do desenvolvedor.AWS Glue

O Security Lake não pode excluir nem atualizar os crawlers existentes na sua conta. Se você excluir uma fonte personalizada, recomendamos excluir o crawler associado se você planeja criar uma fonte personalizada com o mesmo nome no futuro.

Classes de eventos do OCSF suportadas

As classes de eventos do Open Cybersecurity Schema Framework (OCSF) descrevem o tipo de dados que a fonte personalizada enviará ao Security Lake. A lista de classes de eventos suportadas é:

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

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

```
}
```

Excluindo uma fonte personalizada de Security Lake

Exclua uma fonte personalizada para parar de enviar dados da fonte para o Security Lake. Quando você remove a fonte, o Security Lake interrompe a coleta de dados dessa fonte nas regiões e contas especificadas, e os assinantes não podem mais consumir novos dados da fonte. No entanto, os assinantes ainda podem consumir dados que o Security Lake coletou da fonte antes da remoção. Você só pode usar essas instruções para remover uma fonte personalizada. Para obter informações sobre como remover um suporte nativo, consulte. AWS service (Serviço da AWS)Coletando dados Serviços da AWS do Security Lake

Ao excluir uma fonte personalizada no Security Lake, você deve desativar cada fonte fora do console do Security Lake com a fonte. A falha na desativação de uma integração pode fazer com que as integrações de origem continuem enviando registros para o Amazon S3.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região da qual você deseja remover a fonte personalizada.
3. No painel de navegação, escolha Fontes personalizadas.
4. Selecione a fonte personalizada que deseja remover.
5. Escolha Cancelar o registro da fonte personalizada e Excluir para confirmar a ação.

API

Para excluir uma fonte personalizada programaticamente, use a DeleteCustomLogSourceoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o delete-custom-log-sourcecomando. Use a operação na Região da AWS em que você deseja excluir a fonte personalizada.

Em sua solicitação, use o parâmetro `sourceName` para especificar o nome da fonte personalizada a ser excluída. Ou especifique o nome da fonte personalizada e use o parâmetro `sourceVersion` para limitar o escopo da exclusão somente a uma versão específica dos dados da fonte personalizada.

O exemplo a seguir exclui uma fonte de log personalizada do Security Lake.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

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

Gerenciamento de assinantes no Security Lake

Um assinante do Amazon Security Lake consome registros e eventos do Security Lake. Para controlar os custos e seguir as práticas recomendadas de acesso com privilégio mínimo, você fornece aos assinantes acesso aos dados por fonte. Para obter mais informações sobre fontes, consulte Gerenciamento de fontes no Security Lake.

O Security Lake oferece suporte a dois tipos de acesso de assinantes:

- Acesso aos dados Os assinantes com acesso aos dados de origem no Amazon Security Lake são notificados sobre novos objetos para a fonte à medida que os dados são gravados no bucket do S3. Por padrão, os assinantes são notificados sobre novos objetos por meio de um endpoint HTTPS fornecido por eles. Como alternativa, assinantes podem ser notificados sobre novos objetos por uma fila do Amazon Simple Queue Service (Amazon SQS).
- Acesso à consulta — Os assinantes com acesso à consulta podem consultar os dados que o Security Lake coleta. Esses assinantes consultam diretamente as tabelas do AWS Lake Formation em seu bucket do S3 com serviços como o Amazon Athena.

Os assinantes só têm acesso aos dados de origem Região da AWS que você seleciona ao criar o assinante. Para dar a um assinante acesso aos dados de várias regiões, você pode especificar a região em que você cria o assinante como uma região cumulativa e fazer com que outras regiões contribuam enviando dados para ela. Para obter mais informações sobre regiões cumulativas e regiões contributivas, consulte Gerenciando regiões no Security Lake.

> **Important**
>
> O número máximo de fontes que o Security Lake permite adicionar por assinante é 10. Isso pode ser uma combinação de AWS fontes e fontes personalizadas.

Tópicos

- Como gerenciar o acesso a dados para assinantes do Security Lake
- Gerenciando o acesso de consulta para assinantes do Security Lake

Como gerenciar o acesso a dados para assinantes do Security Lake

Os assinantes com acesso aos dados da fonte no Amazon Security Lake são notificados sobre novos objetos de uma fonte à medida que os dados são gravados no bucket do S3. Por padrão, os assinantes são notificados sobre novos objetos por meio de um endpoint HTTPS fornecido por eles. Como alternativa, assinantes podem ser notificados sobre novos objetos por uma fila do Amazon Simple Queue Service (Amazon SQS).

Os assinantes são notificados sobre novos objetos do Amazon S3 para uma fonte à medida que os objetos são gravados no data lake do Security Lake. Os assinantes podem acessar diretamente os objetos do S3 e receber notificações de novos objetos por meio de um endpoint de assinatura ou por meio de uma pesquisa em uma fila do Amazon Simple Queue Service (Amazon SQS). Esse tipo de assinatura é identificado como `S3` no `accessTypes` parâmetro da CreateSubscriberAPI.

Tópicos

Pré-requisitos para criar um assinante com acesso a dados no Security Lake

É necessário concluir os pré-requisitos a seguir antes de criar um assinante com acesso a dados no Security Lake.

Verificar permissões

Para verificar suas permissões, use o IAM para revisar as políticas do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações dessas políticas com a seguinte lista de ações (de permissões) que você deve ter para notificar os assinantes quando novos dados são gravados no data lake.

Serão necessárias permissões para executar as seguintes ações:

- `iam:CreateRole`

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

Além da lista anterior, você também precisará de permissão para executar as seguintes ações:

- 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

Obtenha o ID externo do assinante

Para criar um assinante, além do Conta da AWS ID do assinante, você também precisará obter o ID externo. O ID externo é um identificador exclusivo que o assinante fornece a você. O Security Lake

adiciona o ID externo ao perfil do IAM do assinante que ele cria. Você usa o ID externo ao criar um assinante no console do Security Lake, por meio da API ou da AWS CLI.

Para obter mais informações sobre o externo IDs, consulte Como usar um ID externo ao conceder acesso aos seus AWS recursos a terceiros no Guia do usuário do IAM.

> **Important**
>
> Se você planeja usar o console do Security Lake para adicionar um assinante, você pode pular a próxima etapa e ir para Criação de um assinante com acesso a dados no Security Lake. O console do Security Lake oferece um processo simplificado para começar e cria todos os perfis necessários do IAM ou usa os perfis existentes em seu nome.
> Se você planeja usar a API Security Lake ou AWS CLI adicionar um assinante, continue com a próxima etapa para criar uma função do IAM para invocar destinos de EventBridge API.

Crie uma função do IAM para invocar EventBridge destinos de API (API e AWS CLI etapa somente)

Se você estiver usando o Security Lake por meio da API ou AWS CLI, crie uma função no AWS Identity and Access Management (IAM) que conceda à Amazon EventBridge permissões para invocar destinos de API e enviar notificações de objetos para os endpoints HTTPS corretos.

Depois de criar esse perfil do IAM, você precisará do nome do recurso da Amazon (ARN) da função para criar o assinante. Esse perfil do IAM não é necessária se o assinante pesquisar dados de uma fila do Amazon Simple Queue Service (Amazon SQS) ou consultar dados diretamente do AWS Lake Formation. Para obter mais informações sobre esse tipo de método de acesso aos dados (tipo de acesso), consulte Gerenciando o acesso de consulta para assinantes do Security Lake.

Anexe a política a seguir ao seu perfil do IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInvokeApiDestination",
            "Effect": "Allow",
```

```
            "Action": [
                "events:InvokeApiDestination"
            ],
            "Resource": [
            "arn:aws:events:us-east-1:123456789012:api-destination/
AmazonSecurityLake*/*"
            ]
        }
    ]
}
```

Anexe a seguinte política de confiança à sua função do IAM EventBridge para permitir que você assuma a função:

JSON

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

O Security Lake cria automaticamente um perfil do IAM que permite ao assinante ler dados do data lake (ou pesquisar eventos de uma fila do Amazon SQS, se esse for o método preferido de notificação). Essa função é protegida por uma política AWS gerenciada chamada `AmazonSecurityLakePermissionsBoundary`.

Criação de um assinante com acesso a dados no Security Lake

Escolha um dos métodos de acesso a seguir para criar um assinante com acesso aos dados atuais Região da AWS.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja criar o assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, escolha Criar assinante.
5. Para obter Detalhes do assinante, insira o Nome do assinante e uma Descrição opcional.

   A região é preenchida automaticamente conforme sua seleção atual Região da AWS e não pode ser modificada.
6. Para Fontes de log e eventos, escolha quais fontes o assinante está autorizado a consumir.
7. Para Método de acesso a dados, escolha S3 para configurar o acesso aos dados para o assinante.
8. Para credenciais de assinante, forneça o ID do assinante e o Conta da AWS ID externo.
9. (Opcional) Para obter Detalhes da notificação, se você quiser que o Security Lake crie uma fila do Amazon SQS que o assinante possa sondar para receber notificações de objetos, selecione fila SQS. Se você quiser que o Security Lake envie notificações EventBridge para um endpoint HTTPS, selecione Endpoint de assinatura.

   Se você selecionar Endpoint da assinatura, faça também o seguinte:

   a. Insira o Endpoint da assinatura. Exemplos de formatos de endpoint válidos incluem **`http://example.com`**. Opcionalmente, você também pode fornecer um nome de chave HTTPS e um valor de chave HTTPS.

   b. Para o Service Access, crie uma nova função do IAM ou use uma função existente do IAM que dê EventBridge permissão para invocar destinos de API e enviar notificações de objetos para os endpoints corretos.

      Para obter informações sobre como criar uma nova função do IAM, consulte Criar função do IAM para invocar destinos de EventBridge API.
10. (Opcional) Em Tags, insira até 50 tags para atribuir ao assinante.

    Uma tag é um rótulo que você pode definir e atribuir a determinados tipos de AWS recursos. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. As tags

podem ajudar você a identificar, categorizar e gerenciar recursos de diferentes maneiras. Para saber mais, consulte Marcando recursos do Security Lake.

11. Escolha Criar.

API

Para criar um assinante com acesso a dados de forma programática, use a CreateSubscriberoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando create-subscriber.

Em sua solicitação, use esses parâmetros para especificar as seguintes configurações para o assinante:

- Para `sources`, especifique cada fonte que você deseja que o assinante acesse.
- Para`subscriberIdentity`, especifique o ID da AWS conta e o ID externo que o assinante usará para acessar os dados de origem.
- Para`subscriber-name`, especifique o nome do assinante.
- Em `accessTypes`, especifique `S3`.

Exemplo 1

O exemplo a seguir cria um assinante com acesso aos dados na AWS região atual para a identidade de assinante especificada para uma AWS fonte.

```
$ 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
```

Exemplo 2

O exemplo a seguir cria um assinante com acesso aos dados na AWS região atual para a identidade de assinante especificada para uma fonte 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
```

Os exemplos anteriores estão formatados para Linux, macOS ou Unix e usam o caractere de continuação de linha com barra invertida (\) para melhorar a legibilidade.

(Opcional) Depois de criar um assinante, use a CreateSubscriberNotificationoperação para especificar como notificar o assinante quando novos dados forem gravados no data lake para as fontes que você deseja que o assinante acesse. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o create-subscriber-notificationcomando.

- Para substituir o método de notificação padrão (endpoint HTTPS) e criar uma fila do Amazon SQS, especifique valores para os parâmetros `sqsNotificationConfiguration`.
- Se você preferir a notificação com um endpoint HTTPS, especifique valores para os parâmetros `httpsNotificationConfiguration`.
- Para o `targetRoleArn` campo, especifique o ARN da função do IAM que você criou para invocar EventBridge destinos de 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 obter `osubscriberID`, use a ListSubscribersoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando list-subscriber.

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

Para alterar posteriormente o método de notificação (fila Amazon SQS ou endpoint HTTPS) para o assinante, use a UpdateSubscriberNotificationoperação ou, se estiver usando o, execute o AWS CLI comando. update-subscriber-notification Você também pode alterar o método de notificação usando o console do Security Lake: selecione o assinante na página Assinantes e escolha Editar.

Exemplo de mensagem de notificação de objeto

O exemplo a seguir mostra a notificação de evento no formato de estrutura JSON para a `CreateSubscriberNotification` operação.

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

Atualizando um assinante de dados no Security Lake

Você pode atualizar um assinante alterando as fontes que o assinante consome. Você também pode atribuir tags ou editar tags para um assinante. Uma tag é um rótulo que você pode definir e atribuir a determinados tipos de AWS recursos, incluindo assinantes. Para saber mais, consulte Marcando recursos do Security Lake.

Escolha um dos métodos de acesso e siga estas etapas para definir novas fontes para uma assinatura existente.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, escolha Assinantes.

3. Selecione o assinante.
4. Escolha Editar e execute uma das seguintes ações:
   - Para atualizar as fontes do assinante, insira as novas configurações na seção Fontes de log e eventos.
   - Para atribuir ou editar tags para o assinante, altere as tags conforme necessário na seção Tags.
5. Ao concluir, escolha Salvar.

API

Para atualizar programaticamente as fontes de acesso aos dados de um assinante, use a UpdateSubscriberoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando update-subscriber. Em sua solicitação, use os parâmetros `sources` para especificar cada fonte que você deseja que o assinante acesse.

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

Para obter uma lista de assinantes associados a uma organização específica Conta da AWS ou a uma organização, use a ListSubscribersoperação. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando list-subscribers.

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

Para revisar as configurações atuais de um assinante específico, use a GetSubscriberoperação. execute o comando get-subscriber. Em seguida, o Security Lake retorna o nome e a descrição do assinante, o ID externo e informações adicionais. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando get-subscriber.

Para atualizar o método de notificação para um assinante, use a UpdateSubscriberNotificationoperação. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o update-subscriber-notificationcomando. Por exemplo, você pode especificar um novo endpoint HTTPS para o assinante ou alternar de um endpoint HTTPS para uma fila do Amazon SQS.

Removendo um assinante de dados do Security Lake

Se você não quiser mais que um assinante consuma dados do Security Lake, você pode remover o assinante seguindo estas etapas.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, escolha Assinantes.
3. Selecione o assinante que deseja remover.
4. Selecione Excluir e confirme a ação. Isso excluirá o assinante e todas as configurações de notificação associadas.

API

Com base no seu cenário, siga um destes procedimentos:

- Para excluir o assinante e todas as configurações de notificação associadas, use a DeleteSubscriberoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando delete-subscriber.
- Para reter o assinante, mas interromper futuras notificações para o assinante, use a DeleteSubscriberNotificationoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o delete-subscriber-notificationcomando run the.

Gerenciando o acesso de consulta para assinantes do Security Lake

Os assinantes com acesso de consulta podem consultar os dados que o Security Lake coleta. Esses assinantes consultam diretamente AWS Lake Formation as tabelas em seu bucket do S3 com serviços como o Amazon Athena. Embora o principal mecanismo de consulta do Security Lake seja o Athena, você também pode usar outros serviços, como Amazon Redshift Spectrum e Spark SQL, que se integram com o AWS Glue Data Catalog.

Os assinantes consultam os dados de origem das AWS Lake Formation tabelas em seu bucket do S3 usando serviços como o Amazon Athena. Esse tipo de assinatura é identificado como `LAKEFORMATION` no `accessTypes` parâmetro da CreateSubscriberAPI.

> **Note**
>
> Esta seção explica como conceder acesso de consulta a um assinante terceirizado. Para obter informações sobre como executar consultas em seu próprio data lake, consulte Etapa 4: visualizar e consultar seus próprios dados.

Tópicos

Pré-requisitos para criar um assinante com acesso a consultas no Security Lake

É necessário concluir os pré-requisitos a seguir antes de criar um assinante com acesso a dados no Security Lake.

Verificar permissões

Antes de criar um assinante com acesso de consulta, verifique se você tem permissão para executar a lista de ações a seguir.

Para verificar suas permissões, use o IAM para revisar as políticas do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações nessas políticas com a seguinte lista de ações que você deve ter permissão para realizar para criar um assinante com acesso de consulta.

- `glue:PutResourcePolicy`
- `glue:DeleteResourcePolicy`
- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `lakeformation:GrantPermissions`

- `lakeformation:ListPermissions`
- `lakeformation:RegisterResource`
- `lakeformation:RevokePermissions`
- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

> **Important**
>
> Depois de verificar as permissões:
>
> - Se você planeja usar o console do Security Lake para adicionar um assinante com acesso de consulta, você pode pular a próxima etapa e ir para Conceda permissões de administrador do Lake Formation. O Security Lake cria todos os perfis necessários do IAM ou usa os perfis existentes em seu nome.
> - Se você planeja usar a API do Security Lake ou a CLI para adicionar um assinante com acesso de consulta, vá para a próxima etapa para criar um perfil do IAM para consultar dados do Security Lake.

Crie uma função do IAM para consultar dados do Security Lake (API e etapa AWS CLI somente)

Ao usar a API Security Lake ou AWS CLI para conceder acesso de consulta a um assinante, você precisará criar uma função chamada`AmazonSecurityLakeMetaStoreManager`. O Security Lake usa essa função para registrar AWS Glue partições e atualizar AWS Glue tabelas. Talvez você já tenha criado esse perfil ao Criar os perfis necessários do IAM.

Conceda permissões de administrador do Lake Formation

Você também precisará adicionar permissões de administrador do Lake Formation ao perfil do IAM que você usa para acessar o console do Security Lake e adicionar assinantes.

Você pode conceder permissões de administrador do Lake Formation para sua função seguindo estas etapas:

1. Abra o console do Lake Formation em https://console.aws.amazon.com/lakeformation/.

2. Faça login como usuário administrador.
3. Se a janela Bem-vindo ao Lake Formation for exibida, escolha o usuário que você criou ou selecionou na Etapa 1 e, escolha Começar.
4. Se você não vir a janela de Boas-vindas ao Lake Formation, execute as etapas a seguir para configurar um administrador do Lake Formation.

    1. No painel de navegação, em Permissões, selecione Perfis e tarefas administrativas. Na seção Administradores do Data Lake, selecione Escolher administradores.
    2. Na caixa de diálogo Gerenciar administradores do data lake, para usuários e perfis do IAM, escolha o perfil de administrador usado ao acessar o console do Security Lake e escolha Salvar.

Para obter mais informações sobre a alteração de permissões para administradores de data lake, consulte Criar um administrador de data lake no Guia do desenvolvedor do AWS Lake Formation .

O perfil do IAM deve ter privilégios `SELECT` no banco de dados e nas tabelas aos quais você deseja conceder acesso a um assinante. Para obter instruções sobre como fazer isso, consulte Conceder permissões ao catálogo de dados usando o método de recurso nomeado no Guia do desenvolvedor do AWS Lake Formation .

Criação de um assinante com acesso a consultas no Security Lake

Escolha seu método preferido para criar um assinante com acesso à consulta no atual Região da AWS. Um assinante só pode consultar dados do local em Região da AWS que ele foi criado. Para criar um assinante, você precisará ter o Conta da AWS ID e o ID externo do assinante. O ID externo é um identificador exclusivo que o assinante fornece a você. Para obter mais informações sobre o externo IDs, consulte Como usar um ID externo ao conceder acesso aos seus AWS recursos a terceiros no Guia do usuário do IAM.

> **Note**
>
> O Security Lake não é compatível com a versão 1 do compartilhamento de dados entre contas do Lake Formation. Você deve atualizar o compartilhamento de dados entre contas do Lake Formation para a versão 2 ou versão 3. Para ver as etapas para atualizar as configurações da versão entre contas por meio do AWS Lake Formation console ou da AWS CLI, consulte Para habilitar a nova versão no Guia do AWS Lake Formation desenvolvedor.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login na conta do administrador delegado.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja criar o assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, escolha Criar assinante.
5. Para obter Detalhes do assinante, insira um Nome de assinante e uma Descrição opcional.

   A região é preenchida automaticamente conforme sua seleção atual Região da AWS e não pode ser modificada.
6. Em Fontes de log e eventos, escolha quais fontes você deseja que o Security Lake inclua ao retornar os resultados da consulta.
7. Em Método de acesso a dados, escolha Lake Formation para criar acesso de consulta para o assinante.
8. Para as credenciais do assinante, forneça o ID do assinante e o Conta da AWS ID externo.
9. (Opcional) Em Tags, insira até 50 tags para atribuir ao assinante.

   Uma tag é um rótulo que você pode definir e atribuir a determinados tipos de AWS recursos. Cada tag consiste em uma chave de tag necessária e um valor de tag opcional. As tags podem ajudar você a identificar, categorizar e gerenciar recursos de diferentes maneiras. Para saber mais, consulte Marcando recursos do Security Lake.
10. Escolha Criar.

API

Para criar um assinante com acesso à consulta de forma programática, use a CreateSubscriberoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando create-subscriber.

Em sua solicitação, use esses parâmetros para especificar as seguintes configurações para o assinante:

- Em `accessTypes`, especifique `LAKEFORMATION`.

- Para `sources`, especifique cada fonte que você deseja que o Security Lake inclua ao retornar os resultados da consulta.
- Para `subscriberIdentity`, especifique a AWS identidade e a ID externa que o assinante usa para consultar os dados de origem.

O exemplo a seguir cria um assinante com acesso de consulta na AWS região atual para a identidade de assinante especificada. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

```
$ 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
```

Como configurar o compartilhamento de tabelas entre contas (etapa do assinante)

O Security Lake usa o compartilhamento de tabelas entre contas do Lake Formation para oferecer suporte ao acesso de consultas para assinantes. Quando você cria um assinante com acesso de consulta no console do Security Lake, na API ou AWS CLI, o Security Lake compartilha informações sobre as tabelas relevantes do Lake Formation com o assinante criando um compartilhamento de recursos em AWS Resource Access Manager ()AWS RAM.

Quando você faz certos tipos de edições em um assinante com acesso de consulta, o Security Lake cria um novo compartilhamento de recursos. Para obter mais informações, consulte Editando um assinante com acesso à consulta no Security Lake.

O assinante deve seguir estas etapas para consumir dados de suas tabelas do Lake Formation:

1. Aceitar o compartilhamento de recursos: o assinante deve aceitar o compartilhamento de recursos que tem o `resourceShareArn` e `resourceShareName` que é gerado quando você cria ou edita o assinante. Escolha um dos seguintes métodos:
   - Para console e AWS CLI, consulte Aceitar um convite de compartilhamento de recursos de AWS RAM.
   - Para API, invoque a GetResourceShareInvitationsAPI. Filtre por `resourceShareArn` e `resourceShareName` para encontrar o compartilhamento de recursos correto. Aceite o convite com a AcceptResourceShareInvitationAPI.

O convite de compartilhamento de recursos expira em 12 horas, então você deve validar e aceitar o convite em 12 horas. Se o convite expirar, você continuará a vê-lo em um estado `PENDING`, mas aceitá-lo não lhe dará acesso aos recursos compartilhados. Depois de 12 horas, exclua o assinante do Lake Formation e recrie o assinante para receber um novo convite de compartilhamento de recursos.

2. Criar um link de recurso para o banco de dados compartilhado — O assinante deve criar um link de recurso para o banco de dados compartilhado do Lake Formation AWS Lake Formation (se estiver usando o console) ou AWS Glue (se estiver usando API/AWS CLI). Esse link de recurso direciona a conta do assinante para o banco de dados compartilhado. Escolha um dos seguintes métodos:
   - Para o console e AWS CLI, consulte Criação de um link de recurso para um banco de dados compartilhado do Catálogo de Dados. no Guia do AWS Lake Formation desenvolvedor.
   - Recomendamos que os assinantes também criem um banco de dados exclusivo com a CreateDatabaseAPI para armazenar tabelas de links de recursos.
3. Consulte as tabelas compartilhadas: serviços como o Amazon Athena podem consultar as tabelas diretamente, e os novos dados que o Security Lake coleta estão automaticamente disponíveis para consulta. As consultas são executadas no assinante e os custos incorridos com as consultas são cobrados do assinante. Conta da AWS Você pode controlar o acesso de leitura aos recursos em sua própria conta do Security Lake.

Para obter mais informações sobre a concessão de permissões entre contas, consulte Compartilhamento de dados entre contas no Lake Formation no Guia do desenvolvedor do AWS Lake Formation .

Editando um assinante com acesso à consulta no Security Lake

O Security Lake oferece suporte para fazer edições em um assinante com acesso de consulta. Você pode editar o nome, a descrição, o ID externo, o principal (Conta da AWS ID) e as fontes de registro do assinante que o assinante pode consumir. Escolha seu método preferido e siga as etapas para editar um assinante com acesso de consulta na Região da AWS atual.

> **Note**
>
> O Security Lake não é compatível com a versão 1 do compartilhamento de dados entre contas do Lake Formation. Você deve atualizar o compartilhamento de dados entre contas do Lake Formation para a versão 2 ou versão 3. Para ver as etapas para atualizar as

configurações da versão entre contas por meio do AWS Lake Formation console ou da AWS CLI, consulte Para habilitar a nova versão no Guia do AWS Lake Formation desenvolvedor.

Console

Com base nos detalhes que você deseja editar, siga as etapas fornecidas somente para essa ação.

Para editar o nome do assinante

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login na conta do administrador delegado.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja editar os detalhes do assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, use o botão de opção para selecionar o assinante que você deseja editar. O Método de acesso aos dados do assinante selecionado deve ser LAKEFORMATION.
5. Escolha Editar.
6. Insira o novo Nome do assinante e escolha Salvar.

Para editar a descrição do assinante

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login na conta do administrador delegado.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja editar o assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, use o botão de opção para selecionar o assinante que você deseja editar. O Método de acesso aos dados do assinante selecionado deve ser LAKEFORMATION.
5. Escolha Editar.
6. Insira a nova descrição para o assinante e escolha Salvar.

Para editar o ID externo

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login na conta do administrador delegado.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja editar os detalhes do assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, use o botão de opção para selecionar o assinante que você deseja editar. O Método de acesso aos dados do assinante selecionado deve ser LAKEFORMATION.
5. Escolha Editar.
6. Insira o novo ID externo fornecido pelo assinante e escolha Salvar.

   Salvar a nova ID externa remove automaticamente o compartilhamento de AWS RAM recursos anterior e cria um novo compartilhamento de recursos para o assinante.
7. O assinante deve aceitar o novo compartilhamento de recursos seguindo a etapa 1 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante). Certifique-se de que o nome do recurso da Amazon (ARN) que aparece nos detalhes do assinante seja o mesmo do console do Lake Formation. O link do recurso para as tabelas compartilhadas permanece como está, portanto, o assinante não precisa criar um novo link de recurso.

Para editar o principal (Conta da AWS ID)

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login na conta do administrador delegado.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja editar os detalhes do assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, use o botão de opção para selecionar o assinante que você deseja editar. O Método de acesso aos dados do assinante selecionado deve ser LAKEFORMATION.
5. Escolha Editar.
6. Insira o novo ID da Conta da AWS do assinante e escolha Salvar.

Salvar o novo ID da conta remove automaticamente o compartilhamento de AWS RAM recursos anterior para que o diretor anterior não possa consumir as fontes de registro e eventos. O Security Lake cria um novo compartilhamento de recursos.

7. Usando as credenciais da nova entidade principal, o assinante deve aceitar o novo compartilhamento de recursos e criar um link de recurso para as tabelas compartilhadas. Isso dá à nova entidade principal acesso aos recursos compartilhados. Para obter instruções, consulte as etapas 1 e 2 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante). Certifique-se de que o nome do recurso da Amazon (ARN) que aparece nos detalhes do assinante seja o mesmo do console do Lake Formation.

Para editar fontes de log e eventos

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.

   Faça login na conta do administrador delegado.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja editar os detalhes do assinante.
3. No painel de navegação, escolha Assinantes.
4. Na página Assinantes, use o botão de opção para selecionar o assinante que você deseja editar. O Método de acesso aos dados do assinante selecionado deve ser LAKEFORMATION.
5. Escolha Editar.
6. Desmarque as fontes existentes ou selecione as fontes que você deseja adicionar. Se você desmarcar uma fonte, nenhuma ação adicional será necessária de sua parte. Se você selecionar para adicionar uma fonte, nenhum novo convite de compartilhamento de recursos será criado. No entanto, o Security Lake atualiza as tabelas compartilhadas do Lake Formation com base nas fontes adicionadas. O assinante deve criar um link de recurso para as tabelas compartilhadas atualizadas para poder consultar os dados da fonte. Para obter instruções, consulte a etapa 2 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante).
7. Escolha Salvar.

API

Para editar programaticamente um assinante com acesso à consulta, use a UpdateSubscriberoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando update-subscriber. Em sua solicitação, use os parâmetros compatíveis para especificar as seguintes configurações para o assinante:

- Para `subscriberName`, especifique o novo nome do assinante.
- Para `subscriberDescription`, especifique a nova descrição.
- Para`subscriberIdentity`, especifique o ID principal (Conta da AWS ID) e externo que o assinante usará para consultar os dados de origem. Você deve fornecer a entidade principal e o ID externo. Se você quiser manter um desses valores igual, passe o valor atual.
  - Atualizar somente o ID externo: essa ação remove o compartilhamento de recursos do AWS RAM anterior e cria um novo compartilhamento de recursos para o assinante. O assinante deve aceitar o novo compartilhamento de recursos seguindo a etapa 1 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante). O link do recurso para as tabelas compartilhadas permanece como está, portanto, o assinante não precisa criar um novo link de recurso.
  - Atualizar somente o principal — Essa ação remove o compartilhamento de AWS RAM recursos anterior para que o principal anterior não possa consumir as fontes de log e eventos. O Security Lake cria um novo compartilhamento de recursos. Usando as credenciais da nova entidade principal, o assinante deve aceitar o novo compartilhamento de recursos e criar um link de recurso para as tabelas compartilhadas. Isso dá à nova entidade principal acesso aos recursos compartilhados. Para obter instruções, consulte as etapas 1 e 2 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante).

  Para atualizar o ID externo e a entidade principal, siga as etapas 1 e 2 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante).
- Para `sources`, remova as fontes existentes ou especifique as fontes que você deseja adicionar. Se você remover uma fonte, nenhuma ação adicional será necessária de sua parte. Se você adicionar uma fonte, nenhum novo convite de compartilhamento de recursos será criado. No entanto, o Security Lake atualiza as tabelas compartilhadas do Lake Formation com base nas fontes adicionadas. O assinante deve criar um link de recurso para as tabelas compartilhadas atualizadas para poder consultar os dados da fonte. Para obter instruções, consulte a etapa 2 em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante).

Consultas do Security Lake

Você pode consultar os dados que o Security Lake armazena em AWS Lake Formation bancos de dados e tabelas. Você também pode criar assinantes terceirizados no console, na API do Security Lake ou na AWS CLI. Assinantes terceirizados também podem consultar dados do Lake Formation nas fontes que você especificar.

O administrador do data lake do Lake Formation deve conceder permissões `SELECT` nos bancos de dados e tabelas relevantes à identidade do IAM que consulta os dados. Um assinante também deve ser criado no Security Lake antes de poder consultar dados. Para obter mais informações sobre como criar um assinante com acesso a consultas, consulte Gerenciando o acesso de consulta para assinantes do Security Lake.

Consultando dados com configurações de retenção

> As configurações do ciclo de vida do Amazon S3 afetam por quanto tempo os dados são mantidos, o que, por sua vez, afeta o tempo que você pode consultar. Se você tiver configurações de retenção definidas no Security Lake, deverá incluir um filtro baseado em tempo em suas consultas para garantir que seus conjuntos de resultados tenham como escopo os arquivos de dados que não expiraram. Para obter mais informações sobre retenção de dados no Security Lake, consulteGerenciamento de ciclo de vida.

Os exemplos de consulta nas seções a seguir incluem filtros baseados em tempo, como `eventDay` `outime_dt`, para demonstrar essa prática recomendada.

Tópicos

- Consultas do Security Lake para a versão de AWS origem 1 (OCSF 1.0.0-rc.2)
- Consultas do Security Lake para a versão AWS de origem 2 (OCSF 1.1.0)

Consultas do Security Lake para a versão de AWS origem 1 (OCSF 1.0.0-rc.2)

A seção a seguir fornece orientação sobre como consultar dados do Security Lake e inclui alguns exemplos de consulta para AWS fontes com suporte nativo para a versão de origem 1.AWS Essas consultas são projetadas para recuperar dados em um local específico.Região da AWS Esses

exemplos usam us-east-1 (Leste dos EUA (Norte da Virgínia)). Além disso, as consultas de exemplo usam um parâmetro `LIMIT 25`, que retorna até 25 registros. Você pode omitir esse parâmetro ou ajustá-lo com base nas suas preferências. Para obter mais exemplos, consulte o diretório de consultas GitHub OCSF do Amazon Security Lake.

As consultas a seguir incluem filtros baseados em tempo `eventDay` para garantir que sua consulta esteja dentro das configurações de retenção definidas. Para obter mais informações, consulte Querying data with retention settings.

Por exemplo, se dados com mais de 60 dias expiraram, suas consultas devem incluir restrições de tempo para impedir o acesso a dados expirados. Por um período de retenção de 60 dias, inclua a seguinte cláusula em sua consulta:

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

Essa cláusula usa 59 dias (em vez de 60) para evitar qualquer sobreposição de dados ou tempo entre o Amazon S3 e o Apache Iceberg.

Tabela de origem do log

Ao consultar dados do Security Lake, você deve incluir o nome da tabela do Lake Formation na qual os dados residem.

```
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
```

Os valores comuns da tabela de origem do log incluem o seguinte:

- `cloud_trail_mgmt_1_0`— eventos AWS CloudTrail de gerenciamento

- `lambda_execution_1_0`— eventos CloudTrail de dados para Lambda
- `s3_data_1_0`— eventos CloudTrail de dados para S3
- `route53_1_0` – Logs de consulta do Amazon Route 53 Resolver
- `sh_findings_1_0`—AWS Security Hub CSPM descobertas
- `vpc_flow_1_0` – Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)

Exemplo: Todas as descobertas do CSPM do Security Hub na tabela da região **`sh_findings_1_0`** us-east-1

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

Região do banco de dados

Ao consultar dados do Security Lake, você deve incluir o nome da região do banco de dados da qual você está consultando os dados. Para obter uma lista completa das regiões do banco de dados em que o Security Lake está disponível atualmente, consulte os endpoints do Amazon Security Lake.

Exemplo: Listar AWS CloudTrail atividades do IP de origem

O exemplo a seguir lista todas as CloudTrail atividades do IP de origem *192.0.2.1* que foram registradas após *20230301* (01 de março de 2023), na tabela *cloud_trail_mgmt_1_0* do *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
```

Data da partição

Ao particionar os dados, você pode restringir a quantidade que cada consulta verifica, melhorando a performance e reduzindo o custo. O Security Lake implementa o particionamento por meio dos parâmetros `eventDay`, `region` e `accountid`. As partições `eventDay` usam o formato `YYYYMMDD`.

Este é um exemplo de consulta usando a partição `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
```

Os valores comuns de `eventDay` incluem o seguinte:

Eventos ocorridos no último 1 ano

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

Eventos ocorridos no último 1 mês

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

Eventos ocorridos nos últimos 30 dias

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

Eventos ocorridos nas últimas 12 horas

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

Eventos ocorridos nos últimos 5 minutos

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

Eventos ocorridos entre 7 e 14 dias atrás

```
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 ocorridos na data específica ou após

```
>= '20230301'
```

Exemplo: lista de todas as CloudTrail atividades do IP de origem **`192.0.2.1`** em ou após 1º de março de 2023 na tabela **`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
```

Exemplo: lista de todas as CloudTrail atividades do IP de origem **`192.0.2.1`** nos últimos 30 dias na tabela **`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
```

Exemplos de consultas do Security Lake para dados CloudTrail

AWS CloudTrail rastreia a atividade do usuário e o uso da API em Serviços da AWS. Os assinantes podem consultar CloudTrail dados para aprender os seguintes tipos de informações:

Aqui estão alguns exemplos de consultas de CloudTrail dados para a versão de AWS origem 1:

Tentativas não autorizadas contra Serviços da AWS nos últimos 7 dias

```
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 todas as CloudTrail atividades do IP de origem **`192.0.2.1`** nos últimos 7 dias

```
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 todas as atividades do IAM nos últimos 7 dias

```
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
```

Instâncias em que a credencial **`AIDACKCEVSQ6C2EXAMPLE`** foi usada nos últimos 7 dias

```
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 com falha nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para registros de consultas do resolvedor do Route 53

Os logs de consulta do Amazon Route 53 Resolver rastreiam consultas ao DNS feitas por recursos dentro da sua Amazon VPC. Os assinantes podem consultar os registros de consulta do Route 53 Resolver para aprender os seguintes tipos de informações:

Aqui estão alguns exemplos de consultas dos registros de consultas do resolvedor do Route 53 para a versão AWS de origem 1:

Lista de consultas de DNS dos CloudTrail últimos 7 dias

```
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 ao DNS que corresponderam a **`s3.amazonaws.com`** nos últimos 7 dias

```
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 ao DNS que não foram resolvidas nos últimos 7 dias

```
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 ao DNS que foram resolvidas para **`192.0.2.1`** nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para descobertas do CSPM do Security Hub

O Security Hub CSPM fornece uma visão abrangente do seu estado de segurança AWS e ajuda você a verificar seu ambiente de acordo com os padrões e as melhores práticas do setor de segurança. O Security Hub CSPM produz descobertas para verificações de segurança e recebe descobertas de serviços de terceiros.

Aqui estão alguns exemplos de consultas das descobertas do CSPM do Security Hub:

Novas descobertas com severidade maior ou igual à **`MEDIUM`** nos últimos 7 dias

```
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
```

Descobertas duplicadas nos últimos 7 dias

```
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
```

Todas as descobertas não informativas nos últimos 7 dias

```
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
```

Descobertas em que o recurso é um bucket do Amazon S3 (sem restrição de tempo)

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

Resultados com uma pontuação do Common Vulnerability Scoring System (CVSS) maior do que **1** (sem restrição de tempo)

```
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
```

Descobertas que correspondem a Common Vulnerabilities and Exposures (CVE) **CVE-0000-0000** (sem restrição de tempo)

```
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
```

Contagem de produtos que enviaram descobertas do Security Hub CSPM nos últimos 7 dias

```
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
```

Contagem dos tipos de recursos nas descobertas nos últimos 7 dias

```
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
```

Pacotes vulneráveis nas descobertas nos últimos 7 dias

```
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
```

Descobertas que foram alteradas nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para Amazon VPC Flow Logs

O Amazon Virtual Private Cloud (Amazon VPC) fornece detalhes sobre o tráfego IP de e para interfaces de rede na sua VPC.

Aqui estão alguns exemplos de consultas dos Amazon VPC Flow Logs AWS para a versão de origem 1:

Tráfego específico Regiões da AWS nos últimos 7 dias

```
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 atividades do IP de origem **`192.0.2.1`** e da porta de origem **22** nos últimos 7 dias

```
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
```

Contagem de endereços IP de destino distintos nos últimos 7 dias

```
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
```

Tráfego originado de 198.51.100.0/24 nos últimos 7 dias

```
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 o tráfego HTTPS nos últimos 7 dias

```
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
```

Ordenar por contagem de pacotes as conexões destinadas à porta **443** nos últimos 7 dias

```
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 o tráfego entre IPs **192.0.2.1** e **192.0.2.2** nos últimos 7 dias

```
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 o tráfego de entrada nos últimos 7 dias

```
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 o tráfego de saída nos últimos 7 dias

```
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 o tráfego rejeitado nos últimos 7 dias

```
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 do Security Lake para a versão AWS de origem 2 (OCSF 1.1.0)

A seção a seguir fornece orientação sobre como consultar dados do Security Lake e inclui alguns exemplos de consulta para AWS fontes com suporte nativo para a versão de origem 2.AWS Essas consultas são projetadas para recuperar dados em um local específico.Região da AWS Esses exemplos usam us-east-1 (Leste dos EUA (Norte da Virgínia)). Além disso, as consultas de exemplo usam um parâmetro `LIMIT 25`, que retorna até 25 registros. Você pode omitir esse parâmetro ou ajustá-lo com base nas suas preferências. Para obter mais exemplos, consulte o diretório de consultas GitHub OCSF do Amazon Security Lake.

Você pode consultar os dados que o Security Lake armazena em AWS Lake Formation bancos de dados e tabelas. Você também pode criar assinantes terceirizados no console, na API do Security Lake ou na AWS CLI. Assinantes terceirizados também podem consultar dados do Lake Formation nas fontes que você especificar.

O administrador do data lake do Lake Formation deve conceder permissões `SELECT` nos bancos de dados e tabelas relevantes à identidade do IAM que consulta os dados. Um assinante também deve ser criado no Security Lake antes de poder consultar dados. Para obter mais informações sobre como criar um assinante com acesso a consultas, consulte Gerenciando o acesso de consulta para assinantes do Security Lake.

As consultas a seguir incluem filtros baseados em tempo `eventDay` para garantir que sua consulta esteja dentro das configurações de retenção definidas. Para obter mais informações, consulte Querying data with retention settings.

Por exemplo, se dados com mais de 60 dias expiraram, suas consultas devem incluir restrições de tempo para impedir o acesso a dados expirados. Por um período de retenção de 60 dias, inclua a seguinte cláusula em sua consulta:

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

```
...
```

Essa cláusula usa 59 dias (em vez de 60) para evitar qualquer sobreposição de dados ou tempo entre o Amazon S3 e o Apache Iceberg.

Tabela de origem do log

Ao consultar dados do Security Lake, você deve incluir o nome da tabela do Lake Formation na qual os dados residem.

```
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
```

Os valores comuns da tabela de origem do log incluem o seguinte:

- `cloud_trail_mgmt_2_0`— eventos AWS CloudTrail de gerenciamento
- `lambda_execution_2_0`— eventos CloudTrail de dados para Lambda
- `s3_data_2_0`— eventos CloudTrail de dados para S3
- `route53_2_0` – Logs de consulta do Amazon Route 53 Resolver
- `sh_findings_2_0`—AWS Security Hub CSPM descobertas
- `vpc_flow_2_0` – Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)
- `eks_audit_2_0`— Registros de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS)
- `waf_2_0`—AWS WAF Registros v2

Exemplo: Todas as descobertas do CSPM do Security Hub na tabela da região **`sh_findings_2_0`** us-east-1

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

Região do banco de dados

Ao consultar dados do Security Lake, você deve incluir o nome da região do banco de dados da qual você está consultando os dados. Para obter uma lista completa das regiões do banco de dados em que o Security Lake está disponível atualmente, consulte os endpoints do Amazon Security Lake.

Exemplo: Listar a atividade da Amazon Virtual Private Cloud a partir do IP de origem

O exemplo a seguir lista todas as atividades da Amazon VPC do IP de origem *192.0.2.1* que foram registradas após *20230301* (01 de março de 2023), na tabela *vpc_flow_2_0* do. *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
```

Data da partição

Ao particionar os dados, você pode restringir a quantidade que cada consulta verifica, melhorando a performance e reduzindo o custo. As partições funcionam um pouco diferente no Security Lake 2.0 em comparação com o Security Lake 1.0. O Security Lake agora implementa o particionamento por meio `detime_dt`, e. `region` `accountid` Já o Security Lake 1.0 implementou o particionamento por meio `eventDay` `region` de parâmetros e. `accountid`

A consulta `time_dt` produzirá automaticamente as partições de data do S3 e pode ser consultada como qualquer campo baseado em horário no Athena.

Este é um exemplo de consulta usando a `time_dt` partição para consultar os registros após o horário de 01 de março 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
```

Os valores comuns de `time_dt` incluem o seguinte:

Eventos ocorridos no último 1 ano

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

Eventos ocorridos no último 1 mês

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

Eventos ocorridos nos últimos 30 dias

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

Eventos ocorridos nas últimas 12 horas

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

Eventos ocorridos nos últimos 5 minutos

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

Eventos ocorridos entre 7 e 14 dias atrás

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

Eventos ocorridos na data específica ou após

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

Exemplo: lista de todas as CloudTrail atividades do IP de origem **`192.0.2.1`** em ou após 1º de março de 2023 na tabela **`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
```

Exemplo: lista de todas as CloudTrail atividades do IP de origem **`192.0.2.1`** nos últimos 30 dias na tabela **`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 os observáveis do Security Lake

Observables é um novo recurso agora disponível no Security Lake 2.0. O objeto observável é um elemento pivô que contém informações relacionadas encontradas em vários lugares do evento. A consulta de observáveis permite que os usuários obtenham insights de segurança de alto nível de seus conjuntos de dados.

Ao consultar elementos específicos nos observáveis, você pode restringir os conjuntos de dados a coisas como nomes de usuário específicos, recursos UIDs IPs, hashes e outras informações do tipo de IOC

Este é um exemplo de consulta usando a matriz observables para consultar os registros nas tabelas VPC Flow e Route53 contendo o 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
```

Exemplos de consultas do Security Lake para dados CloudTrail

AWS CloudTrail rastreia a atividade do usuário e o uso da API em Serviços da AWS. Os assinantes podem consultar CloudTrail dados para aprender os seguintes tipos de informações:

Aqui estão alguns exemplos de consultas de CloudTrail dados para a versão AWS de origem 2:

Tentativas não autorizadas contra Serviços da AWS nos últimos 7 dias

```
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 todas as CloudTrail atividades do IP de origem **`192.0.2.1`** nos últimos 7 dias

```
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 todas as atividades do IAM nos últimos 7 dias

```
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
```

Instâncias em que a credencial **`AIDACKCEVSQ6C2EXAMPLE`** foi usada nos últimos 7 dias

```
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 com falha nos últimos 7 dias

```
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
```

Exemplos de consultas para logs de consulta do Route 53 Resolver

Os logs de consulta do Amazon Route 53 Resolver rastreiam consultas ao DNS feitas por recursos dentro da sua Amazon VPC. Os assinantes podem consultar os registros de consulta do Route 53 Resolver para aprender os seguintes tipos de informações:

Aqui estão alguns exemplos de consultas para registros de consulta do reesolver do Route 53 para AWS a versão de origem 2:

Lista de consultas de DNS dos CloudTrail últimos 7 dias

```
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 ao DNS que corresponderam a **`s3.amazonaws.com`** nos últimos 7 dias

```
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 ao DNS que não foram resolvidas nos últimos 7 dias

```
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 ao DNS que foram resolvidas para **`192.0.2.1`** nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para descobertas do CSPM do Security Hub

O Security Hub CSPM fornece uma visão abrangente do seu estado de segurança AWS e ajuda você a verificar seu ambiente de acordo com os padrões e as melhores práticas do setor de segurança. O Security Hub CSPM produz descobertas para verificações de segurança e recebe descobertas de serviços de terceiros.

Aqui estão alguns exemplos de consultas sobre as descobertas do CSPM do Security Hub para a versão de AWS origem 2:

Novas descobertas com severidade maior ou igual à **`MEDIUM`** nos últimos 7 dias

```
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
```

Descobertas duplicadas nos últimos 7 dias

```
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
```

Todas as descobertas não informativas nos últimos 7 dias

```
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
```

Descobertas em que o recurso é um bucket do Amazon S3 (sem restrição de tempo)

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

Resultados com uma pontuação do Common Vulnerability Scoring System (CVSS) maior do que **1** (sem restrição de tempo)

```
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
```

Descobertas que correspondem a Common Vulnerabilities and Exposures (CVE) **CVE-0000-0000** (sem restrição de tempo)

```
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
```

Contagem de produtos que enviaram descobertas do Security Hub CSPM nos últimos 7 dias

```
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
```

Contagem dos tipos de recursos nas descobertas nos últimos 7 dias

```
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
```

Pacotes vulneráveis nas descobertas nos últimos 7 dias

```
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
```

Descobertas que foram alteradas nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para Amazon VPC Flow Logs

O Amazon Virtual Private Cloud (Amazon VPC) fornece detalhes sobre o tráfego IP de e para interfaces de rede na sua VPC.

Aqui estão alguns exemplos de consultas para Amazon VPC Flow Logs AWS para a versão de origem 2:

Tráfego específico Regiões da AWS nos últimos 7 dias

```
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 atividades do IP de origem **`192.0.2.1`** e da porta de origem **22** nos últimos 7 dias

```
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
```

Contagem de endereços IP de destino distintos nos últimos 7 dias

```
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
```

Tráfego originado de 198.51.100.0/24 nos últimos 7 dias

```
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 o tráfego HTTPS nos últimos 7 dias

```
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
```

Ordenar por contagem de pacotes as conexões destinadas à porta **443** nos últimos 7 dias

```
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 o tráfego entre IPs **192.0.2.1** e **192.0.2.2** nos últimos 7 dias

```
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 o tráfego de entrada nos últimos 7 dias

```
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 o tráfego de saída nos últimos 7 dias

```
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 o tráfego rejeitado nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para registros de auditoria do Amazon EKS

Os registros do Amazon EKS rastreiam a atividade do plano de controle e fornecem registros de auditoria e diagnóstico diretamente do plano de controle do Amazon EKS para CloudWatch os registros em sua conta. Esses logs facilitam a proteção e a execução dos clusters. Os assinantes podem consultar os registros do EKS para aprender os seguintes tipos de informações.

Aqui estão alguns exemplos de consultas para registros de auditoria do Amazon EKS para a versão AWS de origem 2:

Solicitações para um URL específico nos últimos 7 dias

```
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
```

Solicitações de atualização de '10.0.97.167' nos últimos 7 dias

```
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
```

Solicitações e respostas associadas ao recurso kube-controller-manager '' nos últimos 7 dias

```
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
```

Exemplos de consultas do Security Lake para registros AWS WAF v2

AWS WAFé um firewall de aplicativo da web que você pode usar para monitorar as solicitações da web que seus usuários finais enviam aos seus aplicativos e para controlar o acesso ao seu conteúdo.

Aqui estão alguns exemplos de consultas para registros AWS WAF v2 para a versão de AWS origem 2:

Publique solicitações de um IP de origem específico nos últimos 7 dias

```
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
```

Solicitações que corresponderam a um tipo de firewall MANAGED_RULE_GROUP nos últimos 7 dias

```
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
```

Solicitações que corresponderam a uma REGEX em uma regra de firewall nos últimos 7 dias

```
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
```

Solicitações de AWS credenciais negadas que acionaram a AWS WAF regra nos últimos 7 dias

```
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
```

Receba solicitações de AWS credenciais, agrupadas por país nos últimos 7 dias

```
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
```

Gerenciamento do ciclo de vida no Security Lake

Você pode personalizar o Security Lake para armazenar dados de sua preferência Regiões da AWS pelo período de tempo de sua preferência. O gerenciamento do ciclo de vida pode ajudá-lo a cumprir diferentes requisitos de conformidade.

Gerenciamento de retenção

Para gerenciar seus dados de forma que sejam armazenados de forma econômica, você pode configurar a retenção dos dados usando as configurações do ciclo de vida no Security Lake. Essas configurações de retenção ajudam você a especificar sua classe de armazenamento preferida do Amazon S3 e o período de tempo para que os objetos do Amazon S3 permaneçam nessa classe de armazenamento antes de fazerem a transição para uma classe de armazenamento diferente e expirarem.

> **Warning**
>
> Recomendamos gerenciar as configurações de retenção por meio do console, da API ou da CLI do Security Lake. Isso ocorre porque a modificação das configurações do ciclo de vida do Amazon S3 diretamente no serviço Amazon S3 pode potencialmente excluir metadados e impedir que você acesse seus dados.

Considerações importantes sobre as configurações de retenção no Security Lake

Analise as seguintes considerações ao gerenciar a retenção de dados no Security Lake:

- O Security Lake não é compatível com o Amazon S3 Object Lock. Quando os buckets do data lake são criados, o bloqueio de objetos do S3 é desabilitado por padrão. A ativação do S3 Object Lock com o modo de retenção padrão interrompe a entrega de dados de log normalizados ao data lake.
- A classe de armazenamento padrão do Amazon S3 é S3 Standard. Se você não definir as configurações de retenção, o Security Lake usa as configurações padrão para uma configuração de ciclo de vida do Amazon S3 — armazene os dados indefinidamente usando a classe de armazenamento S3 Standard.

- No Security Lake, você especifica as configurações de retenção no nível da região. Por exemplo, você pode configurar todos os objetos do S3 de uma forma específica Região da AWS para fazer a transição para a classe de armazenamento S3 Standard-IA 30 dias depois de serem gravados no data lake.
- Embora as configurações de retenção sejam aplicadas somente aos dados armazenados no bucket do S3, os metadados do Apache Iceberg são excluídos da política de retenção.

Como definir as configurações de retenção ao habilitar o Security Lake

Siga estas instruções para definir as configurações de retenção para uma ou mais regiões ao se integrar ao Security Lake.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Ao chegar à Etapa 2: Definir o objetivo alvo do fluxo de trabalho de integração, escolha Adicionar transição em Selecionar classes de armazenamento. Em seguida, escolha a classe de armazenamento do Amazon S3 para a qual você deseja fazer a transição de objetos do S3. (A classe de armazenamento não listada, padrão, é S3 Standard.) Especifique também um período de retenção (em dias) para essa classe de armazenamento. Para fazer a transição de objetos para outra classe de armazenamento após esse período, escolha Adicionar transição e insira as configurações para a classe de armazenamento e o período de retenção subsequentes.
3. Para especificar quando você deseja que os objetos do S3 expirem, escolha Adicionar transição. Em seguida, para a classe de armazenamento, escolha Expirar. Para o período de retenção, insira o número total de dias pelo qual você deseja armazenar objetos no Amazon S3, usando qualquer classe de armazenamento, após a criação dos objetos. Quando esse período termina, os objetos expiram e o Amazon S3 os exclui.
4. Ao terminar, escolha Avançar.

Suas alterações se aplicarão a todas as regiões nas quais você ativou o Security Lake durante as etapas anteriores de integração.

API

Para definir as configurações de retenção programaticamente ao se integrar ao Security Lake, use a CreateDataLakeoperação da API do Security Lake. Se você estiver usando a AWS CLI,

execute o comando create-data-lake. Especifique as configurações de retenção desejadas nos `lifecycleConfiguration` parâmetros da seguinte forma:

- Para `transitions`, especifique o número total de dias (`days`) pelo qual você deseja armazenar objetos do S3 em uma determinada classe de armazenamento do Amazon S3 (`storageClass`).
- Para `expiration`, especifique o número total de dias pelo qual você deseja armazenar objetos no Amazon S3, usando qualquer classe de armazenamento, após a criação dos objetos. Quando esse período termina, os objetos expiram e o Amazon S3 os exclui.

O Security Lake aplica as configurações à Região que você especifica no campo `region` do objeto `configurations`.

Por exemplo, o comando a seguir ativa o Security Lake na `us-east-1` região. Nessa região, os objetos expiram após 365 dias e os objetos fazem a transição para a classe de armazenamento `ONEZONE_IA` S3 após 60 dias. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ 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"
```

Como atualizar configurações de retenção

Siga estas instruções para atualizar as configurações de retenção para uma ou mais regiões depois de ativar o Security Lake.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, escolha Regiões
3. Selecione uma região e escolha Editar.

4. Na seção Selecionar classes de armazenamento, insira as configurações desejadas. Na classe de armazenamento, escolha a classe de armazenamento do Amazon S3 para a qual deseja fazer a transição dos objetos do S3. (A classe de armazenamento não listada, padrão, é S3 Standard.) Para o período de retenção, insira o número de dias pelos quais você deseja armazenar objetos nessa classe de armazenamento. Você pode especificar várias transições.

   Para especificar também quando você deseja que os objetos do S3 expirem, escolha Expirar na classe de armazenamento. Em seguida, para o período de retenção, insira o número total de dias pelo qual você deseja armazenar objetos no Amazon S3, usando qualquer classe de armazenamento, após a criação dos objetos. Quando esse período termina, os objetos expiram e o Amazon S3 os exclui.
5. Ao concluir, escolha Salvar.

API

Para atualizar as configurações de retenção programaticamente, use a UpdateDataLakeoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o update-data-lakecomando. Em sua solicitação, use o `lifecycleConfiguration` parâmetro para especificar as novas configurações:

- Para alterar as configurações de transição, use os parâmetros `transitions` para especificar cada novo período em dias (`days`) em que você deseja armazenar objetos do S3 em uma determinada classe de armazenamento do Amazon S3 (`storageClass`).
- Para alterar o período geral de retenção, use o parâmetro `expiration` para especificar o número total de dias pelo qual você deseja armazenar objetos do S3, usando qualquer classe de armazenamento, após a criação dos objetos. Quando esse período de retenção termina, os objetos expiram e o Amazon S3 os exclui.

O Security Lake aplica as configurações à Região que você especifica no campo `region` do objeto `configurations`.

A `UpdateDataLake` operação da API Security Lake funciona como uma operação “upsert” que executa uma inserção se o item ou registro especificado não existir, ou uma atualização se ele já existir. O Security Lake armazena com segurança seus dados em repouso usando soluções de AWS criptografia.

Omitir a chave `encryptionConfiguration` de uma região incluída em uma chamada de atualização que atualmente usa o KMS deixará a chave KMS dessa região em vigor, mas especificar uma chave redefinirá a chave na mesma região.

Por exemplo, o AWS CLI comando a seguir atualiza as configurações de expiração de dados e as configurações de transição de armazenamento para a `us-east-1` região. Nessa região, os objetos expiram após 500 dias e os objetos fazem a transição para a classe de armazenamento `ONEZONE_IA` S3 após 30 dias. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

```
$ 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"
```

Regiões de rollup

Uma região de rollup consolida dados de uma ou mais regiões contribuintes. Isso pode ajudar você a cumprir os requisitos regionais de conformidade de dados.

Para obter instruções sobre como configurar regiões cumulativas, consulte. Configurando regiões cumulativas no Security Lake

Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake

O que é o OCSF?

O Open Cybersecurity Schema Framework (OCSF) é um esforço colaborativo AWS e de código aberto de parceiros líderes no setor de segurança cibernética. O OCSF fornece um esquema padrão para eventos de segurança comuns, define critérios de versionamento para viabilizar a evolução do esquema e inclui um processo de autogovernança para desenvolvedores e consumidores de logs de segurança. O código-fonte público do OCSF está hospedado em. GitHub

O Security Lake converte automaticamente registros e eventos provenientes de suporte nativo para o esquema Serviços da AWS OCSF. Após a conversão para OCSF, o Security Lake armazena os dados em um bucket do Amazon Simple Storage Service (Amazon S3) (um bucket por) em seu.Região da AWSConta da AWS Os logs e eventos gravados no Security Lake a partir de fontes personalizadas devem seguir o esquema do OCSF e o formato Apache Parquet. Os assinantes podem tratar os logs e eventos como logs genéricos do Parquet ou aplicar a classe de eventos do esquema do OCSF para interpretar com mais precisão as informações contidas em um registro.

Classes de evento do OCSF

Os logs e eventos de uma determinada fonte do Security Lake correspondem a uma classe de evento específica definida no OCSF. Atividade do DNS, Atividade de SSH e Autenticação são exemplos de classes de eventos no OCSF. Você pode especificar a qual classe de evento uma determinada fonte corresponde.

Identificação da fonte do OCSF

O OCSF usa uma variedade de campos para ajudá-lo a determinar a origem de um conjunto específico de logs ou eventos. Esses são os valores dos campos relevantes Serviços da AWS que são suportados nativamente como fontes no Security Lake.

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

Fonte	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadados.versão
CloudTrail Eventos de dados Lambda	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail Eventos de gerenciamento	CloudTrail	AWS	Management	API Activity, Authentication ou Account Change	1.0.0-rc.2
CloudTrail Eventos de dados do S3	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.0.0-rc.2
CSPM do Security Hub	Security Hub CSPM	AWS	Corresponde ao valor ProductName_CSPM do Security Hub	Security Finding	1.0.0-rc.2
Logs de fluxo da 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.

Fonte	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadados.versão
CloudTrail Eventos de dados Lambda	`CloudTrail`	`AWS`	`Data`	`API Activity`	`1.1.0`
CloudTrail Eventos de gerenciamento	`CloudTrail`	`AWS`	`Management`	`API Activity, Authentication ou Account Change`	`1.1.0`
CloudTrail Eventos de dados do S3	`CloudTrail`	`AWS`	`Data`	`API Activity`	`1.1.0`
Route 53	`Route 53`	`AWS`	`Resolver Query Logs`	`DNS Activity`	`1.1.0`
CSPM do Security Hub	Corresponde ao AWS valor do formato de descoberta de segurança (ASFF) `ProductName`	Corresponde ao AWS valor do formato de descoberta de segurança (ASFF) `CompanyName`	Corresponde `featureName` ao valor do ASFF `ProductFields`	`Vulnerability Finding, Compliance Finding, or Detection Finding`	`1.1.0`
Logs de fluxo da VPC	`Amazon VPC`	`AWS`	`Flowlogs`	`Network Activity`	`1.1.0`

Fonte	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadados.versão
Registros de auditoria do EKS	`Amazon EKS`	`AWS`	`Elastic Kubernetes Service`	`API Activity`	`1.1.0`
AWS WAF Registros v2	`AWS WAF`	`AWS`	—	`HTTP Activity`	`1.1.0`

Integrações com o Security Lake

O Amazon Security Lake se integra a outros produtos Serviços da AWS e a produtos de terceiros. As integrações podem enviar dados para o Security Lake como fonte ou consumir dados no Security Lake como assinante. Os tópicos a seguir explicam quais produtos Serviços da AWS e produtos de terceiros se integram ao Security Lake.

Tópicos

AWS service (Serviço da AWS) integrações com Security Lake

O Amazon Security Lake se integra com outros Serviços da AWS. Um serviço pode operar como uma integração de fonte, uma integração de assinante ou ambas.

As integrações de fonte têm as seguintes propriedades:

- Enviar dados para o Security Lake
- Os dados chegam no esquema do Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake
- Os dados chegam no formato Apache Parquet

As integrações de assinantes podem acessar os dados do Security Lake de uma das seguintes formas:

- Leia os dados de origem do Security Lake por meio de um endpoint HTTPS
- Leia os dados de origem do Security Lake por meio de um Amazon Simple Queue Service (Amazon SQS)
- Ao consultar diretamente os dados de origem usando AWS Lake Formation

A tabela a seguir fornece uma lista das AWS service (Serviço da AWS) integrações suportadas pelo Security Lake.

AWS service (Serviço da AWS)	Tipo de integração	Description	Como funciona a integração
Amazon Bedrock	Assinante	Gere insights baseados em IA para analisar os dados do Security Lake.	Integração do Amazon Bedrock
Amazon Detective	Assinante	Analise, investigue e identifique rapidamente a causa raiz das descobertas de segurança ou atividades suspeitas consultando o Security Lake.	Integração do Amazon Detective
OpenSearch Serviço Amazon	Assinante	Gere insights de segurança a partir dos dados do Security Lake usando a ingestão de OpenSearch serviços.	Integração com OpenSearch o Amazon Service
Pipeline OpenSearch de ingestão de serviços da Amazon	Assinante, Fonte	Transmita registros, métricas e dados de rastreamento para o OpenSearch Service and Security Lake.	Integração do pipeline OpenSearch de ingestão de serviços da Amazon
OpenSearch Serviço Amazon Zero-ETL	Assinante (Consulta)	Consulte dados no Security Lake com zero ETL.	Integração de consulta direta com o Amazon OpenSearch Service Zero-ETL
Rápido	Assinante	Visualize, explore e interprete registros no	Integração rápida

AWS service (Serviço da AWS)	Tipo de integração	Description	Como funciona a integração
		Security Lake com o Quick.	
SageMaker IA da Amazon	Assinante	Gere insights baseados em IA para analisar os dados do Security Lake.	Integração com Amazon SageMaker AI
AWS AppFabric	Fonte	Ingere e normaliza os registros de aplicativos de software como serviço (SaaS) no formato padrão do Security Lake.	Integração do AWS AppFabric
AWS Security Hub CSPM	Fonte	Centralize e armazene as descobertas de segurança do Security Hub CSPM no formato padrão do Security Lake.	AWS Security Hub CSPM integração

Integração com o Amazon Bedrock

O Amazon Bedrock é um serviço totalmente gerenciado que disponibiliza modelos básicos de alto desempenho (FMs) das principais startups de IA e da Amazon para seu uso por meio de uma API unificada. Com a experiência sem servidor do Amazon Bedrock, você pode começar rapidamente, personalizar de forma privada os modelos básicos com seus próprios dados e integrá-los e implantá-los de forma fácil e segura em seus aplicativos usando AWS ferramentas sem precisar gerenciar nenhuma infraestrutura.

IA generativa

Você pode usar os recursos generativos de IA do Amazon Bedrock e a entrada de linguagem natural no SageMaker AI Studio para analisar dados no Security Lake e trabalhar para reduzir o risco da sua organização e aumentar sua postura de segurança. Você pode reduzir o tempo necessário para conduzir uma investigação identificando automaticamente as fontes de dados apropriadas, gerando e invocando consultas SQL e visualizando os dados de sua investigação. Para obter mais detalhes, consulte Gerar insights baseados em IA para o Amazon Security Lake usando o Amazon SageMaker AI Studio e o Amazon Bedrock.

Integração com o Amazon Detective

Tipo de integração: assinante

O Amazon Detective ajuda a analisar, investigar e identificar rapidamente a causa raiz de descobertas de segurança ou atividades suspeitas. O Detective coleta automaticamente dados de log dos seus recursos da AWS . Em seguida, ele usa machine learning, análises estatísticas e a teoria de grafos para gerar visualizações que ajudam a realizar investigações de segurança eficazes com maior rapidez. O Detective faz a pré-construção de agregações de dados, resumos e contexto predefinidos que podem ajudar você a analisar e determinar a natureza e a extensão de possíveis problemas de segurança.

Ao integrar o Security Lake e o Detective, você pode consultar os dados de log brutos armazenados pelo Security Lake a partir do Detective. Para obter mais informações, consulte Integração com o Amazon Security Lake.

Integração com o Amazon OpenSearch Service

Tipo de integração: assinante

O Amazon OpenSearch Service é um serviço gerenciado que facilita a implantação, operação e escalabilidade OpenSearch de clusters de serviços no Nuvem AWS. Usando a ingestão de OpenSearch serviços para ingerir dados em seu cluster OpenSearch de serviços, você pode obter insights mais rapidamente para investigações de segurança urgentes. Você pode responder rapidamente aos incidentes de segurança, ajudando a proteger os dados e sistemas essenciais da sua empresa.

OpenSearch Painel de serviços

Depois de integrar o OpenSearch Service com o Security Lake, você pode configurar o Security Lake para enviar dados de segurança de diferentes fontes para o OpenSearch Service por meio da ingestão de OpenSearch serviços sem servidor. Para obter mais informações sobre como configurar a ingestão de OpenSearch serviços para processar dados de segurança, consulte Gerar insights de segurança a partir dos dados do Amazon Security Lake usando o Amazon OpenSearch Service Ingestion.

Depois que o OpenSearch Service Ingestion começar a gravar seus dados em seu domínio OpenSearch de serviço. Para visualizar os dados usando os painéis pré-criados, navegue até os painéis e escolha qualquer um dos painéis instalados.

Integração com o pipeline OpenSearch de ingestão de serviços da Amazon

Tipo de integração: Assinante, Fonte

O Amazon OpenSearch Service Ingestion é um coletor de dados totalmente gerenciado e sem servidor que transmite registros, métricas e dados de rastreamento para OpenSearch o Service e o Security Lake.

Envie dados para o Security Lake usando o OpenSearch pipeline de ingestão

> Você pode usar um plug-in de coletor do Amazon Simple Storage Service (Amazon S3) OpenSearch na Ingestão para enviar dados de qualquer fonte compatível para o Security Lake. O Security Lake centraliza automaticamente os dados de segurança de AWS ambientes, ambientes locais e provedores de SaaS em um data lake específico. Para obter mais informações, consulte Como usar um pipeline OpenSearch de ingestão com o Amazon Security Lake como coletor.

Envie dados do Security Lake para OpenSearch usar o OpenSearch pipeline de ingestão

> Você pode usar um plug-in de origem do Amazon S3 para ingerir dados em seu OpenSearch pipeline de ingestão. Para obter mais informações, consulte Como usar um pipeline de OpenSearch ingestão com o Amazon Security Lake como fonte.

Integração com a consulta direta Zero-ETL do Amazon OpenSearch Service

Tipo de integração: Assinante (consulta)

Você pode usar a consulta direta do OpenSearch Service para analisar dados no Amazon Security Lake. OpenSearch O serviço fornece integração sem ETL como uma forma de consultar diretamente seus dados no Security Lake usando OpenSearch SQL ou OpenSearch Piped Processing Language (PPL) sem incorrer no atrito de criar pipelines de ingestão ou alternar entre ferramentas de análise. Essa abordagem elimina a necessidade de movimentação ou duplicação de dados, permitindo que você analise seus dados onde eles estão usando a experiência Discover em OpenSearch Service Dashboards. Quando quiser mudar da consulta de dados em repouso para o monitoramento ativo com painéis, você pode criar visualizações indexadas dos resultados da consulta e inseri-las em um índice de serviços. OpenSearch Para obter mais informações sobre consultas diretas, consulte Como trabalhar com consultas diretas no Amazon OpenSearch Service Developer Guide.

OpenSearch O serviço usa uma coleção OpenSearch sem servidor para consultar diretamente os dados no Security Lake e armazenar suas visualizações indexadas. Para fazer isso, você cria uma fonte de dados que permite usar recursos de OpenSearch ETL zero nos dados do Security Lake. Ao criar uma fonte de dados, você pode pesquisar diretamente, obter insights e analisar os dados armazenados no Security Lake. Você pode acelerar o desempenho da consulta e usar OpenSearch análises avançadas em conjuntos de dados selecionados do Security Lake usando indexação sob demanda.

- Para obter detalhes sobre a criação da integração da fonte de dados do OpenSearch Service, consulte Criação de uma integração de fonte de dados do Amazon Security Lake no Guia do desenvolvedor do Amazon OpenSearch Service.
- Para obter detalhes sobre a configuração da fonte de dados do Security Lake no OpenSearch Service, consulte Configurando uma fonte de dados do Security Lake em OpenSearch Service Dashboards no Amazon OpenSearch Service Developer Guide.

Para obter mais informações sobre como usar o OpenSearch Service with Security Lake, use os seguintes recursos.

- Apresentando a integração entre o Amazon OpenSearch Service e o Amazon Security Lake para simplificar a análise de segurança
- Introdução ao Zero-ETL em serviço OpenSearch com o Amazon Security Lake

Introdução ao Zero-ETL em serviço OpenSearch com o Amazon Security Lake

Integração com o Amazon Quick

Tipo de integração: assinante

O Amazon Quick é um serviço de inteligência de negócios (BI) em escala de nuvem que você pode usar para fornecer easy-to-understand insights às pessoas com quem você trabalha, onde quer que elas estejam. Conecta-se rapidamente aos seus dados na nuvem e combina dados de várias fontes diferentes. O Quick oferece aos tomadores de decisão a oportunidade de explorar e interpretar informações em um ambiente visual interativo. Eles têm acesso seguro a painéis de qualquer dispositivo em sua rede e de dispositivos móveis.

Painel rápido

Para visualizar seus dados do Amazon Security Lake no Quick, criar os AWS objetos necessários e implantar fontes de dados básicas, conjuntos de dados, análises, painéis e grupos de usuários no Quick com relação ao Security Lake. Para obter instruções detalhadas, consulte Integração com o Amazon Quick.

Para obter mais informações sobre a visualização de dados do Security Lake com o Quick, consulte os recursos a seguir.

Visualizando dados do Security Lake com o Quick: série de aprendizado rápido de 2024

Operacionalize os registros do AWS WAF Web ACL com o Security Lake

Integração com Amazon SageMaker AI

Tipo de integração: assinante

O Amazon SageMaker AI é um serviço de aprendizado de máquina (ML) totalmente gerenciado. Com o Security Lake, cientistas de dados e desenvolvedores podem criar, treinar e implantar modelos de ML com rapidez e confiança em um ambiente hospedado pronto para produção. Ele fornece uma experiência de interface de usuário para executar fluxos de trabalho de ML que disponibiliza as ferramentas de SageMaker AI ML em vários ambientes de desenvolvimento integrados (IDEs).

SageMaker Insights de IA

Você pode gerar insights de aprendizado de máquina para o Security Lake usando o SageMaker AI Studio. Este estúdio é um ambiente de desenvolvimento integrado da web (IDE) para aprendizado de máquina que fornece ferramentas para cientistas de dados prepararem, criarem, treinarem e implantarem modelos de aprendizado de máquina. Com essa solução, você pode implantar rapidamente um conjunto básico de notebooks Python com foco nas AWS Security Hub

CSPMdescobertas no Security Lake, que também pode ser expandido para incorporar outras AWS fontes ou fontes de dados personalizadas no Security Lake. Para obter mais detalhes, consulte Gerar insights de aprendizado de máquina para dados do Amazon Security Lake usando a Amazon SageMaker AI.

Integração com AWS AppFabric

Tipo de integração: fonte

AWS AppFabricé um serviço sem código que conecta aplicativos de software como serviço (SaaS) em toda a sua organização, ou seja, aplicativos de TI e segurança usando um esquema padrão e um repositório central.

Como o Security Lake recebe AppFabric as descobertas

Você pode enviar dados de log de AppFabric auditoria para o Security Lake selecionando o Amazon Kinesis Data Firehose como destino e configurando o Kinesis Data Firehose para entregar dados no esquema OCSF e no formato Apache Parquet para o Security Lake.

Pré-requisitos

Antes de enviar registros de AppFabric auditoria para o Security Lake, você deve enviar seus registros de auditoria normalizados do OCSF para um stream do Kinesis Data Firehose. Em seguida, você pode configurar o Kinesis Data Firehose para enviar a saída para seu bucket do Amazon S3 do Security Lake. Para obter mais informações, consulte Escolher o Amazon S3 como seu destino no Guia do desenvolvedor do Amazon Kinesis.

Envie suas AppFabric descobertas para o Security Lake

Para enviar registros de AppFabric auditoria para o Security Lake após concluir o pré-requisito anterior, você deve habilitar os dois serviços e adicioná-los AppFabric como fonte personalizada no Security Lake. Para obter instruções sobre como adicionar uma fonte personalizada, consulte Coletando dados de fontes personalizadas no Security Lake.

Pare de receber AppFabric registros no Security Lake

Para parar de receber registros de AppFabric auditoria, você pode usar o console do Security Lake, a API do Security Lake ou AWS CLI excluir AppFabric como uma fonte personalizada. Para instruções, consulte Excluindo uma fonte personalizada de Security Lake.

Integração com AWS Security Hub CSPM

Tipo de integração: fonte

AWS Security Hub CSPMfornece uma visão abrangente do seu estado de segurança AWS e ajuda seu ambiente em relação aos padrões e às melhores práticas do setor de segurança. O Security Hub CSPM coleta dados de segurança de vários Contas da AWS serviços e produtos de parceiros terceirizados compatíveis e ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade.

Quando você ativa o CSPM do Security Hub e adiciona as descobertas do CSPM do Security Hub como fonte no Security Lake, o Security Hub CSPM começa a enviar novas descobertas e atualizações das descobertas existentes para o Security Lake.

Como o Security Lake recebe as descobertas do CSPM do Security Hub

No CSPM do Security Hub, os problemas de segurança são rastreados como descobertas. Algumas descobertas vêm de problemas detectados por outros parceiros Serviços da AWS ou por parceiros terceirizados. O Security Hub CSPM também gera suas próprias descobertas executando verificações de segurança automatizadas e contínuas em relação às regras. As regras são representadas por controles de segurança.

Todas as descobertas no CSPM do Security Hub usam um formato JSON padrão chamado Formato de Descobertas de Segurança da AWS (ASFF).

O Security Lake recebe as descobertas do CSPM do Security Hub e as transforma em. Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake

Envie suas descobertas de CSPM do Security Hub para o Security Lake

Para enviar as descobertas do CSPM do Security Hub para o Security Lake, você deve habilitar os dois serviços e adicionar as descobertas do CSPM do Security Hub como uma fonte no Security Lake. Para obter instruções sobre como adicionar uma AWS fonte, consulteAdicionando um AWS service (Serviço da AWS) como fonte.

Se você quiser que o Security Hub CSPM gere descobertas de controle e as envie para o Security Lake, você deve habilitar os padrões de segurança relevantes e ativar o registro de recursos em uma base regional em. AWS Config Para mais informações, consulte Habilitar e configurar o AWS Config no Guia do usuário do AWS Security Hub .

Pare de receber as descobertas do CSPM do Security Hub no Security Lake

Para parar de receber as descobertas do Security Hub CSPM, você pode usar o console CSPM do Security Hub, a API CSPM do Security Hub ou os seguintes tópicos AWS CLI no Guia do Usuário:AWS Security Hub

- Desabilitar e habilitar o fluxo de descobertas em uma integração (console)
- Desabilitando o fluxo de descobertas de uma integração (API do Security Hub, AWS CLI)

Integrações de terceiros com o Security Lake

O Amazon Security Lake se integra com vários provedores de terceiros. Um provedor pode oferecer uma integração de fonte, uma integração de assinante ou uma integração de serviço. Os provedores podem oferecer um ou mais tipos de integração.

As integrações de fonte têm as seguintes propriedades:

- Enviar dados para o Security Lake
- Os dados chegam no formato Apache Parquet
- Os dados chegam no esquema do Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake

As integrações de assinante têm as seguintes propriedades:

- Leia os dados de origem do Security Lake em um endpoint HTTPS ou na fila do Amazon Simple Queue Service (Amazon SQS) ou consultando diretamente os dados de origem do AWS Lake Formation
- Pode ler dados no formato Apache Parquet
- Pode ler dados no esquema do OCSF

As integrações de serviços podem ajudá-lo a implementar o Security Lake e outros Serviços da AWS em sua organização. Eles também podem fornecer assistência com relatórios, análises e outros casos de uso.

Para pesquisar um fornecedor parceiro específico, consulte o Localizador de Soluções de Parceiro. Para comprar um produto de terceiros, consulte o AWS Marketplace.

Para solicitar a inclusão como uma integração de parceiros ou se tornar um parceiro do Security Lake, envie um e-mail para <securitylake-partners@amazon.com>.

Se você usa integrações de terceiros que enviam descobertas para AWS Security Hub CSPM, você também pode revisar essas descobertas no Security Lake se a integração CSPM do Security Hub para o Security Lake estiver habilitada. Para obter informações sobre como habilitar a integração, consulte Integração com AWS Security Hub CSPM. Para obter uma lista de integrações de terceiros que enviam descobertas para o Security Hub CSPM, consulte Integrações de produtos de parceiros terceirizados disponíveis no Guia do Usuário.AWS Security Hub

Antes de configurar seus assinantes, verifique o suporte de registro do OCSF do seu assinante. Para obter os detalhes mais recentes, revise a documentação do seu assinante.

Integração de consultas

Você pode consultar os dados que o Security Lake armazena em AWS Lake Formation bancos de dados e tabelas. Você também pode criar assinantes terceirizados no console, na API ou no console do Security Lake AWS Command Line Interface.

O administrador do data lake do Lake Formation deve conceder permissões `SELECT` nos bancos de dados e tabelas relevantes à identidade do IAM que consulta os dados. Você deve criar um assinante no Security Lake antes de consultar os dados. Para obter mais informações sobre como criar um assinante com acesso a consultas, consulte Gerenciando o acesso de consulta para assinantes do Security Lake.

Você pode configurar a integração de consultas com o Security Lake para os seguintes parceiros terceirizados.

- Cribl – Search
- IBM – QRadar
- Palo Alto Networks – XSOAR
- Query.AI – Query Federated Search
- SOC Prime
- Splunk – Federated Analytics
- Tego Cyber

Accenture – MxDR

Tipo de integração: assinante, serviço

A integração do MxDR da Accenture's com o Security Lake oferece ingestão de dados em tempo real de logs e eventos, detecção gerenciada de anomalias, busca de ameaças e operações de segurança. Isso ajuda na análise e na detecção e resposta gerenciadas (MDR).

Como integração de serviço, a Accenture também pode ajudar a implementar o Security Lake em sua organização.

Documentação de integração

Aqua Security

Tipo de integração: fonte

O Aqua Security pode ser adicionado como uma fonte personalizada para enviar eventos de auditoria ao Security Lake. Os eventos de auditoria são convertidos no esquema do OCSF e no formato Parquet.

Documentação de integração

Barracuda – Email Protection

Tipo de integração: fonte

O Barracuda Email Protection pode enviar eventos para o Security Lake quando novos ataques de phishing por e-mail são detectados. Você pode receber esses eventos junto com outros dados de segurança em seu data lake.

Documentação de integração

Booz Allen Hamilton

Tipo de integração: serviços

Como integração de serviço, o Booz Allen Hamilton usa uma abordagem baseada em dados para a segurança cibernética, combinando dados e análises com o serviço Security Lake.

Link do parceiro

Bosch Software and Digital Solutions – AIShield

Tipo de integração: fonte

AIShieldA powered by Bosch fornece análise automatizada de vulnerabilidades e proteção de terminais para ativos de IA por meio de sua integração com o Security Lake.

Documentação de integração

ChaosSearch

Tipo de integração: assinante

ChaosSearchoferece acesso a dados de vários modelos para usuários com sistemas abertos APIs , como Elasticsearch e SQL, ou com o Kibana e o Superset incluídos nativamente. UIs Você pode consumir seus dados do Security Lake no ChaosSearch sem limites de retenção para monitorar, alertar e caçar ameaças. Isso ajuda você a enfrentar os complexos ambientes de segurança atuais e as ameaças persistentes.

Documentação de integração

Cisco Security – Secure Firewall

Tipo de integração: fonte

Ao integrar o Cisco Secure Firewall com o Security Lake, é possível armazenar logs de firewall de forma estruturada e escalável. O cliente eNcore da Cisco transmite logs de firewall do Firewall Management Center, realiza a conversão do esquema para o esquema do OCSF e os armazena no Security Lake.

Documentação de integração

Claroty – xDome

Tipo de integração: fonte

O Claroty xDome envia alertas detectados nas redes para o Security Lake com configuração mínima. As opções de implantação flexíveis e rápidas ajudam a xDome proteger ativos estendidos da Internet das Coisas (XIoT), que consistem em ativos de IIo IoT, T e BMS, em sua rede, enquanto detectam automaticamente os primeiros indicadores de ameaças.

Documentação de integração

CMD Solutions

Tipo de integração: serviços

A CMD Solutions ajuda as empresas a aumentar sua agilidade integrando a segurança de forma precoce e contínua por meio de processos de design, automação e garantia contínua. Como integração de serviço, a CMD Solutions pode ajudar a implementar o Security Lake em sua organização.

Link do parceiro

Confluent – Amazon S3 Sink Connector

Tipo de integração: fonte

A Confluent conecta, configura e orquestra automaticamente as integrações de dados com conectores pré-criados e totalmente gerenciados. O Confluent S3 Sink Connector permite que você insira dados brutos no Security Lake em escala no formato Parquet nativo.

Documentação de integração

Contrast Security

Tipo de integração: fonte

Produto parceiro para a integração: Contrast Assess

Contrast Security Assessé uma ferramenta IAST que oferece detecção de vulnerabilidades em tempo real em aplicativos da web e microsserviços. APIs O Assess se integra ao Security Lake para ajudar a fornecer visibilidade centralizada de todas as suas workloads.

Documentação de integração

Cribl – Search

Tipo de integração: assinante

Você pode usar o Cribl Search para pesquisar dados do Security Lake.

Documentação de integração

Cribl – Stream

Tipo de integração: fonte

Você pode usar o Cribl Stream para enviar dados de qualquer fonte de terceiros compatível com Cribl para o Security Lake no esquema do OCSF.

Documentação de integração

CrowdStrike – Falcon Data Replicator

Tipo de integração: fonte

Essa integração extrai dados do CrowdStrike Falcon Data Replicator em streaming contínuo, transforma os dados no esquema do OCSF e os envia para o Security Lake.

Documentação de integração

CrowdStrike – Next Gen SIEM

Tipo de integração: assinante

Simplifique a ingestão de dados do Security Lake com o conector de CrowdStrike Falcon Next-Gen SIEM dados com analisadores de esquema OCSF nativos. Falcon NG SIEMrevoluciona a detecção, a investigação e a resposta a ameaças ao reunir profundidade e amplitude de segurança incomparáveis em uma plataforma unificada para impedir violações.

Documentação de integração

CyberArk – Unified Identify Security Platform

Tipo de integração: fonte

CyberArk Audit Adapter, uma AWS Lambda função, coleta eventos de segurança CyberArk Identity Security Platform e envia os dados para o Security Lake no esquema OCSF.

Documentação de integração

Cyber Security Cloud – Cloud Fastener

Tipo de integração: assinante

CloudFasteneraproveita o Security Lake para facilitar a consolidação dos dados de segurança de seus ambientes em nuvem.

Documentação de integração

DataBahn

Tipo de integração: fonte

Centralize seus dados de segurança no Security Lake usando o DataBahn's Security Data Fabric.

Documentação de integração (entre no portal do DataBahn para revisar a documentação)

Darktrace – Cyber AI Loop

Tipo de integração: fonte

A integração do Darktrace com o Security Lake traz o poder do autoaprendizado do Darktrace para o Security Lake. Os insights do Cyber AI Loop podem ser correlacionados com outros fluxos de dados e elementos da pilha de segurança da sua organização. A integração registra violações do modelo do Darktrace como descobertas de segurança.

Documentação de integração (entre no portal do Darktrace para revisar a documentação)

Datadog

Tipo de integração: assinante

Datadog Cloud SIEMdetecta ameaças em tempo real ao seu ambiente de nuvem, incluindo dados no Security Lake, e unifica DevOps as equipes de segurança em uma única plataforma.

Documentação de integração

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

Tipo de integração: assinante, serviço

O Deloitte MXDR CAE ajuda você a armazenar, analisar e visualizar rapidamente seus dados de segurança padronizados. O pacote CAE de recursos personalizados de análise, IA e ML fornece automaticamente insights acionáveis com base em modelos que são executados em dados formatados em OCSF no Security Lake.

Como integração de serviço, a Deloitte também pode ajudá-lo a implementar o Security Lake em sua organização.

Documentação de integração

Devo

Tipo de integração: assinante

O Devo coletor para AWS suporte à ingestão do Security Lake. Essa integração pode ajudá-lo a analisar e abordar uma variedade de casos de uso de segurança, como detecção de ameaças, investigação e resposta a incidentes.

Documentação de integração

DXC – SecMon

Tipo de integração: assinante, serviço

O DXC SecMon coleta eventos de segurança do Security Lake e os monitora para detectar e alertar sobre possíveis ameaças à segurança. Isso ajuda as organizações a entender melhor sua postura de segurança e a identificar e responder proativamente às ameaças.

Como integração de serviço, a DXC também pode ajudá-lo a implementar o Security Lake em sua organização.

Documentação de integração

Eviden – AIsaac (antigo Atos)

Tipo de integração: assinante

A plataforma AIsaac MDR consome logs de fluxo da VPC que foram ingeridos no esquema do OCSF no Security Lake e utiliza modelos de IA para detectar ameaças.

Documentação de integração

ExtraHop – Reveal(x) 360

Tipo de integração: fonte

Você pode aprimorar a segurança da carga de trabalho e dos aplicativos integrando dados de rede, incluindo detecções de, de IOCsExtraHop Reveal(x) 360, até o Security Lake no esquema OCSF

Documentação de integração

Falcosidekick

Tipo de integração: fonte

O Falcosidekick coleta e envia eventos do Falco para o Security Lake. Essa integração exporta eventos de segurança usando o esquema do OCSF.

Documentação de integração

Fortinet - Cloud Native Firewall

Tipo de integração: fonte

Ao criar instâncias FortiGate CNF em AWS, você pode especificar o Amazon Security Lake como um destino de saída de log.

Documentação de integração

Gigamon – Application Metadata Intelligence

Tipo de integração: fonte

O Gigamon Application Metadata Intelligence (AMI) capacita suas ferramentas de observabilidade, SIEM e monitoramento de desempenho de rede com atributos críticos de metadados. Isso ajuda a fornecer uma visibilidade mais profunda da aplicação para que você possa identificar gargalos de desempenho, problemas de qualidade e possíveis riscos à segurança da rede.

Documentação de integração

Hoop Cyber

Tipo de integração: serviços

O Hoop Cyber FastStart inclui avaliação, priorização e integração de fonte de dados e ajuda os clientes a consultar seus dados com ferramentas e integrações existentes oferecidas pelo Security Lake.

Link do parceiro

HTCD – AI-First Cloud Security Platform

Tipo de integração: assinante

Obtenha automação instantânea de conformidade, priorização de descobertas de segurança e patches personalizados. O HTCD pode consultar o Security Lake para ajudá-lo a descobrir ameaças com consultas em linguagem natural e insights baseados em IA.

Documentação de integração

IBM – QRadar

Tipo de integração: assinante

O IBM Security QRadar SIEM with UAX integra o Security Lake a uma plataforma de análise que identifica e evita ameaças em nuvens híbridas. Essa integração oferece suporte a acesso a dados e acesso de consulta.

Documentação de integração sobre o consumo de AWS CloudTrail registros

Documentação de integração sobre o uso do Amazon Athena para consultas

Infosys

Tipo de integração: serviços

A Infosys ajuda você a personalizar a implementação do Security Lake conforme as suas necessidades organizacionais e fornece insights personalizados.

Link do parceiro

Insbuilt

Tipo de integração: serviços

A Insbuilt é especializada em serviços de consultoria em nuvem e pode ajudá-lo a entender como implementar o Security Lake em sua organização.

Link do parceiro

Kyndryl – AIOps

Tipo de integração: assinante, serviço

O Kyndryl se integra ao Security Lake para fornecer interoperabilidade de dados cibernéticos, inteligência de ameaças e análises baseadas em IA. Como assinante de acesso a dados, Kyndryl ingere eventos AWS CloudTrail de gerenciamento do Security Lake para fins de análise.

Como integração de serviço, a Kyndryl também pode ajudá-lo a implementar o Security Lake em sua organização.

Documentação de integração

Lacework – Polygraph

Tipo de integração: fonte

Lacework Polygraph® Data Platformintegra-se ao Security Lake como fonte de dados e fornece descobertas de segurança sobre vulnerabilidades, configurações incorretas e ameaças conhecidas e desconhecidas em todo o seu ambiente. AWS

Documentação de integração

Laminar

Tipo de integração: fonte

O Laminar envia eventos de segurança de dados para o Security Lake no esquema do OCSF, disponibilizando-os para casos de uso de análises adicionais, como resposta a incidentes e investigação.

Documentação de integração

MegazoneCloud

Tipo de integração: serviços

A MegazoneCloud é especializada em serviços de consultoria em nuvem e pode ajudá-lo a entender como implementar o Security Lake em sua organização. Conectamos o Security Lake com soluções ISV integradas para criar tarefas personalizadas e criar insights personalizados relacionados às necessidades do cliente.

Documentação de integração

Monad

Tipo de integração: fonte

O Monad transforma automaticamente seus dados em esquema do OCSF e os envia para o data lake do Security Lake.

Documentação de integração

NETSCOUT – Omnis Cyber Intelligence

Tipo de integração: fonte

Ao se integrar ao Security Lake, o NETSCOUT torna-se uma fonte personalizada de descobertas de segurança e insights de segurança detalhados sobre o que está acontecendo em sua empresa, como ameaças cibernéticas, riscos de segurança e mudanças na superfície de ataque. Essas descobertas são produzidas na conta do cliente por NETSCOUT CyberStreams e Omnis Cyber Intelligence, em seguida, enviadas ao Security Lake no esquema OCSF. Os dados ingeridos também atendem a outros requisitos e às melhores práticas para uma fonte do Security Lake, incluindo formato, esquema, particionamento e aspectos relacionados ao desempenho.

Documentação de integração

Netskope – CloudExchange

Tipo de integração: fonte

Netskopeajuda você a fortalecer sua postura de segurança compartilhando registros relacionados à segurança e informações sobre ameaças com o Security Lake. Netskopeas descobertas são enviadas ao Security Lake com um CloudExchange plug-in, que pode ser lançado como um ambiente baseado em docker dentro AWS ou em um data center local.

Documentação de integração

New Relic ONE

Tipo de integração: assinante

O New Relic ONE é uma aplicação de assinante baseado em Lambda. Ele é implantado em sua conta, acionado pelo Amazon SQS e envia dados para o New Relic usando chaves de licença do New Relic

Documentação de integração

Okta – Workforce Identity Cloud

Tipo de integração: fonte

Oktaenvia registros de identidade para o Security Lake no esquema OCSF por meio de uma integração com a Amazon. EventBridge Okta System Logsno esquema OCSF, ajudará as equipes de cientistas de dados e de segurança a consultar eventos de segurança por meio de um padrão de código aberto. A geração de logs padronizados em OCSF do Okta ajuda você a realizar atividades de auditoria e gerar relatórios relacionados à autenticação, autorização, alterações de conta e alterações de entidade em um esquema consistente.

Documentação de integração

AWS CloudFormation modelo para adicionar Okta como fonte personalizada no Security Lake

Orca – Cloud Security Platform

Tipo de integração: fonte

A plataforma de segurança em nuvem Orca sem agente AWS se integra ao Security Lake enviando eventos de Detecção e Resposta de Nuvem (CDR) no esquema OCSF.

Documentação de integração (entre no portal do Orca para revisar a documentação)

Palo Alto Networks – Prisma Cloud

Tipo de integração: fonte

Palo Alto Networks Prisma Cloudagrega dados de detecção de vulnerabilidades VMs em seus ambientes nativos da nuvem e os envia para o Security Lake.

Documentação de integração

Palo Alto Networks – XSOAR

Tipo de integração: Assinante

Palo Alto Networks XSOARcriou uma integração de assinantes com o XSOAR e o Security Lake.

Documentação de integração

Panther

Tipo de integração: assinante

Panthersuporta a ingestão de registros do Security Lake para uso em pesquisa e detecção.

Documentação de integração

Ping Identity – PingOne

Tipo de integração: fonte

O PingOne envia alertas de modificação da conta para o Security Lake no esquema do OCSF e no formato Parquet, permitindo que você descubra e direcione sua ação conforme as alterações da conta.

Documentação de integração

PwC – Fusion center

Tipo de integração: assinante, serviço

A PwC traz conhecimento e experiência para ajudar os clientes na implementação de um centro de fusão para atender às suas necessidades individuais. Integrado ao Amazon Security Lake, um centro de fusão oferece a capacidade de combinar dados de várias fontes para criar uma visão centralizada e quase em tempo real.

Documentação de integração

Query.AI – Query Federated Search

Tipo de integração: assinante

Query Federated Searchpode consultar diretamente qualquer tabela do Security Lake via Amazon Athena para apoiar a resposta a incidentes, investigações, busca de ameaças e pesquisa geral em uma variedade de observáveis, eventos e objetos no esquema OCSF.

Documentação de integração

Rapid7 – InsightIDR

Tipo de integração: assinante

InsightIDR, a Rapid7 SIEM/XDR solução, pode ingerir registros no Security Lake para detecção de ameaças e investigação de atividades suspeitas.

Documentação de integração

RipJar – Labyrinth for Threat Investigations

Tipo de integração: assinante

O Labyrinth for Threat Investigations fornece uma abordagem corporativa para a exploração de ameaças em escala com base na fusão de dados, com segurança refinada, fluxos de trabalho adaptáveis e relatórios.

Documentação de integração

Sailpoint

Tipo de integração: fonte

Produto parceiro para a integração: SailPoint IdentityNow

Essa integração permite que os clientes transformem dados de eventos do SailPoint IdentityNow. A integração tem como objetivo fornecer um processo automatizado para trazer a atividade do usuário e os eventos de governança do IdentityNow para o Security Lake para melhorar os insights dos produtos de monitoramento de incidentes e eventos de segurança.

Documentação de integração

Securonix

Tipo de integração: assinante

O Securonix Next-Gen SIEM se integra ao Security Lake, capacitando as equipes de segurança a ingerir dados mais rapidamente e a expandir os recursos de detecção e resposta.

Documentação de integração

SentinelOne

Tipo de integração: assinante

A plataforma SentinelOne Singularity™ XDR estende a detecção e a resposta em tempo real às workloads de endpoint, identidade e nuvem em execução on-premises e em infraestrutura de nuvem pública, incluindo o Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Kubernetes Service (Amazon EKS).

Documentação de integração (entre no portal do SentinelOne para revisar a documentação)

Sentra – Data Lifecyle Security Platform

Tipo de integração: fonte

Depois de implantar a infraestrutura de digitalização do Sentra em sua conta, o Sentra busca as descobertas e as ingere em seu SaaS. Essas descobertas são metadados que o Sentra armazena e, posteriormente, transmite para o Security Lake no esquema do OCSF para consulta.

Documentação de integração

SOC Prime

Tipo de integração: assinante

SOC Primese integra ao Security Lake por meio do Amazon OpenSearch Service e do Amazon Athena para facilitar a orquestração inteligente de dados e a busca por ameaças com base em marcos de confiança zero. SOC Primecapacita as equipes de segurança a aumentar a visibilidade das ameaças e investigar incidentes sem um grande volume de alertas. Você pode economizar tempo de desenvolvimento com regras e consultas reutilizáveis que são automaticamente conversíveis em Athena OpenSearch e Service no esquema OCSF.

Documentação de integração

Splunk

Tipo de integração: assinante

O Splunk AWS complemento para Amazon Web Services (AWS) suporta a ingestão do Security Lake. Essa integração ajuda você a acelerar a detecção, a investigação e a resposta a ameaças assinando dados no esquema do OCSF do Security Lake.

Documentação de integração

Stellar Cyber

Tipo de integração: assinante

O Stellar Cyber consome logs do Security Lake e adiciona os logs ao data lake do Stellar Cyber. Esse conector usa o esquema OCSF.

Documentação de integração

Sumo Logic

Tipo de integração: assinante

Sumo Logicconsome dados do Security Lake e fornece ampla visibilidade em ambientes AWS de nuvem híbrida e no local. O Sumo Logic oferece às equipes de segurança visibilidade abrangente, automação e monitoramento de ameaças em todas as suas ferramentas de segurança.

Documentação de integração

Swimlane – Turbine

Tipo de integração: assinante

O Swimlane ingere dados do Security Lake no esquema do OCSF e os envia por meio de manuais de low-code e gerenciamento de casos para facilitar a detecção de ameaças, a investigação e a resposta a incidentes mais rápidas.

Documentação de integração (entre no portal do Swimlane para revisar a documentação)

Sysdig Secure

Tipo de integração: fonte

Sysdig Secure'sa plataforma de proteção de aplicativos nativa em nuvem (CNAPP) envia eventos de segurança ao Security Lake para maximizar a supervisão, agilizar as investigações e simplificar a conformidade.

Documentação de integração

Talon

Tipo de integração: fonte

Produto parceiro para integração: Talon Enterprise Browser

O Talon's Enterprise Browser, um ambiente de endpoint seguro e isolado baseado em navegador, envia ao Talon acesso, proteção de dados, ações de SaaS e eventos de segurança para o Security Lake, fornecendo visibilidade e opção de correlação cruzada de eventos para detecção, análise forense e investigações.

Documentação de integração (entre no portal do Talon para revisar a documentação)

Tanium

Tipo de integração: fonte

A plataforma Tanium Unified Cloud Endpoint Detection, Management, and Security fornece dados de inventário para o Security Lake no esquema do OCSF.

Documentação de integração

TCS

Tipo de integração: serviços

O TCS AWS Business Unit oferece inovação, experiência e talento. Essa integração é impulsionada por uma década de criação conjunta de valor, profundo conhecimento do setor, experiência em tecnologia e sabedoria de entrega. Como integração de serviço, a TCS pode ajudá-lo a implementar o Security Lake em sua organização.

Documentação de integração

Tego Cyber

Tipo de integração: assinante

O Tego Cyber se integra ao Security Lake para ajudar a detectar e investigar rapidamente possíveis ameaças à segurança. Ao correlacionar diversos indicadores de ameaças em extensos prazos e origem de log, a Tego Cyber descobre ameaças ocultas. A plataforma é enriquecida com inteligência

de ameaças altamente contextual, fornecendo precisão e insight na detecção de ameaças e investigações.

Documentação de integração

Tines – No-code security automation

Tipo de integração: assinante

O Tines No-code security automation ajuda você a tomar decisões mais precisas aproveitando os dados de segurança centralizados no Security Lake.

Documentação de integração

Torq – Enterprise Security Automation Platform

Tipo de integração: fonte, assinante

O Torq se integra perfeitamente ao Security Lake como fonte personalizada e assinante. O Torq ajuda você a implementar automação e orquestração em escala empresarial com uma plataforma simples sem código.

Documentação de integração

Trellix – XDR

Tipo de integração: fonte, assinante

Como uma plataforma XDR aberta, o Trellix XDR suporta a integração do Security Lake. O Trellix XDR pode aproveitar dados no esquema do OCSF para casos de uso de análise de segurança. Você também pode aumentar seu data lake do Security Lake com mais de 1.000 fontes de eventos de segurança do Trellix XDR. Isso ajuda você a ampliar os recursos de detecção e resposta para seu AWS ambiente. Os dados ingeridos são correlacionados a outros riscos de segurança, fornecendo os manuais necessários para responder a um risco em tempo hábil.

Documentação de integração

Trend Micro – CloudOne

Tipo de integração: fonte

O Trend Micro CloudOne Workload Security envia as seguintes informações das instâncias do Amazon Elastic Compute Cloud (EC2) ao Security Lake:

- Atividade de consulta ao DNS
- Atividade de arquivos
- Atividade de rede
- Atividade de processos
- Atividade de valores de registro
- Atividade de contas de usuário

Documentação de integração

Uptycs – Uptycs XDR

Tipo de integração: fonte

O Uptycs envia uma grande quantidade de dados no esquema do OCSF de ativos on-premises e na nuvem para o Security Lake. Os dados incluem detecções de ameaças comportamentais de workloads de endpoints e de nuvem, detecções de anomalias, violações de políticas, políticas arriscadas, configurações incorretas e vulnerabilidades.

Documentação de integração

Vectra AI – Vectra Detect for AWS

Tipo de integração: fonte

Ao usarVectra Detect for AWS, você pode enviar alertas de alta fidelidade para o Security Lake como uma fonte personalizada usando um modelo dedicado CloudFormation .

Documentação de integração

VMware Aria Automation for Secure Clouds

Tipo de integração: fonte

Com essa integração, é possível detectar configurações incorretas na nuvem e enviá-las ao Security Lake para análise avançada.

Documentação de integração

Wazuh

Tipo de integração: assinante

O Wazuh visa lidar com os dados do usuário com segurança, fornecer acesso às consultas para cada fonte e otimizar os custos de consulta.

Documentação de integração

Wipro

Tipo de integração: fonte, serviço

Essa integração permite que você colete dados da plataforma Wipro Cloud Application Risk Governance (CARG) para fornecer uma visão unificada de suas aplicações em nuvem e posturas de conformidade em toda a empresa.

Como integração de serviço, a Wipro também pode ajudá-lo a implementar o Security Lake em sua organização.

Documentação de integração

Wiz – CNAPP

Tipo de integração: fonte

A integração entre o Security Lake e o Wiz facilita a coleta de dados de segurança na nuvem em um único data lake de segurança, aproveitando o esquema OCSF, um padrão de código aberto projetado para troca de dados de segurança extensível e normalizada.

Documentação de integração (entre no portal do Wiz para revisar a documentação)

Zscaler – Zscaler Posture Control

Tipo de integração: fonte

O Zscaler Posture Control™, uma plataforma de proteção de aplicativos nativos de nuvem, envia descobertas de segurança para o Security Lake no esquema OCSF.

Documentação de integração

Segurança em Security Lake

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O Modelo de Responsabilidade Compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Security Lake, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Security Lake. Os tópicos a seguir mostram como configurar o Security Lake para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Security Lake.

Tópicos

Gerenciamento de identidade e acesso para Security Lake

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar recursos do Security Lake. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso do Amazon Security Lake).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como o Security Lake funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para Security Lake)

Autenticação com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Security Lake funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Security Lake, saiba quais recursos do IAM estão disponíveis para uso com o Security Lake.

Atributos do IAM que você pode usar com o Amazon Security Lake

Recurso do IAM	Suporte ao Security Lake
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Perfis vinculados ao serviço	Sim

Para ter uma visão de alto nível de como o Security Lake e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para Security Lake

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

O Security Lake é compatível com políticas baseadas em identidade. Para obter mais informações, consulte Exemplos de políticas baseadas em identidade para Security Lake.

Políticas baseadas em recursos no Security Lake

Compatível com políticas baseadas em recursos: sim

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

O serviço Security Lake cria políticas baseadas em recursos para os buckets do Amazon S3 que armazenam seus dados. Você não anexa essas políticas baseadas em recursos aos seus buckets do S3. O Security Lake cria automaticamente essas políticas em seu nome.

Um exemplo de recurso é um bucket do S3 com um nome do recurso da Amazon (ARN) de `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`. Neste exemplo, `region` é um Região da AWS local específico em que você ativou o Security Lake e `bucket-identifier` é uma sequência alfanumérica regionalmente exclusiva que o Security Lake atribui ao bucket. O Security Lake cria o bucket S3 para armazenar dados dessa região. A política de

recursos define quais entidades principais podem realizar ações no bucket. Aqui está um exemplo de política baseada em recursos (política de bucket) que o Security Lake anexa ao bucket:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        },
        {
            "Sid": "PutSecurityLakeObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "securitylake.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
```

```
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-
east-1:111122223333:*"
                }
            }
        }
    ]
}
```

Para obter mais informações sobre as políticas de acesso baseadas em recursos, consulte Políticas baseadas em identidade e em recursos no Guia do usuário do IAM.

Ações da política para Security Lake

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para obter uma lista de ações do Security Lake, consulte Ações definidas pelo Amazon Security Lake na Referência de autorização do serviço.

As ações de políticas no Security Lake usam o seguinte prefixo antes da ação:

```
securitylake
```

Por exemplo, para conceder permissão a um usuário para acessar informações sobre um assinante específico, inclua a ação `securitylake:GetSubscriber` na política atribuída a esse usuário. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Security Lake define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "securitylake:action1",
```

```
      "securitylake:action2"
]
```

Para visualizar exemplos de políticas baseadas em identidade do Security Lake, consulte Exemplos de políticas baseadas em identidade para Security Lake.

Recursos de políticas para Security Lake

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

O Security Lake define os seguintes tipos de recursos: assinante e a configuração do data lake para um Conta da AWS em um determinado Região da AWS. Você pode especificar esses tipos de recursos nas políticas usando ARNs.

Para obter uma lista dos tipos de recursos do Security Lake e a sintaxe dos ARNs para cada um, consulte Tipos de recursos definidos pelo Amazon Security Lake na Referência de autorização do serviço. Para saber quais ações você pode especificar para cada tipo de recurso, consulte Ações definidas pelo Amazon Security Lake na Referência de autorização do serviço.

Para visualizar exemplos de políticas baseadas em identidade do Security Lake, consulte Exemplos de políticas baseadas em identidade para Security Lake.

Chaves de condição de política do Security Lake

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para obter uma lista de chaves de condição do Security Lake, consulte Chaves de condição do Amazon Security Lake na Referência de autorização do serviço. Para saber com que ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon Security Lake na Referência de autorização do serviço. Para obter exemplos de políticas que usam chaves de condição, consulte Exemplos de políticas baseadas em identidade para Security Lake.

Listas de controle de acesso (ACLs) no Security Lake

Suportes ACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Security Lake não oferece suporte ACLs, o que significa que você não pode anexar uma ACL a um recurso do Security Lake.

Controle de acesso por atributo (ABAC) com o Security Lake

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Você pode anexar tags aos recursos do Security Lake — assinantes e à configuração do data lake para um indivíduo Conta da AWS . Regiões da AWS Você também pode controlar o acesso a esses tipos de recursos fornecendo informações de tag no elemento `Condition` de uma política. Para obter mais informações sobre recursos de marcação do Security Lake, consulte Marcando recursos do Security Lake. Para obter exemplos de políticas baseadas em identidade visando controlar o acesso a um recurso baseado nas tags desse recurso, consulte Exemplos de políticas baseadas em identidade para Security Lake.

Usar credenciais temporárias com o Security Lake

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

O Security Lake oferece suporte ao uso de credenciais temporárias.

Sessões de acesso direto para o Security Lake

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Algumas ações do Security Lake exigem permissões adicionais para ações dependentes em outros Serviços da AWS. Para obter uma lista dessas ações, consulte Ações definidas pelo Amazon Security Lake na Referência de autorização do serviço.

Perfis de serviço do Security Lake

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

O Security Lake não assume nem usa perfis de serviço. No entanto, serviços relacionados, como Amazon e Amazon S3 EventBridge AWS Lambda, assumem funções de serviço quando você usa o Security Lake. Para executar ações em seu nome, o Security Lake usa uma função vinculada a serviços.

> **Warning**
>
> A alteração das permissões em um perfil de serviço pode criar problemas operacionais no uso do Security Lake. Edite os perfis de serviço somente quando o Security Lake orientar você a fazê-lo.

Funções vinculadas a serviços do Security Lake

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

O Security Lake usa uma função vinculada a serviços do IAM chamada `AWSServiceRoleForAmazonSecurityLake`. A função vinculada a serviços do Security Lake concede permissões para operar um serviço de data lake de segurança em nome dos clientes. Um perfil vinculado a serviços é um perfil do IAM que está vinculada diretamente ao Security Lake. É predefinido pelo Security Lake e inclui todas as permissões que o Security Lake exige para ligar para outras pessoas Serviços da AWS em seu nome. O Security Lake usa essa função vinculada ao serviço em todos os lugares em Regiões da AWS que o Security Lake está disponível.

Para obter detalhes sobre como criar ou gerenciar função vinculada a serviços do Security Lake, consulte Usando funções vinculadas ao serviço para o Security Lake.

Exemplos de políticas baseadas em identidade para Security Lake

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Security Lake. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Security Lake, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Security Lake na Referência de autorização de serviço. ARNs

Tópicos

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Security Lake em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações

que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Como usar o console do Security Lake

Para acessar o console do Amazon Security Lake, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Security Lake em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Para garantir que usuários e funções possam usar o console do Security Lake, crie políticas do IAM que forneçam acesso ao console. Para ter mais informações, consulte Identidades do IAM no Manual do usuário do IAM.

Se você criar uma política que permita que usuários ou funções usem o console do Security Lake, certifique-se de que a política inclua as ações apropriadas para os recursos que esses usuários ou funções precisam acessar no console. Caso contrário, eles não conseguirão navegar ou exibir detalhes sobre esses recursos no console.

Por exemplo, para adicionar uma fonte personalizada usando o console, um usuário deve ter permissão para realizar estas ações:

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

Exemplo: permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

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

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: permitir que a conta de gerenciamento da organização designe e remova um administrador delegado

Este exemplo mostra como você pode criar uma política que permite que um usuário de uma conta de gerenciamento do AWS Organizations designe e remova o administrador delegado do Security Lake da organização.

JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "securitylake:RegisterDataLakeDelegatedAdministrator",
                "securitylake:DeregisterDataLakeDelegatedAdministrator"
            ],
            "Resource": "arn:aws:securitylake:*:*:*"
        }
    ]
}
```

Exemplo: permitir que os usuários avaliem os assinantes com base em tags

Você pode usar condições em uma política baseada em identidade para controlar o acesso aos recursos do Security Lake com base em tags. Este exemplo mostra como você pode criar uma política que permite que um usuário avalie os assinantes usando o console do Security Lake ou a API do Security Lake. No entanto, a permissão é concedida somente se o valor da tag do `Owner` tiver o valor do nome de usuário desse assinante.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewSubscriberDetailsIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:GetSubscriber",
            "Resource": "arn:aws:securitylake:*:*:subscriber/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListSubscribersIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:ListSubscribers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
```

```
            }
        }
    ]
}
```

Neste exemplo, se um usuário com o nome de usuário `richard-roe` tentar revisar os detalhes de assinantes individuais, um assinante deverá ter a tag `0wner=richard-roe` ou `owner=richard-roe`. Caso contrário, o usuário terá o acesso negado. A chave da tag de condição `0wner` corresponde a `0wner` e a `owner` porque os nomes de chaves de condição não diferenciam letras maiúsculas de minúsculas. Para obter mais informações sobre o uso de chaves de condição, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM. Para obter mais informações sobre recursos de marcação do Security Lake, consulte Marcando recursos do Security Lake.

AWS políticas gerenciadas para Security Lake

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para saber mais, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

AWS política gerenciada: AmazonSecurityLakeMetastoreManager

O Amazon Security Lake usa uma AWS Lambda função para gerenciar metadados em seu data lake. Com o uso dessa função, o Security Lake pode indexar partições do Amazon Simple Storage Service (Amazon S3) que contêm seus dados e arquivos de dados nas AWS Glue tabelas do Catálogo de Dados. Essa política gerenciada contém todas as permissões da função Lambda para indexar as partições e arquivos de dados do S3 nas tabelas. AWS Glue

Detalhes de permissões

Esta política inclui as seguintes permissões:

- `logs`— Permite que os diretores registrem a saída da função Lambda no Amazon CloudWatch Logs.
- `glue`— Permite que os diretores executem ações de gravação específicas para tabelas do Catálogo AWS Glue de Dados. Isso também permite que AWS Glue os rastreadores identifiquem partições em seus dados.
- `sqs`— Permite que os diretores realizem ações específicas de leitura e gravação para filas do Amazon SQS que enviam notificações de eventos quando objetos são adicionados ou atualizados em seu data lake.
- `s3`— Permite que os diretores realizem ações específicas de leitura e gravação para o bucket do Amazon S3 que contém seus dados.

Para verificar as permissões para esta política, consulte AmazonSecurityLakeMetastoreManager no Guia de referência de políticas gerenciadas pela AWS .

AWS política gerenciada: AmazonSecurityLakePermissionsBoundary

O Amazon Security Lake cria perfis do IAM para fontes personalizadas de terceiros gravarem dados em um data lake e para que assinantes terceirizados consumam dados de um data lake e usa essa política ao criar esses perfis para definir o limite de suas permissões. Você não precisa fazer nada para usar essa política. Se o data lake for criptografado com uma AWS KMS chave gerenciada pelo cliente `kms:Decrypt` e `kms:GenerateDataKey` as permissões forem adicionadas.

Para verificar as permissões para esta política, consulte AmazonSecurityLakePermissionsBoundary no Guia de referência de políticas gerenciadas pela AWS .

AWS política gerenciada: AmazonSecurityLakeAdministrator

Você pode vincular a política `AmazonSecurityLakeAdministrator` a uma entidade principal antes que ela habilite o Amazon Security Lake para sua conta. Essa política concede permissões administrativas que oferecem à entidade principal acesso total a todas as ações do Security Lake. A entidade principal pode então se conectar ao Security Lake e, posteriormente, configurar fontes e assinantes no Security Lake.

Essa política inclui as ações que os administradores do Security Lake podem executar em outros serviços da AWS pelo Security Lake.

A `AmazonSecurityLakeAdministrator` política não suporta a criação de funções utilitárias exigidas pelo Security Lake para gerenciar a replicação entre regiões do Amazon S3, o registro de novas partições de dados, a AWS Glue execução de um rastreador Glue em dados adicionados a fontes personalizadas ou a notificação de novos dados aos assinantes do endpoint HTTPS. Você pode criar essas funções com antecedência, conforme descrito em Conceitos básicos do Amazon Security Lake.

Além da política gerenciada `AmazonSecurityLakeAdministrator`, o Security Lake exige permissões `lakeformation:PutDataLakeSettings` para funções de integração e configuração. `PutDataLakeSettings` permite definir uma entidade principal do IAM como administrador de todos os recursos regionais do Lake Formation na conta. Essa função deve ter `iam:CreateRole permission`, além de uma política `AmazonSecurityLakeAdministrator` associada a ela.

Os administradores do Lake Formation têm acesso total ao console do Lake Formation e controlam a configuração inicial dos dados e as permissões de acesso. O Security Lake atribui a entidade principal que habilita o Security Lake e a função `AmazonSecurityLakeMetaStoreManager` (ou outra função especificada) como administradores do Lake Formation para que eles possam criar tabelas, atualizar o esquema da tabela, registrar novas partições e configurar permissões nas tabelas. Você deve incluir as seguintes permissões na política para o usuário ou a função de administrador do Security Lake:

> **Note**
>
> Para fornecer permissões suficientes para conceder acesso de assinante baseado em Lake Formation, o Security Lake recomenda adicionar as seguintes `glue:PutResourcePolicy` permissões.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutLakeFormationSettings",
      "Effect": "Allow",
      "Action": "lakeformation:PutDatalakeSettings",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowGlueActions",
      "Effect": "Allow",
      "Action": ["glue:PutResourcePolicy", "glue:DeleteResourcePolicy"],
      "Resource": [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    }
  ]
}
```

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `securitylake`: permite que entidades principais tenham total acesso a todas as ações do Security Lake.
- `organizations`: permite que entidades principais recuperem informações das organizações da AWS sobre as contas de uma organização. Se conta for da organização, essas permissões permitem que o console do Security Lake exiba os nomes das contas e os números das contas.
- `iam`— Permite que os diretores criem funções vinculadas a serviços para o Security Lake e AWS Lake Formation Amazon EventBridge, como uma etapa necessária ao habilitar esses serviços. Também permite a criação e edição de políticas para funções de assinante e de fonte personalizada, com as permissões dessas funções limitadas ao que é permitido pela política `AmazonSecurityLakePermissionsBoundary`.
- `ram`— Permite que os diretores configurem o acesso Lake Formation baseado em consultas dos assinantes às fontes do Security Lake.
- `s3`: permite que as entidades principais criem e gerenciem os buckets do Security Lake e leiam o conteúdo desses buckets.
- `lambda`— permite que os diretores gerenciem o Lambda usado para atualizar as partições da AWS Glue tabela após a entrega da AWS fonte e a replicação entre regiões.
- `glue`: permite que as entidades principais criem e gerenciem banco de dados e tabelas do Security Lake.
- `lakeformation`— Permite que os diretores gerenciem Lake Formation as permissões das tabelas do Security Lake.
- `events`: permite que as entidades principais gerenciem as regras usadas para notificar os assinantes sobre novos dados nas fontes do Security Lake.
- `sqs`— Permite que os diretores criem e gerenciem Amazon SQS filas usadas para notificar os assinantes sobre novos dados nas fontes do Security Lake.
- `kms`: permite que as entidades principais concedam acesso ao Security Lake para gravar dados usando uma chave gerenciada pelo cliente.
- `secretsmanager`: permite que as entidades principais gerenciem segredos usados para notificar os assinantes sobre novos dados nas fontes do Security Lake por meio de endpoints HTTPS.

Para verificar as permissões para esta política, consulte AmazonSecurityLakeAdministrator no Guia de referência de políticas gerenciadas pela AWS .

AWS política gerenciada: SecurityLakeServiceLinkedRole

O Security Lake usa a função vinculada ao serviço chamada `AWSServiceRoleForSecurityLake` para criar e operar o data lake de segurança.

Não é possível anexar a política gerenciada `SecurityLakeServiceLinkedRole` às suas entidades do IAM. Essa política é anexada a uma função vinculada a serviços que permite que o Security Lake realize ações em seu nome. Para obter mais informações, consulte Permissões de função vinculada ao serviço para o Security Lake.

AWS política gerenciada: SecurityLakeResourceManagementServiceRolePolicy

O Security Lake usa a função vinculada ao serviço nomeada `AWSServiceRoleForSecurityLakeResourceManagement` para realizar melhorias contínuas de monitoramento e desempenho, o que pode reduzir a latência e os custos. Fornece acesso para gerenciar recursos criados pelo Security Lake. Concede ao Security Lake a capacidade de excluir SecurityLake _Glue_Partition_Updater_Lambda. Esse lambda foi descontinuado para clientes que realizaram a migração do iceberg e migraram para fontes v2. Esse lambda estava usando o tempo de execução do Python 3.9, que será descontinuado em dezembro. Em vez de atualizar o tempo de execução desse lambda para esses clientes, seria melhor excluí-los. Temos um processo de recuperação que determinará se o cliente ainda precisa do lambda ou não e o excluirá se não precisar. Essa atualização do SLR é necessária para nos permitir excluir esse lambda.

Não é possível anexar a política gerenciada `SecurityLakeResourceManagementServiceRolePolicy` às suas entidades do IAM. Essa política é anexada a uma função vinculada a serviços que permite que o Security Lake realize ações em seu nome. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço para gerenciamento de recursos.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `events`— Permite que os diretores listem e gerenciem EventBridge regras para o processamento de eventos do Security Lake.
- `lambda`— Permite que os diretores gerenciem as funções e configurações do Lambda para o processamento de metadados do Security Lake, incluindo a capacidade de excluir funções obsoletas do atualizador de partições.

- `glue`— permite que os diretores criem partições, gerenciem tabelas e acessem bancos de dados no Catálogo de AWS Glue Dados para o gerenciamento de metadados do Security Lake.
- `s3`— Permite que os diretores gerenciem configurações de bucket, políticas de ciclo de vida e objetos de metadados do Amazon S3 para operações de data lake do Security Lake.
- `logs`— Permite que os diretores acessem fluxos de CloudWatch registros e consultem dados de log para funções do Security Lake Lambda.
- `sqs`— Permite que os diretores gerenciem filas e mensagens do Amazon SQS para fluxos de trabalho de processamento de dados do Security Lake.
- `lakeformation`— Permite que os diretores recuperem as configurações e permissões do data lake para o gerenciamento de recursos do Security Lake.

Para visualizar mais detalhes sobre a política, inclusive a versão mais recente do documento de política JSON, consulte SecurityLakeResourceManagementServiceRolePolicy no AWS Managed Policy Reference Guide.

AWS política gerenciada: AWS GlueServiceRole

A política `AWS GlueServiceRole` gerenciada invoca o AWS Glue rastreador e permite rastrear dados de origem personalizados e identificar AWS Glue metadados de partições. Esses metadados são necessários para criar e atualizar tabelas no Catálogo de dados.

Para obter mais informações, consulte Coletando dados de fontes personalizadas no Security Lake.

Atualizações do Security Lake nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Security Lake desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na página Histórico do documento do Security Lake.

Alteração	Descrição	Data
SecurityLakeResourceManagementServic	O Security Lake atualizou a política gerenciada `SecurityLakeResour`	18 de novembro de 2025

Alteração	Descrição	Data
eRolePolicy— Política existente atualizada	ceManagementServic eRolePolicy para adicionar lambda:De leteFunction permissão para funções obsoletas do _Glue_Partition_Updater_Lam bda. SecurityLake Isso permite que o Security Lake limpe funções obsoletas do Lambda como parte da migração para fontes v2 e formato iceberg.	
AWSServiceRoleForS ecurityLakeResourc eManagement— Política existente atualizada	Essa política foi atualizada para substituir o StringLik e operador pelo ArnLike operador para avaliar as chaves do tipo ARN para o bloco lambda:Fu nctionArn aws:Resou rceAccount condicion al. Isso proporciona uma aplicação mais segura.	25 de setembro de 2025
Função vinculada a serviços para Amazon Security Lake — Nova função vinculada a serviços	Adicionamos uma nova função vinculada ao serviço. AWSServiceRoleForS ecurityLakeResourc eManagement Essa função vinculada ao serviço fornece permissões ao Security Lake para realizar melhorias contínuas de monitoramento e desempenho, o que pode reduzir a latência e os custos.	14 de novembro de 2024

Alteração	Descrição	Data
Função vinculada ao serviço para o Amazon Security Lake — Atualização das permissões existentes da função vinculada ao serviço	Adicionamos AWS WAF ações à política AWS gerenciada para a `SecurityLakeServiceLinkedRole` política. As ações adicionais permitem que o Security Lake colete AWS WAF registros, quando habilitado como uma fonte de log no Security Lake.	22 de maio de 2024
AmazonSecurityLakePermissionsBoundary – atualização para uma política existente	O Security Lake adicionou ações de SID à política.	13 de maio de 2024
AmazonSecurityLakeMetastoreManager – atualização para uma política existente	O Security Lake atualizou a política para adicionar uma ação de limpeza de metadados que permite excluir os metadados em seu data lake.	27 de março de 2024
AmazonSecurityLakeAdministrator – atualização para uma política existente	O Security Lake atualizou a política para permitir `iam:PassRole` a nova `AmazonSecurityLakeMetastoreManagerV2` função e permitir que o Security Lake implante ou atualize componentes do data lake.	23 de fevereiro de 2024

Alteração	Descrição	Data
AmazonSecurityLake MetastoreManager – Nova política	O Security Lake adicionou uma nova política gerenciad a que concede permissões para o Security Lake gerenciar metadados em seu data lake.	23 de janeiro de 2024
AmazonSecurityLakeAdministrator – Nova política	O Security Lake adicionou uma nova política gerenciad a que concede ao principal acesso total a todas as ações do Security Lake.	30 de maio de 2023
O Security Lake iniciou o rastreamento de alterações	O Security Lake começou a monitorar as mudanças em suas políticas AWS gerenciad as.	29 de novembro de 2022

Usando funções vinculadas ao serviço para o Security Lake

O Security Lake usa AWS Identity and Access Management funções vinculadas ao serviço (IAM). Uma função vinculada ao serviço é uma função do IAM vinculada diretamente ao Security Lake. Ela é predefinida pelo Security Lake e inclui todas as permissões que o Security Lake exige para chamar todos os outros Serviços da AWS em seu nome e operar o serviço de data lake de segurança. O Security Lake usa essa função vinculada ao serviço em todos os lugares em Regiões da AWS que o Security Lake está disponível.

A função vinculada a serviços elimina a necessidade de adicionar manualmente as permissões necessárias ao configurar o Security Lake. O Security Lake define as permissões dessa função vinculada ao serviço e, a menos que definido em contrário, somente o Security Lake pode assumir a função. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM. Você só pode excluir uma

função vinculada ao serviço depois de excluir seus recursos relacionados. Isso protege seus recursos porque você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS Serviços que funcionam com IAM e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para revisar a documentação da função vinculada a esse serviço.

Tópicos

- Permissões de função vinculada ao serviço (SLR) para Security Lake
- Permissões de função vinculada ao serviço (SLR) para gerenciamento de recursos

Permissões de função vinculada ao serviço (SLR) para Security Lake

O Security Lake usa a função vinculada a serviços chamada `AWSServiceRoleForSecurityLake`. Essa função vinculada a serviços confia no serviço `securitylake.amazonaws.com` para assumir a função. Para obter mais informações sobre políticas AWS gerenciadas para o Amazon Security Lake, consulte AWS Gerenciar políticas para o Amazon Security Lake.

A política de permissões para a função, que é uma política AWS gerenciada chamada`SecurityLakeServiceLinkedRole`, permite que o Security Lake crie e opere o data lake de segurança. Também permite que o Security Lake execute tarefas como as seguintes nos recursos especificados:

- Use AWS Organizations ações para recuperar informações sobre contas associadas
- Usar o Amazon Elastic Compute Cloud (Amazon EC2) para recuperar informações sobre logs de fluxo do Amazon VPC
- Use AWS CloudTrail ações para recuperar informações sobre a função vinculada ao serviço
- Use AWS WAF ações para coletar AWS WAF registros, quando ativada como fonte de log no Security Lake
- Use a `LogDelivery` ação para criar ou excluir uma assinatura de entrega de AWS WAF registros.

Para verificar as permissões para esta política, consulte SecurityLakeServiceLinkedRole no Guia de referência de políticas gerenciadas pela AWS .

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Como criar uma função vinculada a serviços do Security Lake

Você não precisa criar manualmente o perfil vinculado à serviços `AWSServiceRoleForSecurityLake` para o Security Lake. Quando você ativa o Security Lake para você Conta da AWS, o Security Lake cria automaticamente a função vinculada ao serviço para você.

Como editar uma função vinculada a serviços do Security Lake

O Security Lake não permite que você edite a função vinculada a serviços `AWSServiceRoleForSecurityLake`. Após a criação da função vinculada a serviços, você não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Como excluir uma função vinculada a serviços do Security Lake

Não é possível excluir a função vinculada a serviços do Security Lake. Em vez disso, você pode excluir a função vinculada ao serviço do console do IAM, da API ou. AWS CLI Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Antes de excluir a função vinculada a serviços, é necessário confirmar que a função não possui sessões ativas e remover quaisquer recursos que estejam sendo utilizados por `AWSServiceRoleForSecurityLake`.

> **Note**
>
> Se o serviço Security Lake estiver usando a função `AWSServiceRoleForSecurityLake` quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente fazer a operação novamente.

Se excluir a função vinculada a serviços `AWSServiceRoleForSecurityLake` e precisar criá-la novamente, você poderá criá-la novamente ativando o Security Lake em sua conta. Quando você ativa o Security Lake novamente, o Security Lake cria automaticamente uma função vinculada a serviços para você mais uma vez.

Compatível com Regiões da AWS a função vinculada ao serviço Security Lake

O Security Lake suporta o uso da função `AWSServiceRoleForSecurityLake` vinculada ao serviço em todos os locais em Regiões da AWS que o Security Lake está disponível. Para ver uma lista das Regiões em que o Security Lake está disponível atualmente, consulte Regiões e endpoints do Security Lake.

Permissões de função vinculada ao serviço (SLR) para gerenciamento de recursos

O Security Lake usa a função vinculada ao serviço nomeada `AWSServiceRoleForSecurityLakeResourceManagement` para realizar melhorias contínuas de monitoramento e desempenho, o que pode reduzir a latência e os custos. Essa função vinculada a serviços confia no serviço `resource-management.securitylake.amazonaws.com` para assumir a função. A ativação também concederá acesso ao Lake Formation e `AWSServiceRoleForSecurityLakeResourceManagement` registrará automaticamente seus buckets S3 gerenciados pelo Security Lake no Lake Formation em todas as regiões para melhorar a segurança.

A política de permissões para a função, que é uma política AWS gerenciada chamada`SecurityLakeResourceManagementServiceRolePolicy`, permite acesso para gerenciar recursos criados pelo Security Lake, incluindo o gerenciamento dos metadados em seu data lake. Para obter mais informações sobre políticas AWS gerenciadas para o Amazon Security Lake, consulte políticas AWS gerenciadas para o Amazon Security Lake.

Essa função vinculada ao serviço permite que o Security Lake monitore a integridade dos recursos implantados pelo Security Lake (S3 Bucket, tabelas, AWS Glue Amazon SQS Queue, Metastore Manager (MSM) Lambda Function e regras) em sua conta. EventBridge Alguns exemplos de operações que o Security Lake pode realizar com essa função vinculada ao serviço são:

- Compactação de arquivos de manifesto do Apache Iceberg, que melhora o desempenho das consultas e reduz os tempos e custos de processamento do Lambda MSM.
- Monitore o estado do Amazon SQS para detectar problemas de ingestão.
- Otimize a replicação de dados entre regiões para excluir arquivos de metadados.

> **Note**
>
> Se você não instalar a função `AWSServiceRoleForSecurityLakeResourceManagement` vinculada ao serviço, o

Security Lake continuará funcionando, mas é altamente recomendável aceitar essa função vinculada ao serviço para que o Security Lake possa monitorar e otimizar os recursos em sua conta.

Detalhes das permissões

A função está configurada com a seguinte política de permissões:

- `events`— Permite que os diretores gerenciem EventBridge as regras necessárias para fontes e assinantes de registros.
- `lambda`— Permite que os diretores gerenciem o lambda usado para atualizar as partições da AWS Glue tabela após a entrega da AWS fonte e a replicação entre regiões.
- `glue`— Permite que os diretores executem ações de gravação específicas para tabelas do Catálogo AWS Glue de Dados. Isso também permite que AWS Glue os rastreadores identifiquem partições em seus dados e permite que o Security Lake gerencie os metadados do Apache Iceberg para suas tabelas do Apache Iceberg.
- `s3`— Permite que os diretores realizem ações específicas de leitura e gravação nos buckets do Security Lake contendo dados de log e metadados da tabela Glue.
- `logs`— Permite que os diretores tenham acesso de leitura para registrar a saída da função CloudWatch Lambda em Logs.
- `sqs`— Permite que os diretores realizem ações específicas de leitura e gravação para filas do Amazon SQS que recebem notificações de eventos quando objetos são adicionados ou atualizados em seu data lake.
- `lakeformation`— Permite que os diretores leiam as configurações do Lake Formation para monitorar configurações incorretas.

Para verificar as permissões para esta política, consulte SecurityLakeResourceManagementServiceRolePolicy no Guia de referência de políticas gerenciadas pela AWS .

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM.

Como criar uma função vinculada a serviços do Security Lake

Você pode criar a função `AWSServiceRoleForSecurityLakeResourceManagement` vinculada ao serviço para o Security Lake usando o console do Security Lake ou o. AWS CLI

Para criar a função vinculada ao serviço, você deve conceder as seguintes permissões ao seu usuário do IAM ou função do IAM. A função do IAM deve ser de administrador do Lake Formation em todas as regiões habilitadas para o Security Lake.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLakeFormationActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIamActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:PutRolePolicy"
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/resource-
management.securitylake.amazonaws.com/
AWSServiceRoleForSecurityLakeResourceManagement",
        "arn:*:iam::*:role/*AWSServiceRoleForLakeFormationDataAccess",
        "arn:*:iam::aws:policy/service-role/AWSGlueServiceRole",
        "arn:*:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager",
```

```
        "arn:*:iam::aws:policy/aws-service-role/
SecurityLakeResourceManagementServiceRolePolicy"
      ],
      "Condition": {
        "StringLikeIfExists": {
          "iam:AWSServiceName": [
            "securitylake.amazonaws.com",
            "resource-management.securitylake.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowGlueActionsViaConsole",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:*:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ]
    }
  ]
}
```

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Aceite a nova função vinculada ao serviço clicando em Habilitar função vinculada ao serviço na barra de informações na página Resumo.

Depois de habilitar a função vinculada ao serviço, você não precisará repetir esse processo para uso futuro do Security Lake.

CLI

Para criar a função `AWSServiceRoleForSecurityLakeResourceManagement` vinculada ao serviço de forma programática, use o seguinte comando da CLI.

```
$ aws iam create-service-linked-role
--aws-service-name resource-management.securitylake.amazonaws.com
```

Ao criar a função `AWSServiceRoleForSecurityLakeResourceManagement` vinculada ao serviço usando AWS CLI, você também deve conceder permissões em nível de tabela do Lake Formation (ALTER, DESCRIBE) a todas as tabelas no banco de dados do Security Lake Glue para gerenciar os metadados da tabela e acessar os dados. Se as tabelas do Glue em qualquer região fizerem referência a buckets do S3 da ativação anterior do Security Lake, você deverá conceder temporariamente as permissões DATA_LOCATION_ACCESS à função vinculada ao serviço para permitir que o Security Lake corrija essa situação.

Você também precisa conceder permissões de Lake Formation para a função `AWSServiceRoleForSecurityLakeResourceManagement` vinculada ao serviço de sua conta.

O exemplo a seguir mostra como conceder permissões ao Lake Formation para a função vinculada ao serviço na região designada. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ aws lakeformation grant-permissions --region {region} --principal
 DataLakePrincipalIdentifier={AWSServiceRoleForSecurityLakeResourceManagement ARN} \
--permissions ALTER DESCRIBE --resource '{ "Table": { "DatabaseName":
 "amazon_security_lake_glue_db_{region}", "TableWildcard": {} } }'
```

O exemplo a seguir mostra como será a aparência do ARN da função. Você deve editar o ARN da função para corresponder à sua região.

`"AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"`

Você também pode usar a chamada de CreateServiceLinkedRoleAPI. Na solicitação, especifique o `AWSServiceName` com`resource-management.securitylake.amazonaws.com`.

Depois de ativar a `AWSServiceRoleForSecurityLakeResourceManagement` função, se você estiver usando a Chave Gerenciada pelo AWS KMS Cliente (CMK) para criptografia, deverá permitir que a função vinculada ao serviço grave objetos criptografados em buckets do S3 nas regiões em que a CMK existe. AWS No AWS KMS console, adicione a política a seguir à chave KMS AWS nas regiões em que a CMK existe. Para obter detalhes sobre como alterar a política de chaves do KMS, consulte Políticas de chaves AWS KMS no Guia do AWS Key Management Service desenvolvedor.

```
{
    "Sid": "Allow SLR",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::[regional-datalake-s3-
bucket-name]"
        },
        "StringLike": {
            "kms:ViaService": "s3.[region].amazonaws.com"
        }
    }
},
```

Como editar uma função vinculada a serviços do Security Lake

O Security Lake não permite que você edite a função vinculada a serviços `AWSServiceRoleForSecurityLakeResourceManagement`. Após a criação da função vinculada a serviços, você não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

Como excluir uma função vinculada a serviços do Security Lake

Não é possível excluir a função vinculada a serviços do Security Lake. Em vez disso, você pode excluir a função vinculada ao serviço do console do IAM, da API ou. AWS CLI Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Antes de excluir a função vinculada a serviços, é necessário confirmar que a função não possui sessões ativas e remover quaisquer recursos que estejam sendo utilizados por `AWSServiceRoleForSecurityLakeResourceManagement`.

> **Note**
>
> Se o serviço Security Lake estiver usando a função `AWSServiceRoleForSecurityLakeResourceManagement` quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente fazer a operação novamente.

Se excluir a função vinculada a serviços `AWSServiceRoleForSecurityLakeResourceManagement` e precisar criá-la novamente, você poderá criá-la novamente ativando o Security Lake em sua conta. Quando você ativa o Security Lake novamente, o Security Lake cria automaticamente uma função vinculada a serviços para você mais uma vez.

Compatível com Regiões da AWS a função vinculada ao serviço Security Lake

O Security Lake suporta o uso da função `AWSServiceRoleForSecurityLakeResourceManagement` vinculada ao serviço em todos os locais em Regiões da AWS que o Security Lake está disponível. Para ver uma lista das Regiões em que o Security Lake está disponível atualmente, consulte Regiões e endpoints do Security Lake.

Proteção de dados no Amazon Security Lake

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no Amazon Security Lake. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Data Privacy FAQ. Para obter mais

informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sigilosas, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Security Lake ou outro Serviços da AWS usando o console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia em repouso

O Amazon Security Lake armazena com segurança seus dados em repouso usando soluções de AWS criptografia. Os dados brutos de log e eventos de segurança são armazenados em buckets

multilocatários do Amazon Simple Storage Service (Amazon S3) específicos da fonte em uma conta gerenciada pelo Security Lake. Cada fonte de log tem seu próprio bucket multilocatário. O Security Lake criptografa esses dados brutos usando uma AWS chave própria de AWS Key Management Service (AWS KMS). AWS chaves próprias são uma coleção de AWS KMS chaves que um AWS serviço — nesse caso, o Security Lake — possui e gerencia para uso em várias contas. AWS

O Security Lake executa trabalhos de extração, transformação e carregamento (ETL) em dados brutos de log e eventos.

Depois que os trabalhos de ETL forem concluídos, o Security Lake cria buckets S3 de inquilino único em sua conta (um bucket para cada um no qual você ativou Região da AWS o Security Lake). Os dados são armazenados nos buckets S3 multilocatários apenas temporariamente até que o Security Lake possa entregar os dados de forma confiável aos buckets S3 de inquilino único. Os buckets de locatário único incluem uma política baseada em recursos que dá permissão ao Security Lake para gravar dados de log e eventos nos buckets. Para criptografar dados em seu bucket do S3, você pode escolher uma chave de criptografia gerenciada pelo S3 ou uma chave gerenciada pelo cliente (de). AWS KMS Ambas as opções usam criptografia simétrica.

Como usar uma chave do KMS para criptografia dos dados

Por padrão, os arquivos de log entregues pelo Security Lake ao seu bucket do S3 são criptografados criptografia do servidor da Amazon com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3). Para fornecer uma camada de segurança que você gerencia diretamente, você pode usar criptografia do lado do servidor com AWS KMS chaves (SSE-KMS) para seus dados do Security Lake.

O SSE-KMS não é compatível com o console do Security Lake. Para usar o SSE-KMS com a API do Security Lake ou a CLI, primeiro você cria uma chave do KMS ou usa uma chave existente. Você anexa uma política à chave que determina quais usuários podem usar as chaves para criptografar e descriptografar os arquivos de log do Security Lake.

Se você usar uma chave gerenciada pelo cliente para criptografar dados gravados em seu bucket do S3, não poderá escolher uma chave multirregional. Para chaves gerenciadas pelo cliente, o Security Lake cria uma concessão em seu nome enviando uma solicitação `CreateGrant` para o AWS KMS. As concessões AWS KMS são usadas para dar ao Security Lake acesso a uma chave KMS em uma conta de cliente.

O Security Lake requer a concessão para usar a sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie `GenerateDataKey` solicitações AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie `RetireGrant` solicitações para AWS KMS. Quando você faz atualizações no seu data lake, essa operação permite a retirada da concessão que foi adicionada à chave do AWS KMS para processamento de ETL.

O Security Lake não precisa de permissões `Decrypt`. Quando os usuários autorizados da chave leem dados do Security Lake, o S3 gerencia a descriptografia, e os usuários autorizados podem ler os dados de modo não criptografado. No entanto, um assinante precisa de permissões `Decrypt` para consumir os dados da fonte. Para obter mais informações sobre permissões do assinante, consulte Como gerenciar o acesso a dados para assinantes do Security Lake.

Se quiser usar uma chave KMS existente para criptografar dados do Security Lake, você deve modificar a política de chaves para a chave KMS. A política de chaves deve permitir que a função do IAM associada à localização do data lake do Lake Formation use a chave KMS para descriptografar os dados. Para obter instruções sobre como alterar a política de chaves de uma chave KMS, consulte Alteração de uma política de chaves no Guia do AWS Key Management Service desenvolvedor.

Sua chave KMS pode aceitar solicitações de concessão, permitindo que o Security Lake acesse a chave quando você cria uma política de chaves ou usa uma política de chaves existente com as permissões apropriadas. Para obter mais informações sobre como criar uma política de chave, consulte Criar uma política de chave no Guia do desenvolvedor do AWS Key Management Service .

Anexe a seguinte política de chaves à sua chave do KMS:

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

Permissões do IAM obrigatórias ao usar uma chave gerenciada pelo cliente

Consulte a seção Conceitos básicos: pré-requisitos para ter uma visão geral dos perfis do IAM que você precisa criar para usar o Security Lake.

Quando você adiciona uma fonte personalizada ou um assinante, o Security Lake cria perfis do IAM em sua conta. Esses perfis devem ser compartilhados com outras identidades do IAM. Eles permitem que uma fonte personalizada grave dados no data lake e que um assinante consuma dados do data lake. Uma política AWS gerenciada chamada `AmazonSecurityLakePermissionsBoundary` define os limites de permissão para essas funções.

Criptografar filas do Amazon SQS

Quando você cria seu data lake, o Security Lake cria duas filas não criptografadas do Amazon Simple Queue Service (Amazon SQS) na conta delegada do administrador do Security Lake. Você deve criptografar essas filas para proteger os dados. A criptografia do lado do servidor (SSE) padrão fornecida pelo Amazon Simple Queue Service não é suficiente. Você deve criar uma chave gerenciada pelo cliente em AWS Key Management Service (AWS KMS) para criptografar as filas e conceder ao serviço Amazon S3 permissões principais para trabalhar com as filas criptografadas. Para obter instruções sobre como conceder essas permissões, consulte Por que as notificações de eventos do Amazon S3 não são entregues a uma fila do Amazon SQS que usa criptografia do lado do servidor? no Centro de AWS Conhecimento.

Como o Security Lake usa AWS Lambda para suportar trabalhos de extração, transferência e carregamento (ETL) em seus dados, você também deve conceder permissões ao Lambda para gerenciar mensagens em suas filas do Amazon SQS. Para obter mais informações, consulte Permissões de função de execução no Guia do desenvolvedor do AWS Lambda .

Criptografia em trânsito

O Security Lake criptografa todos os dados em trânsito entre os AWS serviços. O Security Lake protege os dados em trânsito, à medida que viajam de e para o serviço, criptografando automaticamente todos os dados entre redes usando o protocolo de criptografia Transport Layer Security (TLS) 1.2. As solicitações HTTPS diretas enviadas ao Security Lake APIs são assinadas usando o algoritmo AWS Signature versão 4 para estabelecer uma conexão segura.

Optar por não usar seus dados para melhorar o serviço

Você pode optar por não ter seus dados usados para desenvolver e melhorar o Security Lake e outros serviços AWS de segurança usando a política AWS Organizations de exclusão. Você

pode rejeitar, mesmo que o Security Lake não colete esses dados no momento. Para obter mais informações sobre como optar por não participar, consulte as políticas de exclusão dos serviços de IA no Guia do usuário do AWS Organizations .

Atualmente, o Security Lake não coleta nenhum dado de segurança que processa em seu nome ou dados de segurança que você carrega no seu data lake de segurança criado por esse serviço. Para desenvolver e melhorar o serviço Security Lake e as funcionalidades de outros serviços de AWS segurança, o Security Lake poderá coletar esses dados no futuro, incluindo dados que você carrega de fontes de dados de terceiros. Atualizaremos esta página quando o Security Lake pretender coletar esses dados e descreveremos como isso funcionará. Você ainda terá a oportunidade de rejeitar a qualquer momento.

> **Note**
>
> Para que você use a política de exclusão, suas AWS contas devem ser gerenciadas centralmente pelo. AWS Organizations Se você ainda não criou uma organização para suas AWS contas, consulte Criação e gerenciamento de uma organização no Guia do AWS Organizations usuário.

A exclusão tem os seguintes efeitos:

- O Security Lake excluirá os dados que foram coletados e armazenados antes da rejeição (se houver).
- Depois de rejeitar, o Security Lake não coletará mais nem armazenará esses dados.

Validação de conformidade do Amazon Security Lake

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis

e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a Documentação AWS de segurança.

Práticas recomendadas de segurança no Security Lake

Veja as práticas recomendadas a seguir para o Amazon Security Lake.

Conceder o mínimo de permissões possível aos usuários do Security Lake

Siga o princípio do menor privilégio concedendo o conjunto mínimo de permissões de política de acesso para seus usuários, grupos de usuários e funções AWS Identity and Access Management (IAM). Por exemplo, você pode permitir que um usuário do IAM visualize uma lista de fontes de log no Security Lake, mas não crie fontes ou assinantes. Para obter mais informações, consulte Exemplos de políticas baseadas em identidade para Security Lake.

Você também pode usar AWS CloudTrail para rastrear o uso da API no Security Lake. CloudTrail fornece um registro das ações de API realizadas por um usuário, grupo ou função no Security Lake. Para obter mais informações, consulte Registrando chamadas de API do Security Lake usando CloudTrail.

Visualizar a página Resumo

A página Resumo do console do Security Lake fornece uma visão geral dos problemas dos últimos 14 dias que estão afetando o serviço Security Lake e os buckets do Amazon S3 nos quais seus dados são armazenados. Você pode investigar mais detalhadamente esses problemas para ajudar a mitigar possíveis impactos relacionados à segurança.

Integre com o Security Hub CSPM

Integre o Security Lake e receba AWS Security Hub CSPM as descobertas do CSPM do Security Hub no Security Lake. O Security Hub CSPM gera descobertas de várias integrações diferentes Serviços da AWS e de terceiros. Receber as descobertas do CSPM do Security Hub ajuda você a ter uma visão geral de sua postura de conformidade e se você está cumprindo as melhores práticas AWS de segurança.

Para obter mais informações, consulte Integração com AWS Security Hub CSPM.

Excluir AWS Lambda

Ao excluir uma AWS Lambda função, recomendamos não desativá-la primeiro. Desabilitar uma função Lambda antes da exclusão pode interferir nos recursos de consulta de dados e potencialmente impactar outras funcionalidades. É melhor excluir a função Lambda diretamente sem desativá-la. Para obter mais informações sobre como excluir a função Lambda, AWS Lambda consulte o guia do desenvolvedor.

Monitorar eventos do Security Lake

Você pode monitorar o Security Lake usando CloudWatch métricas da Amazon. CloudWatch coleta dados brutos do Security Lake a cada minuto e os processa em métricas. Você pode definir alarmes que acionam notificações quando as métricas correspondem aos limites especificados.

Para obter mais informações, consulte CloudWatch métricas para o Amazon Security Lake.

Resiliência no Amazon Security Lake

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. As zonas de disponibilidade oferecem a você uma forma eficiente para criar e operar aplicações e bancos de dados. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

A disponibilidade do Security Lake está vinculada à disponibilidade da região. A distribuição em várias zonas de disponibilidade ajuda o serviço a tolerar falhas em qualquer zona de disponibilidade.

A disponibilidade do plano de dados do Security Lake não está vinculada à disponibilidade de nenhuma região. No entanto, a disponibilidade do ambiente de gerenciamento do Security Lake está intimamente ligada à disponibilidade da região Leste dos EUA (Norte da Virgínia).

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Security Lake, no qual os dados são apoiados pelo Amazon Simple Storage Service (Amazon S3), oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Configuração do ciclo de vida

Uma configuração de ciclo de vida é um conjunto de regras que definem as ações aplicadas pelo Amazon S3 a um grupo de objetos. Com regras de configuração de ciclo de vida, é possível solicitar que o Amazon S3 faça a transição de objetos para classes de armazenamento menos caras, arquive-os ou exclua-os. Para obter mais informações, consulte Gerenciar ciclo de vida de armazenamento no Manual do usuário do Amazon S3.

Versionamento

Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar de ações não intencionais de usuários e de falhas da aplicação. Para obter mais informações, consulte Usar o versionamento em buckets do Amazon S3 no Guia do usuário do Amazon S3.

Classes de armazenamento

O Amazon S3 oferece uma variedade de classes de armazenamento para escolher, de acordo com os requisitos da workload. As classes de armazenamento S3 Standard – IA e S3 One Zone – IA foram desenvolvidas para dados que você acessa cerca de uma vez por mês e precisam de acesso de milissegundos. A classe de armazenamento S3 Glacier Instant Retrieval foi projetada para dados de arquivo de longa duração com acesso de milissegundos que você acessa cerca de uma vez por trimestre. Para dados de arquivo que não necessitam de acesso imediato, como backups, use as classes de armazenamento S3 Glacier Flexieval ou S3 Glacier Deep Archive. Para obter mais informações, consulte Uso de classes de armazenamento do Amazon S3 no Guia do usuário do Amazon S3.

Segurança da infraestrutura no Amazon Security Lake

Como um serviço gerenciado, o Amazon Security Lake é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Security Lake pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Configuração e análise de vulnerabilidade no Security Lake

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

Amazon Security Lake e endpoints de interface VPC ()AWS PrivateLink

Você pode estabelecer uma conexão privada entre sua VPC e o Amazon Security Lake criando uma interface VPC endpoint. Os endpoints de interface são alimentados por AWS PrivateLinkuma tecnologia que permite acessar o Security Lake de forma privada APIs sem um gateway de internet, dispositivo NAT, conexão VPN ou conexão AWS Direct Connect. As instâncias em sua VPC não precisam de endereços IP públicos para se comunicar com o Security Lake. APIs O tráfego entre sua VPC e o Security Lake não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais Interfaces de Rede Elástica nas sub-redes.

Para mais informações, consulte Endpoints da VPC de interface(AWS PrivateLink) no Guia AWS PrivateLink .

Considerações sobre os endpoints VPC do Security Lake

Antes de configurar uma interface VPC endpoint para o Security Lake, certifique-se de revisar as propriedades e limitações do endpoint da interface no Guia.AWS PrivateLink

O Security Lake oferece suporte para fazer chamadas para todas as suas ações de API a partir da sua VPC.

O Security Lake oferece suporte a endpoints FIPS VPC somente nas seguintes regiões em que o FIPS existe:

- Leste dos EUA (Norte da Virgínia)

- Leste dos EUA (Ohio)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)

Criação de uma interface VPC endpoint para Security Lake

Você pode criar um VPC endpoint para o serviço Security Lake usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um VPC endpoint para o Security Lake usando o seguinte nome de serviço:

- com.amazonaws. *region*. lago de segurança
- com.amazonaws. *region*.securitylake-fips (endpoint FIPS)

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API ao Security Lake usando seu nome DNS padrão para a região, por exemplo,. `securitylake.us-east-1.amazonaws.com`

Para mais informações, consulte Acessar um serviço por meio de um endpoint de interface no Guia do AWS PrivateLink .

Criação de uma política de VPC endpoint para o Security Lake

Você pode anexar uma política de endpoint ao seu VPC endpoint que controla o acesso ao Security Lake. Essa política especifica as seguintes informações:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia AWS PrivateLink .

Exemplo: política de VPC endpoint para ações do Security Lake

Veja a seguir um exemplo de uma política de endpoint para o Security Lake. Quando anexada a um endpoint, essa política concede acesso às ações listadas do Security Lake para todos os diretores em todos os recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers"
         ],
         "Resource":"*"
      }
   ]
}
```

Sub-redes compartilhadas

Você não pode criar, descrever, modificar ou excluir endpoints da VPC em sub-redes que são compartilhadas com você. No entanto, é possível usar os endpoints da VPC em sub-redes que são compartilhadas com você. Para obter informações sobre o compartilhamento da VPC, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Monitorar o Amazon Security Lake

O Security Lake se integra com AWS CloudTrail, que é um serviço que fornece um registro das ações que foram realizadas no Security Lake por um usuário, uma função ou outra AWS service (Serviço da AWS). Isso inclui ações do console do Security Lake e chamadas programáticas às operações de API do Security Lake. Usando as informações coletadas por CloudTrail, você pode determinar quais solicitações foram feitas ao Security Lake. Para cada solicitação é possível identificar quando ela foi realizada, o endereço IP do qual foi feita, quem fez a solicitação e detalhes adicionais. Para obter mais informações, consulte Registrando chamadas de API do Security Lake usando CloudTrail.

O Security Lake e o Amazon CloudWatch são integrados, para que você possa coletar, visualizar e analisar métricas dos registros que o Security Lake coleta. CloudWatch as métricas do seu data lake do Security Lake são coletadas e enviadas automaticamente CloudWatch em intervalos de um

minuto. Você também pode definir um alarme para enviar uma notificação se um limite especificado para uma métrica do Security Lake for atingido. Para obter uma lista de todas as métricas para as quais o Security Lake envia CloudWatch, consulteMétricas e dimensões do Security Lake.

CloudWatch métricas para o Amazon Security Lake

Você pode monitorar o Security Lake usando a Amazon CloudWatch, que coleta dados brutos a cada minuto e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, permitindo o acesso a informações históricas e proporcionando uma melhor perspectiva sobre os dados do data lake. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos.

Tópicos

Métricas e dimensões do Security Lake

O namespace `AWS/SecurityLake` inclui as métricas a seguir.

Métrica	Description
`ProcessedSize`	O volume de dados com suporte nativo Serviços da AWS que está atualmente armazenado em seu data lake. Unidades: bytes

As dimensões a seguir estão disponíveis para as métricas do Security Lake.

Dimensão	Description
`Account`	Métrica `ProcessedSize` para uma Conta da AWS específica. Essa dimensão está disponíve l somente quando você visualiza o `Per-Accou`

Dimensão	Description
	`nt Source Version Metrics` ativado CloudWatch.
`Region`	Métrica `ProcessedSize` para uma Região da AWS específica.
`Source`	`ProcessedSize` métrica para uma fonte de AWS log específica.
`SourceVersion`	`ProcessedSize` métrica para uma versão específica de uma fonte de AWS log.

Você pode visualizar métricas para contas específicas Contas da AWS (`Per-Account Source Version Metrics`) ou para todas as contas em uma organização (`Per-Source Version Metrics`).

Visualizando CloudWatch métricas do Security Lake

Você pode monitorar as métricas do Security Lake usando o CloudWatch console, a própria interface CloudWatch de linha de comando (CLI) ou programaticamente usando a API. CloudWatch Escolha seu método preferido e siga as etapas para acessar as métricas do Security Lake.

CloudWatch console

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Métricas, Todas as métricas.
3. Na guia Procurar, escolha Security Lake.
4. Escolha Métricas da versão por origem da conta ou Métricas da versão por origem.
5. Selecione uma métrica para visualizá-la em detalhes. Você também pode optar por fazer o seguinte:

   - Para classificar a métrica, use o cabeçalho da coluna.
   - Para criar um gráfico de uma métrica, selecione o nome da métrica e escolha uma opção de criação de um gráfico.
   - Para filtrar por métrica, selecione o nome da métrica e, em seguida, escolha Adicionar à pesquisa.

CloudWatch API

Para acessar as métricas do Security Lake usando a CloudWatch API, use a `GetMetricStatistics`ação.

AWS CLI

Para acessar as métricas do Security Lake usando o AWS CLI, execute o `get-metric-statistics`comando.

Para obter mais informações sobre o monitoramento usando métricas, consulte Usar CloudWatch métricas da Amazon no Guia CloudWatch do usuário da Amazon.

Configurando CloudWatch alarmes para métricas do Security Lake

CloudWatch também permite definir alarmes quando um limite é atingido para uma métrica. Por exemplo, você pode definir um alarme para a ProcessedSizemétrica, para ser notificado quando o volume de dados de uma fonte específica exceder um limite específico.

Para obter instruções sobre como configurar alarmes, consulte Como usar CloudWatch alarmes da Amazon no Guia CloudWatch do usuário da Amazon.

Registrando chamadas de API do Security Lake usando CloudTrail

O Amazon Security Lake se integra com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Security Lake. CloudTrail captura chamadas de API para o Security Lake como eventos. As chamadas capturadas incluem as chamadas de código do console do Security Lake e as chamadas para as operações da API do Security Lake. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Security Lake. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Security Lake, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações sobre Security Lake em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Security Lake, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do Security Lake, crie uma trilha. Uma trilha permite CloudTrail entregar eventos como arquivos de log para um bucket do Amazon S3 que você especificar. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail

- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

As ações do Security Lake são registradas CloudTrail e documentadas na Referência da API do Security Lake. Por exemplo, chamadas para as `CreateSubscriber` ações `UpdateDataLakeListLogSources`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- Se a solicitação foi feita com credenciais raiz ou de AWS Identity and Access Management usuário.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Noções básicas sobre entradas de arquivos de log do Security Lake

CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro para a `GetSubscriber` ação 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"
}
```

Marcando recursos do Security Lake

Uma tag é um rótulo opcional que você pode definir e atribuir aos AWS recursos, incluindo certos tipos de recursos do Amazon Security Lake. As tags podem ajudar a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Por exemplo, você pode usar tags para aplicar políticas, alocar custos, distinguir entre recursos ou identificar recursos que suportam determinados requisitos de conformidade ou fluxos de trabalho.

Você pode atribuir tags aos seguintes tipos de recursos do Security Lake: assinantes e a configuração do data lake individual Regiões da AWS. Conta da AWS

Tópicos

Fundamentos das tags

Um recurso pode ter até 50 tags. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional, ambos definidos por você. Uma chave de tag é uma etiqueta geral que atua como uma categoria para valores de tags mais específicos. Um valor de tag atua como um descritor de uma chave de tag.

Por exemplo, se você adicionar assinantes para analisar dados de segurança de diferentes ambientes (um conjunto de assinantes para dados na nuvem e outro conjunto para dados on-premises), poderá atribuir uma chave de tag `Environment` a esses assinantes. O valor da tag associada pode ser `Cloud` para assinantes que analisam dados de Serviços da AWS e `On-Premises` para os outros.

Ao definir e atribuir tags aos recursos do Amazon Security Lake, lembre-se do seguinte:

- Cada recurso pode ter um máximo de 50 tags.
- Em todos os recursos, cada chave de tag deve ser exclusiva e pode ter apenas um valor de tag.

- As chaves e valores das tags diferenciam maiúsculas de minúsculas. Como práticas recomendadas, recomendamos definir uma estratégia para letras maiúsculas em tags e implementá-las de forma consistente em todos os seus recursos.
- Uma chave de tag pode ter no máximo 128 caracteres UTF-8. Um valor de tag pode ter no máximo 256 caracteres UTF-8. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @
- O `aws:` prefixo é reservado para uso por AWS. Você não pode usá-lo em nenhuma chave ou valor de tag que você definir. Além disso, você não pode alterar ou remover chaves de tag ou valores que usam esse prefixo. As tags que usam esse prefixo não adicionam à cota de 50 tags por recurso.
- Todas as tags que você atribuir estão disponíveis somente para você Conta da AWS e somente no local Região da AWS em que você as atribui.
- Se você atribuir tags a um recurso usando o Security Lake, elas serão aplicadas somente ao recurso armazenado diretamente no Security Lake, na Região da AWS aplicável. As tags não são aplicadas a nenhum recurso associado ou de suporte criado, usado ou mantido pelo Security Lake em outros Serviços da AWS. Por exemplo, se você atribuir tags ao data lake, elas serão aplicadas somente à configuração do data lake no Security Lake para a Região especificada. Elas não são aplicados ao bucket do Amazon Simple Storage Service (Amazon S3) que armazena seus dados de log e de eventos. Para também atribuir tags a um recurso associado, você pode usar AWS Resource Groups ou AWS service (Serviço da AWS) aquele que armazena o recurso — por exemplo, Amazon S3 para um bucket do S3. A atribuição de tags a recursos associados pode ajudar você a identificar recursos de suporte para seu data lake.
- Se você excluir um recurso, todas as tags associadas a ele também serão excluídas.

Para obter mais restrições, dicas e melhores práticas, consulte Como marcar seus AWS recursos no Guia do usuário de AWS recursos de marcação.

> **Important**
>
> Não armazene dados sensíveis ou outros tipos de dados confidenciais em tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive Gerenciamento de Faturamento e Custos da AWS. As tags não devem ser usadas para dados confidenciais.

Para gerenciar tags ou adicioná-las a recursos do Security Lake, você pode usar o console do Security Lake ou a API Security Lake.

Utilizar tags nas políticas do IAM

Depois de começar a atribuir tags aos recursos, defina permissões de recurso baseadas em tags em políticas do AWS Identity and Access Management (IAM). Ao usar tags dessa forma, você pode implementar um controle granular de quais usuários e funções em sua empresa Conta da AWS têm permissão para criar e marcar recursos e quais usuários e funções têm permissão para adicionar, editar e remover tags de forma mais geral. Para controlar o acesso com base em tags, use chaves de condição relacionadas à tag no elemento de Condição das políticas do IAM.

Por exemplo, é possível criar uma política que permita que um usuário tenha acesso completo a todos os recursos do Amazon Security Lake, se a tag `Owner` do recurso especificar esse nome de usuário:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Se você definir permissões em nível de recurso e baseadas em tag, elas entrarão em vigor imediatamente. Isso significa que seus recursos ficam mais seguros assim que são criados, e que você pode começar a aplicar rapidamente o uso de tags em novos recursos. Também é possível usar permissões em nível de recurso para controlar quais valores e chaves de tag podem ser associados a recursos novos e existentes. Para obter mais informações, consulte Controle do acesso a AWS recursos usando tags no Guia do usuário do IAM.

Adicionar tags aos recursos do Amazon Security Lake

Para adicionar tags a um recurso do Amazon Security Lake, use o console do Security Lake ou a API Security Lake.

> **Important**
>
> Adicionar tags a um recurso pode afetar o acesso a ele. Antes de adicionar uma tag a um recurso, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar tags para controlar o acesso aos recursos.

Console

Quando você ativa o Security Lake para um assinante Região da AWS ou cria um, o console do Security Lake fornece opções para adicionar tags ao recurso — a configuração do data lake para a região ou o assinante. Siga as instruções no console para adicionar tags ao recurso quando for criá-lo.

Para adicionar uma ou mais tags a um recurso existente usando o console do Security Lake, siga estas etapas.

Adicionar uma tag a um recurso

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Realize uma das seguintes ações, dependendo do tipo de recurso que vai receber a tag:
   - Para uma configuração de data lake, escolha Regiões no painel de navegação. Em seguida, na tabela Regiões, selecione a Região.
   - Para um assinante, escolha Assinantes no painel de navegação. Em seguida, na tabela Meus assinantes, selecione o assinante.

     Se o assinante não aparecer na tabela, use o seletor Região da AWS no canto superior direito da página para selecionar a Região correspondente. A tabela lista somente os assinantes existentes da atual Região.
3. Escolha Editar.
4. Expanda a seção Tags. Essa seção lista todas as tags atribuídas ao recurso atualmente.
5. Na seção Tags, escolha Adicionar nova tag.

6. Na caixa Chave, insira a chave da tag a ser adicionada ao recurso. Em seguida, na caixa Valor, você tem a opção de inserir o valor da tag.

   Uma chave de tag pode ter até 128 caracteres. Um valor de tag pode conter até 256 caracteres. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @
7. Para adicionar outra tag ao recurso, escolha Adicionar nova tag e repita a etapa anterior. É possível atribuir até 50 tags a um recurso.
8. Quando terminar de adicionar tags, selecione Salvar.

API

Para criar um recurso e adicionar uma ou mais tags a ele programaticamente, use a operação `Create` apropriada para o tipo de recurso que deseja criar:

- Configuração do data lake — Use a CreateDataLakeoperação ou, se estiver usando o AWS Command Line Interface (AWS CLI), execute o create-data-lakecomando.
- Assinante — Use a CreateSubscriberoperação ou, se estiver usando o AWS CLI, execute o comando create-subscriber.

Em sua solicitação, use o parâmetro `tags` para especificar a chave da tag (`key`) e o valor opcional de tag (`value`) para cada tag a ser adicionada ao recurso. O parâmetro `tags` especifica uma matriz de objetos. Cada objeto especifica uma chave de tag e seu valor associado.

Para adicionar uma ou mais tags a um recurso existente, use a TagResourceoperação da API Security Lake ou, se estiver usando a AWS CLI, execute o comando tag-resource. Na solicitação, especifique o nome do recurso da Amazon (ARN) ao qual a tag será adicionada. Use o parâmetro `tags` para especificar a chave da tag (`key`) e o valor opcional de tag (`value`) para cada tag a ser adicionada. Como no caso de operações e comandos `Create`, o parâmetro `tags` especifica uma matriz de objetos, um objeto para cada chave de tag e seu valor de tag associado.

Por exemplo, o AWS CLI comando a seguir adiciona uma chave de `Environment` tag com um valor de `Cloud` tag ao assinante especificado. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ aws securitylake tag-resource \
```

```
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

Em que:

- `resource-arn` especifica o ARN do assinante ao qual a tag será adicionada.
- *`Environment`* é a chave da tag que será adicionada ao assinante.
- *`Cloud`* é o valor da chave de tag especificada (*`Environment`*).

No exemplo a seguir, o comando adiciona várias tags ao assinante.

```
$ 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 em uma matriz `tags`, os argumentos `key` e `value` são obrigatórios. No entanto, o valor do argumento `value` pode ser um segmento vazio. Se você não quiser associar um valor de tag a uma chave de tag, não especifique um valor para o argumento `value`. Por exemplo, o comando a seguir adiciona uma chave de tag `Owner` sem valor associado:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Se uma operação de tag for bem-sucedida, o Security Lake retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Lake retornará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Edição de tags para recursos do Amazon Security Lake

Você pode editar as tags (chaves e valores) de um recurso do Amazon Security Lake usando o console do Security Lake ou a API Security Lake.

> **Important**
>
> Editar as tags de um recurso pode afetar o acesso a ele. Antes de editar a chave ou o valor de uma tag para um recurso, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Console

Siga estas etapas para editar as tags de um recurso usando o console.

Para editar de tags de um recurso

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Realize uma das seguintes ações, dependendo do tipo de recurso da tag a ser editada:
   - Para uma configuração de data lake, escolha Regiões no painel de navegação. Em seguida, na tabela Regiões, selecione a Região.
   - Para um assinante, escolha Assinantes no painel de navegação. Em seguida, na tabela Meus assinantes, selecione o assinante.

     Se o assinante não aparecer na tabela, use o seletor Região da AWS no canto superior direito da página para selecionar a Região correspondente. A tabela lista somente os assinantes existentes da atual Região.
3. Escolha Editar.
4. Expanda a seção Tags. A seção Tags lista todas as tags atribuídas ao recurso atualmente.
5. Faça o seguinte:
   - Para adicionar um valor a uma chave existente, insira o valor na caixa Valor ao lado da chave de tag.
   - Para alterar uma chave existente, escolha Remover ao lado da tag. Depois, selecione Adicionar nova tag. Na caixa Chave, insira a nova chave de tag. Opcionalmente, insira um valor associado à tag na caixa Valor.
   - Para alterar o valor de uma tag existente, selecione X na caixa Valor que contém o valor. Em seguida, digite o novo valor da tag na caixa Valor.
   - Para remover o valor existente de uma tag, selecione X na caixa Valor que contém o valor.

- Para remover uma tag existente (a chave da tag e o valor da tag), selecione Remover ao lado da tag.

Um recurso pode ter até 50 tags. Uma chave de tag pode ter até 128 caracteres. Um valor de tag pode conter até 256 caracteres. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @

6. Depois de concluir a edição das tags, selecione Salvar.

API

Ao editar uma tag para um recurso programaticamente, você substitui a tag existente por novos valores. Portanto, a melhor maneira de editar uma tag depende se você deseja editar uma chave de tag, um valor de tag ou ambos. Para editar uma chave de tag, remova a tag atual e adicione uma nova.

Para editar ou remover somente o valor da tag associado a uma chave de tag, substitua o valor existente usando a TagResourceoperação da API Security Lake. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando tag-resource. Na solicitação, especifique o nome do recurso da Amazon (ARN) cujo valor você quer editar ou remover.

Para editar um valor de tag, use o parâmetro `tags` para especificar a chave que terá seu valor alterado. Especifique também o novo valor da chave. Por exemplo, o AWS CLI comando a seguir altera o valor da tag de `Cloud On-Premises` para para a chave de `Environment` tag atribuída ao assinante especificado. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ 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
```

Em que:

- `resource-arn` especifica o ARN do assinante.
- *`Environment`* é a chave de tag associada ao valor da tag a ser alterado.
- *`On-Premises`* é o novo valor da chave especificada (*`Environment`*).

Para remover um valor de tag de uma chave de tag, não especifique um valor para o argumento `value` da chave no parâmetro `tags`. Por exemplo:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Se a operação for bem-sucedida, o Security Lake retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Lake retornará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Análise de tags para recursos do Amazon Security Lake

Você pode analisar as tags (chaves e valores) de um recurso do Amazon Security Lake usando o console do Security Lake ou a API Security Lake.

Console

Siga estas etapas para analisar as tags de um recurso usando o console.

Para revisar as tags de um recurso

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Realize uma das seguintes ações, dependendo do tipo de recurso da tag a ser analisada:
   - Para uma configuração de data lake, escolha Regiões no painel de navegação. Na tabela Regiões, selecione a Região e escolha Editar. Expanda a seção Tags.
   - Para um assinante, escolha Assinantes no painel de navegação. Em seguida, na tabela Meus assinantes, selecione o nome de assinante.

     Se o assinante não aparecer na tabela, use o seletor Região da AWS no canto superior direito da página para selecionar a Região correspondente. A tabela lista somente os assinantes existentes da atual Região.

A seção Tags lista todas as tags atribuídas ao recurso atualmente.

API

Para recuperar e revisar programaticamente as tags de um recurso existente, use a ListTagsForResourceoperação da API Security Lake. Em sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN).

Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o list-tags-for-resourcecomando e use o `resource-arn` parâmetro para especificar o ARN do recurso. Por exemplo:

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

No exemplo anterior, *arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab* é o ARN de um assinante existente.

Se a operação for bem-sucedida, o Security Lake retornará uma matriz `tags`. Cada objeto na matriz especifica uma tag (tanto a chave quanto o valor) que está atualmente atribuída ao recurso. Por exemplo:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Em que `Environment`, `CostCenter` e `Owner` são as chaves de tag atribuídas ao recurso. `Cloud` é o valor da tag associado à chave da tag `Environment`. `12345` é o valor da tag associado à chave da tag `CostCenter`. A chave de tag `Owner` não tem nenhum valor associado.

Remoção de tags dos recursos do Amazon Security Lake

Para remover tags de um recurso do Amazon Security Lake, use o console do Security Lake ou a API Security Lake.

> **Important**
>
> Remover tags de um recurso pode afetar o acesso a ele. Antes de remover uma tag, revise todas as políticas AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Console

Siga estas etapas para remover uma ou mais tags de um recurso usando o console.

Remover uma tag de um recurso

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Realize uma das seguintes ações, dependendo do tipo de recurso de onde a tag será removida:
   - Para uma configuração de data lake, escolha Regiões no painel de navegação. Em seguida, na tabela Regiões, selecione a Região.
   - Para um assinante, escolha Assinantes no painel de navegação. Em seguida, na tabela Meus assinantes, selecione o assinante.

     Se o assinante não aparecer na tabela, use o seletor Região da AWS no canto superior direito da página para selecionar a Região correspondente. A tabela lista somente os assinantes existentes da atual Região.
3. Escolha Editar.
4. Expanda a seção Tags. A seção Tags lista todas as tags atribuídas ao recurso atualmente.
5. Faça o seguinte:
   - Para remover somente o valor de tag de uma tag, selecione X na caixa Valor que contém o valor a ser removido.
   - Para remover a chave e o valor (enquanto par) de uma tag, escolha Remover ao lado da tag.

6. Para remover outras tags do recurso, repita a etapa anterior para cada tag adicional a ser removida.
7. Ao finalizar a remoção das tags, escolha Salvar.

API

Para remover uma ou mais tags de um recurso de forma programática, use a UntagResourceoperação da API Security Lake. Em sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN) que terá a tag removida. Use o parâmetro `tagKeys` para especificar a chave da tag a ser removida. Para remover várias tags, anexe o parâmetro `tagKeys` e o argumento de cada tag a ser removida, separados por um E comercial (&), por exemplo, `tagKeys=key1&tagKeys=key2`. Para remover somente um valor específico (e não a chave) de um recurso, edite a tag em vez de removê-la.

Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando untag-resource para remover uma ou mais tags de um recurso. Para o parâmetro `resource-arn`, especifique o ARN do recurso que terá a tag removida. Use o parâmetro `tag-keys` para especificar a chave da tag a ser removida. Por exemplo, o comando a seguir remove a tag `Environment` (tanto a chave quanto o valor da tag) do assinante especificado:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

Em que `resource-arn` especifica o ARN do assinante do, e *`Environment`* é a chave da tag a ser removida.

Para remover várias tags de um recurso, acrescente cada chave adicional como argumento para o parâmetro `tag-keys`. Por exemplo:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

Se a operação for bem-sucedida, o Security Lake retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Lake retornará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Solução de problemas no Security Lake

Se você encontrar problemas ao trabalhar com o Amazon Security Lake, use os seguintes recursos de solução de problemas.

Os tópicos a seguir fornecem dicas de solução de problemas para erros e problemas que você pode encontrar relacionados ao status do data lake, ao Lake Formation, às consultas no Amazon Athena AWS Organizations e ao IAM. Se você encontrar um problema que não esteja listado aqui, você pode usar o `Feedback` botão nesta página para denunciá-lo.

Consulte os tópicos a seguir se você encontrar problemas ao usar o Security Lake.

Tópicos

Solução de problemas do status do data lake

A página Problemas do console do Security Lake mostra um resumo dos problemas que estão afetando seu data lake. Por exemplo, o Security Lake não pode habilitar a coleta de registros para eventos de AWS CloudTrail gerenciamento se você não tiver criado uma CloudTrail trilha para sua organização. A página Problemas aborda problemas que ocorreram nos últimos 14 dias. Você pode ver uma descrição de cada problema e as etapas de correção sugeridas.

Para acessar programaticamente um resumo dos problemas, você pode usar a ListDataLakeExceptionsoperação da API Security Lake. Se você estiver usando o AWS CLI, execute o list-data-lake-exceptionscomando. Para o `regions` parâmetro, você pode especificar um ou mais códigos de região — por exemplo, `us-east-1` para a região Leste dos EUA (Norte da Virgínia) — para ver os problemas que afetam essas regiões. Se você não incluir o `regions` parâmetro, os problemas que afetam todas as regiões serão retornados. Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.

Por exemplo, o AWS CLI comando a seguir lista problemas que estão afetando as `eu-west-3` regiões `us-east-1` e. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ aws securitylake list-data-lake-exceptions \
--regions "us-east-1" "eu-west-3"
```

Para notificar um usuário do Security Lake sobre um problema ou erro, use a CreateDataLakeExceptionSubscriptionoperação da API do Security Lake. O usuário pode ser notificado por e-mail, entrega em uma fila do Amazon Simple Queue Service (Amazon SQS), entrega para AWS Lambda uma função ou outro protocolo compatível.

Por exemplo, o AWS CLI comando a seguir envia notificações de exceções do Security Lake para a conta especificada por meio de entrega de SMS. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ aws securitylake create-data-lake-exception-subscription \
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

Para ver detalhes sobre uma assinatura de exceção, você pode usar a GetDataLakeExceptionSubscriptionoperação. Para atualizar uma assinatura de exceção, você pode usar a UpdateDataLakeExceptionSubscriptionoperação. Para excluir uma assinatura de exceção e interromper as notificações, você pode usar a DeleteDataLakeExceptionSubscriptionoperação.

Solução de problemas do Lake Formation

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Security Lake e AWS Lake Formation bancos de dados ou tabelas. Para ver mais tópicos de solução de problemas do Lake Formation, consulte a seção Solução de problemas do Guia do desenvolvedor do AWS Lake Formation .

Tabela não encontrada

Esse erro pode aparecer quando você tentar criar um assinante.

Para solucioná-lo, verifique se você já adicionou fontes na Região. Se você adicionou fontes quando o serviço Security Lake estava na versão prévia, as adicione novamente antes de criar um assinante.

Para obter mais informações sobre como adicionar fontes, consulte Gerenciamento de fontes no Security Lake.

400 AccessDenied

Esse erro pode aparecer quando você adicionar uma fonte personalizada e chamar a API `CreateCustomLogSource`.

Para resolvê-lo, revise suas permissões do Lake Formation. O perfil do IAM que está chamando a API deve ter permissões Create table para o banco de dados do Security Lake. Para mais informações, consulte Conceder permissões de banco de dados usando o console do Lake Formation e o método de recurso nomeado no Guia do desenvolvedor do AWS Lake Formation .

SYNTAX_ERROR: linha 1:8: SELECT * não é permitido a partir de uma relação que não tem colunas

Esse erro pode aparecer ao consultar uma tabela de fonte no Lake Formation pela primeira vez.

Para resolver o erro, conceda `SELECT` permissão à função do IAM que você está usando quando está conectado ao seu Conta da AWS. Para saber como conceder a permissão `SELECT`, consulte Conceder permissões de tabela usando o console do Lake Formation e o método de recurso nomeado no Guia do desenvolvedor do AWS Lake Formation .

O Security Lake não conseguiu adicionar a entidade principal ARN do chamador ao administrador de data lake do Lake Formation. Os atuais administradores de data lake podem incluir entidades principais inválidas que não existem mais.

Você pode receber esse erro ao ativar o Security Lake ou adicionar um AWS service (Serviço da AWS) como fonte de log.

Para resolver esse erro, siga estas etapas:

1. Abra o console do Lake Formation em https://console.aws.amazon.com/lakeformation/.
2. Faça login como usuário administrador.
3. No painel de navegação, em Permissões, selecione Perfis e tarefas administrativas.
4. Na seção Administradores do Data Lake, selecione Escolher administradores.

5. Limpe as entidades principais rotuladas como Não encontradas no IAM e selecione Salvar.
6. Tente a operação Security Lake novamente.

O Security Lake CreateSubscriber com Lake Formation não criou um novo convite de compartilhamento de recursos de RAM para ser aceito

Você pode ver esse erro se tiver compartilhado recursos com o compartilhamento de dados entre contas do Lake Formation versão 2 ou versão 3 antes de criar um assinante do Lake Formation no Security Lake. Isso ocorre porque o compartilhamento entre contas do Lake Formation versão 2 e versão 3 otimiza o número de compartilhamentos de recursos de AWS RAM mapeando várias concessões de permissão entre contas com um compartilhamento de recursos de AWS RAM.

Verifique se o nome do compartilhamento de recursos tem o ID externo que você especificou ao criar o assinante, e se o ARN do compartilhamento de recursos corresponde ao ARN na resposta `CreateSubscriber`.

Solução de problemas de consultas no Amazon Athena

Use as seguintes informações para diagnosticar e corrigir problemas comuns que podem ser encontrados ao usar o Athena para consultar objetos que estão armazenados no bucket S3 do Security Lake. Para ver mais tópicos de solução de problemas do Athena, consulte a seção Solução de problemas do Athena do Guia do usuário do Amazon Athena.

A consulta não está retornando novos objetos no data lake

Sua consulta do Athena pode não retornar novos objetos em seu data lake, mesmo quando o bucket S3 para o Security Lake contém esses objetos. Isso pode ocorrer se você tiver desativado o Security Lake e depois ativado novamente. Como resultado, as AWS Glue partições podem não registrar adequadamente os novos objetos.

Para resolver esse erro, siga estas etapas:

1. Abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. Na barra de navegação, no seletor “Regiões”, escolha a Região onde a consulta do Athena não está retornando resultados mesmo com o Security Lake ativado.
3. No painel de navegação, escolha Funções e selecione a função na lista a seguir, dependendo da versão de origem:

- `Source version 1 (OCSF 1.0.0-rc.2)` — Função SecurityLake*#region>*_Glue_Partition_Updater_Lambda_.
- `Source version 2 (OCSF 1.1.0)`— *#region>* função AmazonSecurityLakeMetastoreManager_.

4. Na guia Configuração, selecione Gatilhos.
5. Selecione a opção ao lado da função e escolha Editar.
6. Selecione Ativar gatilho e escolha Salvar. O estado da função passará a ser Ativado.

Não é possível acessar AWS Glue as tabelas

Um assinante de acesso a consultas pode não conseguir acessar AWS Glue tabelas que contêm dados do Security Lake.

Primeiro, certifique-se de que você seguiu os passos descritos em Como configurar o compartilhamento de tabelas entre contas (etapa do assinante).

Se o assinante ainda não tiver acesso, siga estas etapas:

1. Abra o AWS Glue console em https://console.aws.amazon.com/glue/.
2. No painel de navegação, escolha Catálogo de dados e Configurações do catálogo.
3. Dê permissão ao assinante para acessar as AWS Glue tabelas com uma política baseada em recursos. Para saber como criar políticas baseadas em recursos, consulte Exemplos de políticas baseadas em recursos do AWS Glue, no Guia do desenvolvedor do AWS Glue .

Solução de problemas no Organizations

Use as seguintes informações para diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Security Lake e com o AWS Organizations. Para ver mais tópicos de solução de problemas do Organizations, consulte a seção Solução de problemas do Guia do usuário do AWS Organizations .

Ocorreu um erro de acesso negado ao chamar a CreateDataLake operação: sua conta deve ser a conta de administrador delegado de uma organização ou uma conta independente.

Você pode receber esse erro se excluir a organização à qual uma conta de administrador delegado pertencia e depois tentar usar essa conta para configurar o Security Lake usando o console do Security Lake ou a CreateDataLakeAPI.

Para resolvê-lo, use uma conta de administrador delegado de outra organização ou uma conta independente.

Solução de problemas de identidade e acesso do Amazon Security Lake

Use as seguintes informações para diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Security Lake e com o IAM.

Não tenho autorização para executar uma ação no Security Lake

Se isso Console de gerenciamento da AWS indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu a você suas credenciais.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um *`subscriber`* fictício sem ter as permissões `SecurityLake:`*`GetSubscriber`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas de forma permitir o acesso à informação do *`subscriber`* usando a ação `SecurityLake:`*`GetSubscriber`*.

Quero expandir as permissões além da política gerenciada

Todas as funções do IAM criadas por um assinante ou fonte de registro personalizada APIs estão vinculadas à política `AmazonSecurityLakePermissionsBoundary` gerenciada. Se quiser

expandir as permissões além da política gerenciada, você pode remover a política gerenciada do Limite de Permissões da Função. No entanto, ao interagir com a mutação do Security Lake APIs para DataLakes e assinantes, o limite de permissões deve ser anexado para que o IAM altere a função do IAM.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Security Lake.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Security Lake. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do Security Lake

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Security Lake oferece suporte a esses atributos, consulte Como o Security Lake funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Como os preços do Security Lake são determinados

Os preços do Amazon Security Lake são baseados em duas dimensões: ingestão de dados e conversão de dados. O Security Lake também trabalha com outros Serviços da AWS para armazenar e compartilhar seus dados, e você pode incorrer em cobranças separadas por essas atividades.

Quando você ativa a coleta de registros pela primeira vez Conta da AWS em um aplicativo compatível com o Security Lake, essa conta é automaticamente inscrita em um teste gratuito de 15 dias do Security Lake. Região da AWS Você ainda pode incorrer em cobranças de outros serviços durante o teste gratuito.

> **Note**
>
> Ao continuar usando o Security Lake após o término do teste gratuito de 15 dias, você começará automaticamente a incorrer em custos de uso. Para evitar cobranças após o término do teste gratuito, você deve desativar o Security Lake.

Para entender a metodologia por trás dos preços do Security Lake, assista ao vídeo a seguir: Preços do Amazon Security Lake -->

Ingestão de dados

Esses custos derivam do volume de registros ingeridos e de outros AWS CloudTrail registros e eventos (AWS service (Serviço da AWS) registros de consulta do resolvedor do Amazon Route 53, AWS Security Hub CSPM descobertas e registros de fluxo do Amazon VPC).

Conversão de dados

Esses custos derivam do volume de AWS service (Serviço da AWS) registros e eventos que o Security Lake normaliza em Estrutura aberta do esquema de segurança cibernética (OCSF) no Security Lake esquema e converte para o formato Apache Parquet.

Custos de serviços relacionados

Aqui estão alguns custos que você pode incorrer Serviços da AWS para armazenar e compartilhar os dados em seu data lake de segurança:

- Amazon S3: esses custos derivam da manutenção de buckets do Amazon S3 em sua conta do Security Lake, do armazenamento de seus dados lá e da avaliação e monitoramento de seu bucket para segurança e controle de acesso. Para obter mais informações, consulte Preço do Amazon S3.
- Amazon SQS: esses custos são derivados da criação de uma fila do Amazon SQS para entrega de mensagens. Para obter mais informações, consulte Preços do Amazon SQS.
- Amazon EventBridge — Esses custos derivam do EventBridge envio pela Amazon de notificações de objetos para endpoints de assinatura. Para obter mais informações, consulte os EventBridgepreços da Amazon.
- AWS Glue — Os custos mensais são determinados pelo volume de dados de log e eventos ingeridos dos AWS serviços por gigabyte. Seus dados são armazenados no Amazon Simple Storage Service e as cobranças padrão do Amazon S3 são aplicadas. O Security Lake também orquestra outros AWS serviços em seu nome. Você incorrerá em cobranças separadas pelos AWS serviços usados e pelos recursos configurados como parte do seu data lake de segurança. Veja os preços para Amazon AWS Glue EventBridgeAWS Lambda, Amazon SQS e Amazon Simple Notification Service. Você é responsável pelos custos incorridos ao consultar dados do Security Lake e armazenar os resultados da consulta.

Os custos incorridos por um assinante ao consultar dados do Security Lake e armazenar os resultados da consulta são de responsabilidade do assinante.

Para obter uma lista completa de custos e serviços auxiliares, consulte os preços do Security Lake.

Como analisar o uso e os custos estimados do Security Lake

A página Uso do console do Amazon Security Lake permite que você revise seu uso atual do Security Lake, bem como estimativas futuras de uso e custo. Se você está participando atualmente de um teste gratuito de 15 dias, seu uso durante o teste pode ajudá-lo a estimar seus custos de uso do Security Lake após o término do teste gratuito. Para ter uma visão geral dos preços do Security Lake, consulte Como os preços do Security Lake são determinados. Para obter informações detalhadas e exemplos de custos, consulte Preços do Amazon Security Lake.

No Security Lake, os custos estimados do uso são relatados em dólares americanos e se aplicam somente à Região da AWS atual. Os custos cobrem o uso do Security Lake por todas as contas em sua organização e incluem a conversão para o formato Open Cybersecurity Schema Framework (OCSF) e Apache Parquet. No entanto, os custos previstos não incluem custos de outros serviços com os quais o Security Lake trabalha, como o Amazon Simple Storage Service (Amazon S3) e o AWS Glue.

Na página Uso, você escolhe visualizar dados de uso e custo por período. O período padrão é o último dia corrido. Você deve ter pelo menos 1 dia de uso do Security Lake para ver as projeções de custo.

A parte superior da página mostra o Custo projetado para todas as contas. Esse é o custo previsto do Security Lake atualmente Região da AWS para os próximos 30 dias corridos, com base no seu uso real durante o período selecionado. O uso real e o custo previsto refletem todas as contas em sua organização.

No restante da página, os dados de uso e custo são divididos em duas tabelas da seguinte forma:

- Uso e custo por fonte: esse é o uso atual do Security Lake detalhado por fonte de dados, bem como o uso e os custos estimados para os próximos 30 dias corridos com base no seu uso real durante o período selecionado. O uso real, o uso previsto e o custo previsto refletem todas as contas da sua organização. Se você selecionar uma fonte, um painel dividido será aberto, mostrando quais contas geraram logs e eventos dessa fonte. Para cada conta, o painel dividido inclui o uso real dessa fonte e o uso e os custos previstos.
- Uso e custo por conta: esse é o uso atual do Security Lake detalhado por conta, bem como o uso e os custos estimados para os próximos 30 dias corridos com base no seu uso real durante o período selecionado. Se você selecionar uma conta, um painel dividido será aberto, mostrando

as fontes que contribuíram para o uso dessa conta. Para cada fonte contribuinte, o painel dividido inclui o uso real e o uso e os custos previstos.

Todas as fontes de AWS dados compatíveis aparecem nas tabelas anteriores, mesmo que você não tenha adicionado uma fonte específica no Security Lake. Recomendamos adicionar todas as AWS fontes se você estiver participando do teste gratuito para obter estimativas de custo para seu conjunto completo de registros e eventos. Para obter instruções sobre como adicionar uma AWS fonte, consulteColetando dados Serviços da AWS do Security Lake. As fontes personalizadas não estão incluídas nos cálculos de uso nem de custo.

Siga estas etapas para analisar seus dados de uso e custo no console do Security Lake.

Para analisar o uso do Security Lake e os custos previstos (console)

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região na qual você deseja revisar seu uso e custos.
3. No painel de navegação, escolha Configurações e, em seguida, Uso.
4. Selecione o período para o qual você deseja ver dados de uso e custo. O padrão é o último dia corrido.
5. Selecione a guia Por fonte de dados ou Por contas para analisar o uso e os custos em detalhes.

Regiões e endpoints do Security Lake

Para obter uma lista de regiões e endpoints de serviço compatíveis com o Amazon Security Lake, consulte Endpoints do Amazon Security Lake no Referência geral da AWS.

Recomendamos a habilitação do Security Lake em todas as Regiões da AWS compatíveis. Isso permite que você use o Security Lake para detectar e investigar atividades não autorizadas ou incomuns, mesmo em regiões que você não está usando ativamente.

Como desativar o Security Lake

Quando você desabilita o Amazon Security Lake, o Security Lake para de coletar logs e eventos das suas fontes da AWS . As configurações existentes do Security Lake e os recursos que foram criados na Conta da AWS são mantidos. Além disso, os dados que você armazenou ou publicou para outras Serviços da AWS pessoas, como dados confidenciais em AWS Lake Formation tabelas e AWS CloudTrail registros, permanecem disponíveis. Os dados armazenados no bucket do Amazon Simple Storage Service (Amazon S3) permanecem disponíveis de acordo com o ciclo de vida de armazenamento do Amazon S3.

A desativação do Security Lake na página Configurações no console do Security Lake interrompe a coleta de AWS registros e eventos Regiões da AWS em todos os quais o Security Lake está ativado no momento. Você pode usar a página Regiões no console para interromper a coleta de log em regiões específicas. A API Security Lake AWS CLI também interrompe a coleta de registros nas regiões que você especifica em sua solicitação.

Se você usa a integração com AWS Organizations e sua conta faz parte de uma organização que gerencia centralmente várias contas do Security Lake, somente o administrador delegado do Security Lake pode desativar o Security Lake para si mesmo e para as contas dos membros. No entanto, sair de uma organização interrompe a coleta de log de uma conta de membro.

Quando você desabilita o Security Lake de uma organização, a designação de administrador delegado é mantida se você seguir as instruções de desabilitação fornecidas nesta página. Você não precisa designar o administrador delegado novamente antes de poder reabilitar o Security Lake.

Se você configurou uma ou mais fontes personalizadas no Security Lake e desabilitou o serviço, também deverá desabilitar cada fonte independentemente do Security Lake. Caso contrário, a fonte personalizada continuará enviando registros para o Amazon S3. Além disso, você deve desabilitar a integração de um assinante ou o assinante ainda poderá consumir dados do Security Lake. Para obter detalhes sobre como remover a integração de uma fonte personalizada ou de assinante, consulte a documentação do respectivo provedor.

> **Important**
>
> Se você desativar o Security Lake, exclua também AWS Glue os recursos existentes do seu data lake. Caso contrário, a consulta subsequente não funcionará corretamente se você ativar o Security Lake novamente mais tarde. Embora a exclusão de AWS Glue recursos seja

um requisito primário, as organizações têm flexibilidade na forma como gerenciam recursos adicionais associados ao data lake.
Se você optar por remover recursos além dos AWS Glue componentes, é fundamental seguir uma abordagem do tipo “tudo ou nada”. Se você decidir excluir recursos auxiliares, deverá remover de forma abrangente todos os componentes associados. Esses recursos adicionais incluem: Security Lake SQS Queues (`AmazonSecurityLakeManager-xxx`), a função Security Lake Lambda, mapeamentos de origem de eventos e funções relacionadas do IAM, como a função. `AmazonSecurityLakeMetaStoreManagerV2`
Durante esse processo, você não precisa remover os buckets do Amazon S3 que armazenam dados para o data lake. As organizações podem reter esses compartimentos sem afetar o procedimento de limpeza. A principal consideração é evitar a remoção parcial de recursos, o que poderia causar problemas de configuração em futuras implantações.
Ao planejar a desativação do seu data lake, avalie cuidadosamente se você deseja remover somente os AWS Glue recursos ou realizar uma limpeza completa dos recursos. Se você optar pela remoção abrangente, siga um processo de exclusão sistemático e remova todos os componentes associados.

Quando o Security Lake é reativado, um novo data lake é criado em um novo bucket do Amazon S3 e os dados são coletados nesse novo bucket do S3. Se você tiver excluído AWS Glue tabelas anteriormente, um novo conjunto de AWS Glue tabelas será criado.

Todos os dados coletados antes da desativação do Security Lake permanecerão no bucket anterior do Amazon S3. Se quiser consultar dados antigos, você deve mover os dados para o novo bucket usando o comando Amazon S3`Sync`. Para obter mais detalhes, consulte o comando Sync na Referência de AWS CLI comandos.

Este tópico explica como desabilitar o Security Lake usando o console do Security Lake, a API do Security Lake ou AWS CLI.

Console

1. Abra o console do Security Lake em https://console.aws.amazon.com/securitylake/.
2. No painel de navegação, em Configurações, selecione Geral.
3. Escolha Desabilitar o Security Lake.
4. Quando a confirmação for solicitada, insira **`Disable`** e escolha Desabilitar.

API

Para desativar o Security Lake programaticamente, use a DeleteDataLakeoperação da API do Security Lake. Se você estiver usando o AWS CLI, execute o delete-date-lakecomando. Em sua solicitação, use a `regions` lista para especificar o código da região para cada região na qual você deseja desativar o Security Lake. Para obter uma lista de códigos de região, consulte Endpoints do Amazon Security Lake na Referência geral da AWS.

Para uma implantação do Security Lake utilizando AWS Organizations, somente o administrador delegado do Security Lake da organização pode desativar o Security Lake para contas na organização.

Por exemplo, o AWS CLI comando a seguir desativa o Security Lake nas `eu-central-1` regiões `ap-northeast-1` e. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

Histórico do documento do Guia do usuário do Amazon Security Lake

A tabela a seguir descreve as alterações importantes na documentação desde a última versão do Amazon Security Lake. Para receber notificações sobre atualizações dessa documentação, é possível inscrever-se em um feed RSS.

Última atualização da documentação: 24 de abril de 2025

Alteração	Descrição	Data
Política gerenciada atualizada	O Security Lake atualizou a política gerenciada `SecurityLakeResourceManagementServiceRolePolicy` para adicionar `lambda:DeleteFunction` permissão para funções obsoletas do SecurityLake _Glue_Partition_Updater_Lambda. Isso permite que o Security Lake limpe as funções obsoletas do Lambda como parte da migração para fontes v2 e formato iceberg. Para obter informações, consulte Atualizações do Security Lake para políticas AWS gerenciadas.	18 de novembro de 2025
Permissão de função vinculada ao serviço atualizada	O Security Lake atualizou o `StringLike` substituindo AWSServiceRoleForSecurityLakeResourceManagementpor`ArnLike`.	25 de setembro de 2025

Funcionalidade atualizada - função vinculada ao serviço	O Security Lake agora cria automaticamente a AWSServiceRoleForSecurityLakeResourceManagement SLR durante a criação do data lake. Para obter mais informações, consulte Considerações.	24 de abril de 2025
Tópico significativamente reescrito - integrações AWS	Atualizou o conteúdo que especifica a integração do Security Lake com o específico Serviços da AWS. Para obter mais informações, consulte AWS service (Serviço da AWS) integrações.	31 de março de 2025
Funcionalidade atualizada - Gerenciamento de várias contas	O console do Security Lake agora oferece suporte ao gerenciamento da configuração de ativação automática para contas quando elas ingressam na sua organização. Para obter mais informações, consulte Editando a configuração da nova conta no console.	10 de março de 2025
Funcionalidade atualizada - Proteção de dados em AWS WAF registros	Foi adicionado suporte para proteção de dados quando ativado na Web ACL para contas do Security Lake. Para obter mais informações, consulte AWS WAF registros no Security Lake.	17 de fevereiro de 2025

Novo recurso - Suporte adicionado aos endpoints da VPC	O Security Lake agora está integrado AWS PrivateLink e oferece suporte a endpoints VPC. Para obter mais informações sobre a AWS PrivateLink integração, consulte Amazon Security Lake e a interface VPC endpoints ().AWS PrivateLink	4 de fevereiro de 2025
Novo atributo	O Security Lake agora oferece suporte à consulta direta do OpenSearch Service para analisar dados no Security Lake. Para obter mais detalhes, consulte Integração com o OpenSearch serviço.	1.º de dezembro de 2024
Nova função vinculada ao serviço	Adicionamos uma nova função vinculada ao serviço. `AWSServiceRoleForSecurityLakeResourceManagement` Essa função vinculada ao serviço fornece permissões ao Security Lake para realizar melhorias contínuas de monitoramento e desempenho, o que pode reduzir a latência e os custos.	14 de novembro de 2024

Disponibilidade regional	O Security Lake agora está disponível no AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA). Regiões da AWS Para obter uma lista completa das regiões em que o Security Lake está disponível atualmente, consulte Amazon Security Lake endpoints no Referência geral da AWS.	10 de junho de 2024
Atualização de política gerenciada existente	Adicionamos AWS WAF ações à política AWS gerenciada para a `SecurityLakeServiceLinkedRole` política. As ações adicionais permitem que o Security Lake colete AWS WAF registros, quando está habilitado como uma fonte de log no Security Lake.	22 de maio de 2024
Nova fonte AWS de registro	O Security Lake adicionou os registros do AWS WAF como uma fonte de AWS registro. AWS WAF ajuda você a monitorar as solicitações da web que os usuários finais enviam aos aplicativos.	22 de maio de 2024
Atualização de política gerenciada existente	Adicionamos ações de SID à `AmazonSecurityLakePermissionsBoundary` política.	13 de maio de 2024

Atualização de política gerenciada existente	Atualizamos a AmazonSecurityLakeMetastoreManagerpolítica para adicionar uma ação de limpeza de metadados que permite excluir os metadados em seu data lake.	27 de março de 2024
Novas versões de origem	Atualize suas permissões de função para ingerir dados das novas versões da fonte de dados.	29 de fevereiro de 2024
Nova fonte AWS de registro	O Security Lake adicionou os registros de auditoria do EKS como fonte de AWS registro. Os registros de auditoria do EKS ajudam você a detectar atividades potencialmente suspeitas em seus clusters do EKS no Amazon Elastic Kubernetes Service.	29 de fevereiro de 2024
Atualização de política gerenciada existente	Atualizamos a política para permitir `iam:PassRole` a nova `AmazonSecurityLakeMetastoreManagerV2` função e permitir que o Security Lake implante ou atualize componentes do data lake.	23 de fevereiro de 2024

Nova política gerenciada	Adicionamos uma nova política gerenciada pela AWS, a política `AmazonSecurityLakeMetastoreManager` . Essa política concede permissões para o Security Lake gerenciar metadados em seu data lake.	23 de janeiro de 2024
Disponibilidade regional	O Security Lake agora está disponível nas seguintes regiões Regiões da AWS: Ásia-Pacífico (Osaka), Canadá (Central), Europa (Paris) e Europa (Estocolmo). Para obter uma lista completa das regiões em que o Security Lake está disponível atualmente, consulte Amazon Security Lake endpoints no Referência geral da AWS.	26 de outubro de 2023
Novos recursos	Agora você pode editar determinadas configurações para assinantes com acesso de consulta. Você também pode atribuir tags aos recursos do Security Lake para sua Conta da AWS.	20 de julho de 2023

Nova política gerenciada	O Security Lake adicionou uma nova política AWS gerenciada, a `AmazonSecurityLakeAdministrator` política. Essa política concede permissões administrativas que oferecem à entidade principal acesso total a todas as ações do Security Lake.	30 de maio de 2023
Disponibilidade geral	O Security Lake agora está disponível para o público.	30 de maio de 2023
Novo atributo	O Security Lake agora envia métricas para a Amazon CloudWatch.	4 de maio de 2023
Disponibilidade regional	O Security Lake agora está disponível nas seguintes regiões Regiões da AWS: Ásia-Pacífico (Cingapura), Europa (Londres) e América do Sul (São Paulo).	22 de março de 2023
Novo atributo	O Security Lake agora cria funções AWS Identity and Access Management (IAM) em seu nome quando você usa o console do Security Lake para ativar e começar a usar o Security Lake.	15 de fevereiro de 2023
Lançamento inicial	Esta é versão inicial do Guia do usuário do Amazon Security Lake.	29 de novembro de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.