aws

Guida per l'utente

Amazon Security Lake

Amazon Security Lake: Guida per l'utente

Table of Contents

Cos'è Amazon Security Lake?

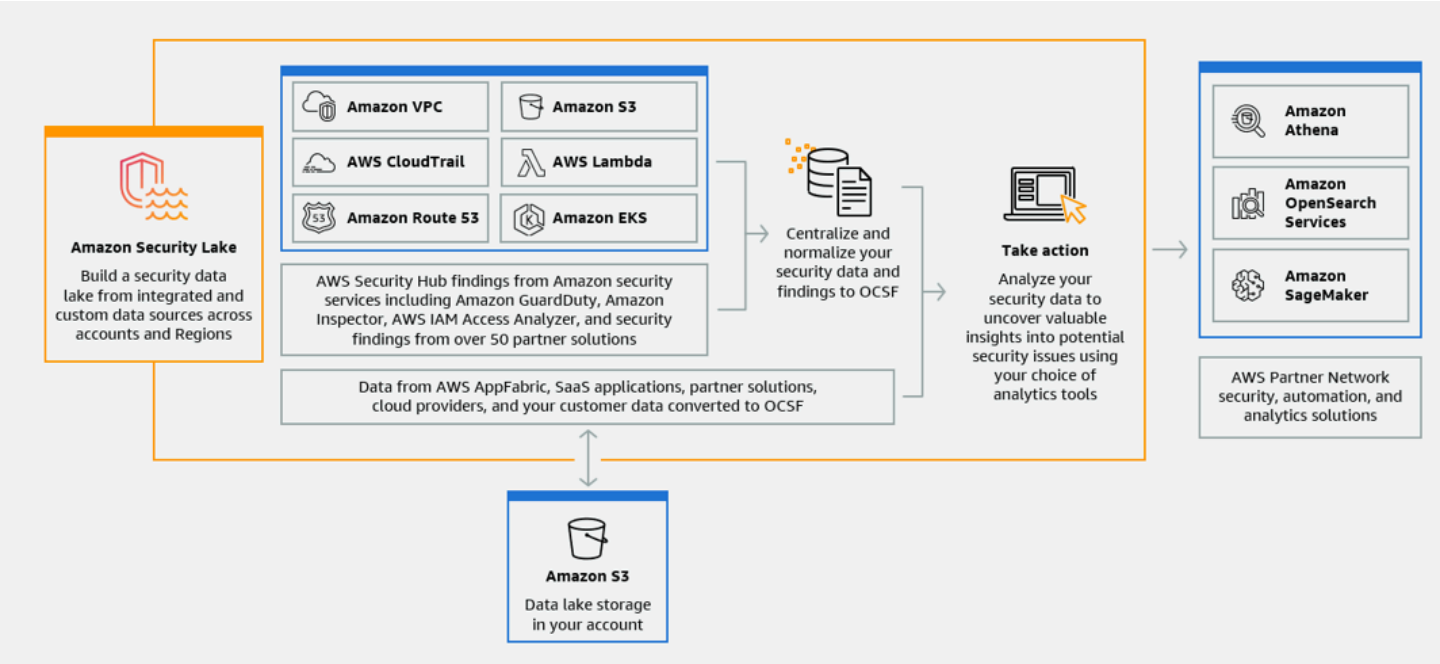
Amazon Security Lake è un servizio di data lake di sicurezza completamente gestito. Puoi utilizzare Security Lake per centralizzare automaticamente i dati di sicurezza provenienti da AWS ambienti, provider SaaS, locali, fonti cloud e fonti di terze parti in un data lake appositamente creato e archiviato nel tuo. Account AWS Security Lake ti aiuta ad analizzare i dati di sicurezza, in modo da ottenere una comprensione più completa del tuo livello di sicurezza in tutta l'organizzazione. Con Security Lake, puoi anche migliorare la protezione dei tuoi carichi di lavoro, applicazioni e dati.

Il data lake è supportato dai bucket Amazon Simple Storage Service (Amazon S3) e tu mantieni la proprietà dei tuoi dati.

Security Lake automatizza la raccolta di dati di log ed eventi relativi alla sicurezza da servizi integrati Servizi AWS e di terze parti. Consente inoltre di gestire il ciclo di vita dei dati con impostazioni di conservazione e replica personalizzabili. Security Lake converte i dati acquisiti nel formato Apache Parquet e in uno schema open source standard chiamato Open Cybersecurity Schema Framework (OCSF). Con il supporto OCSF, Security Lake normalizza e combina i dati di sicurezza provenienti da AWS un'ampia gamma di fonti di dati sulla sicurezza aziendale.

Altri servizi Servizi AWS e di terze parti possono sottoscrivere i dati archiviati in Security Lake per la risposta agli incidenti e l'analisi dei dati di sicurezza.

Panoramica di Security Lake



Caratteristiche di Security Lake

Ecco alcuni modi chiave in cui Security Lake ti aiuta a centralizzare, gestire e sottoscrivere i dati di log ed eventi relativi alla sicurezza.

Aggregazione dei dati nel tuo account

Security Lake crea un data lake di sicurezza appositamente creato nel tuo account. Security Lake raccoglie dati di log ed eventi da fonti di dati cloud, locali e personalizzate in tutti gli account e le regioni. Il data lake è supportato dai bucket Amazon Simple Storage Service (Amazon S3) e tu mantieni la proprietà dei tuoi dati.

Varietà di fonti di log ed eventi supportate

Security Lake raccoglie registri ed eventi di sicurezza da più fonti, inclusi servizi locali e di terze Servizi AWS parti. Dopo aver inserito i log, indipendentemente dalla fonte, puoi accedervi centralmente e gestirne il ciclo di vita. Per informazioni dettagliate sulle fonti da cui i registri e gli eventi vengono raccolti da Security Lake, vedere Gestione del codice in Amazon Security Lake

Trasformazione e normalizzazione dei dati

Security Lake partiziona automaticamente i dati in ingresso da supporti nativi Servizi AWS e li converte in un formato Parquet efficiente per l'archiviazione e le query. Trasforma inoltre i dati da supporto nativo Servizi AWS allo schema open source Open Cybersecurity Schema Framework (OCSF). Ciò rende i dati compatibili con altri fornitori Servizi AWS e di terze parti senza la necessità di post-elaborazione. Poiché Security Lake normalizza i dati, molte soluzioni di sicurezza possono utilizzarli in parallelo.

Livelli di accesso multipli per gli abbonati

Gli abbonati consumano i dati archiviati in Security Lake. Puoi scegliere il livello di accesso di un abbonato ai tuoi dati. Gli abbonati possono utilizzare i dati solo dalle fonti e neiRegioni AWS, specificati dall'utente. Gli abbonati possono ricevere automaticamente una notifica dei nuovi oggetti man mano che vengono scritti nel data lake. In alternativa, gli abbonati possono interrogare i dati dal data lake. Security Lake crea e scambia automaticamente le credenziali necessarie tra Security Lake e l'abbonato.

Gestione dei dati su più account e aree geografiche

Puoi abilitare Security Lake centralmente in tutte le regioni in cui è disponibile e in più regioniAccount AWS. In Security Lake, puoi anche designare regioni cumulative per consolidare i

dati dei registri di sicurezza e degli eventi di più regioni. Questo può aiutarti a rispettare i requisiti di conformità in materia di residenza dei dati.

Configurabile e personalizzabile

Security Lake è un servizio configurabile e personalizzabile. È possibile specificare per quali fonti, account e regioni si desidera configurare la raccolta dei registri. Puoi anche specificare il livello di accesso di un abbonato al data lake.

Gestione e ottimizzazione del ciclo di vita dei dati

Security Lake gestisce il ciclo di vita dei dati con impostazioni di conservazione personalizzabili e costi di archiviazione con una suddivisione automatizzata dello storage su più livelli. Security Lake partiziona e converte automaticamente i dati di sicurezza in ingresso in un formato Apache Parquet efficiente per l'archiviazione e l'interrogazione.

Accesso a Security Lake

Per un elenco delle regioni in cui Security Lake è attualmente disponibile, consultaRegioni ed endpoint Amazon Security Lake Lake Lake. Per ulteriori informazioni sulle regioni, consulta gli endpoint del AWS servizio nel Riferimenti generali di AWS.

In ogni regione, puoi accedere a Security Lake in uno dei seguenti modi:

AWS Management Console

AWS Management ConsoleÈ un'interfaccia basata su browser che è possibile utilizzare per creare e gestire AWS risorse. La console Security Lake fornisce l'accesso all'account e alle risorse di Security Lake. È possibile eseguire la maggior parte delle attività di Security Lake utilizzando la console Security Lake.

API Security Lake

Per accedere a Security Lake in modo programmatico, utilizza l'API Security Lake ed invia richieste HTTPS direttamente al servizio. Per ulteriori informazioni, consulta il Security Lake API Reference.

AWS Command Line Interface (AWS CLI)

Con ilAWS CLI, puoi impartire comandi dalla riga di comando del tuo sistema per eseguire attività e AWS attività di Security Lake. L'uso della riga di comando può essere più rapido e conveniente rispetto all'utilizzo della console. Gli strumenti a riga di comando sono inoltre utili per creare script

che eseguono le attività di . Per informazioni sull'installazione e sull'utilizzo di AWS CLI, consulta AWS Command Line Interface.

SDK AWS

AWSfornisce SDK composti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, come Java, Go, Python, C++ e.NET. Gli SDK forniscono un accesso comodo e programmatico a Security Lake e ad altri. Servizi AWS Gestiscono anche attività come la firma crittografica delle richieste, la gestione degli errori e i tentativi di ripetere automaticamente le richieste. Per informazioni sull'installazione e l'uso degli AWS SDK, consulta Strumenti su AWS cui costruire.

Servizi correlati

Di seguito sono riportati altri Servizi AWS che Security Lake utilizza:

- Amazon EventBridge: Security Lake viene utilizzato EventBridge per notificare agli abbonati quando gli oggetti vengono scritti nel data lake.
- AWS Glue— Security Lake utilizza AWS Glue i crawler per creare le AWS Glue Data Catalog tabelle e inviare dati appena scritti al Data Catalog. Security Lake memorizza anche i metadati delle partizioni per le AWS Lake Formation tabelle nel Data Catalog.
- AWS Lake Formation— Security Lake crea una tabella Lake Formation separata per ogni fonte che fornisce dati a Security Lake. Le tabelle Lake Formation contengono informazioni sui dati provenienti da ciascuna fonte, tra cui informazioni sullo schema, sulla partizione e sulla posizione dei dati. Gli abbonati hanno la possibilità di utilizzare i dati interrogando le tabelle di Lake Formation.
- AWS Lambda— Security Lake utilizza le funzioni Lambda per supportare processi di estrazione, trasformazione e caricamento (ETL) su dati grezzi e per registrare le partizioni in cui inserire i dati di origine. AWS Glue
- Amazon S3: Security Lake archivia i tuoi dati come oggetti Amazon S3. Le classi di storage e le impostazioni di conservazione si basano sulle offerte Amazon S3. Security Lake non supporta Amazon S3 Select.

Security Lake raccoglie dati da fonti personalizzate oltre a quanto segue: Servizi AWS

- AWS CloudTrailgestione ed eventi relativi ai dati (S3, Lambda)
- Log di query di Amazon Route 53 Resolver

- Risultati AWS Security Hub
- Registri di flusso di Amazon Virtual Private Cloud (Amazon VPC)

Per ulteriori informazioni su queste fonti, vedereRaccolta di dati dai AWS servizi. Puoi utilizzare gli oggetti Amazon S3 nel tuo data lake di sicurezza creando un abbonato in grado di leggere i dati nello schema OCSF. Puoi anche interrogare i dati utilizzando Amazon Athena, Amazon Redshift e servizi in abbonamento di terze parti che si integrano con. AWS Glue

Concetti e terminologia

Questa sezione descrive i concetti e i termini chiave per aiutarti a usare Amazon Security Lake.

Regione contribuente

Uno o piùRegioni AWS che forniscono dati a una regione cumulativa.

lake

I dati persistenti archiviati in Amazon Simple Storage Service (Amazon S3) e gestiti da Security lake. Security Lake utilizzaAWS Glue per inviare dati appena scritti al catalogo dati. Security Lake crea anche unaAWS Lake Formation tabella per ogni fonte che fornisce dati al data lake. Un data lake in genere memorizza quanto segue:

- Dati strutturati e non strutturati
- Dati grezzi e trasformati

Security Lake è un servizio di data lake progettato per raccogliere registri ed eventi relativi alla sicurezza.

Struttura aperta dello schema di sicurezza informatica (OCSF)

Uno schema open source standardizzato per registri ed eventi di sicurezza. È stato sviluppato daAWS e da altri leader del settore della sicurezza in vari domini di sicurezza. Security Lake converte automaticamente i registri e gli eventi daServizi AWS cui raccoglie nello schema OCSF. Le fonti personalizzate convertono i log e gli eventi in OCSF prima di inviarli a Security Lake.

Regione di rollup

ERegione AWS che consolida i registri e gli eventi di sicurezza di una o più regioni contribuenti. Specificare una o più regioni di rollup può aiutarti a soddisfare i requisiti di conformità regionali.

Origine

Un insieme di registri ed eventi generati da un singolo sistema che corrisponde a una classe di eventi specifica in OCSF. Secdata lake. Una fonte può essere un altro servizioServizio AWS o un servizio di terze parti. Per le fonti di terze parti, è necessario convertire i dati nello schema OCSF prima di inviarli a Security Lake.

Sottoscrittore

Un servizio che utilizza registri ed eventi da Security Lake. Un abbonato può essere un altro servizioServizio AWS o un servizio di terze parti.

Guida introduttiva ad Amazon Security Lake

Questa sezione spiega come abilitare e iniziare a utilizzare Security Lake. Imparerai come configurare le impostazioni del data lake e configurare la raccolta dei log. Puoi abilitare e utilizzare Security Lake tramite AWS Management Console o a livello di codice. Indipendentemente dal metodo utilizzato, è necessario innanzitutto configurare un utente Account AWS e un utente amministrativo. I passaggi successivi variano in base al metodo di accesso. La console Security Lake offre un processo semplificato per iniziare e crea tutti i ruoli AWS Identity and Access Management (IAM) necessari per creare il data lake.

Configurazione iniziale Account AWS

Iscriviti per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Creazione di un utente amministratore

Dopo la registrazione Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accesso come utente root della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In Centro identità AWS IAM, assegna l'accesso amministrativo a un utente amministrativo.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Identifica l'account che utilizzerai per abilitare Security Lake

Security Lake si integra AWS Organizations per gestire la raccolta dei log su più account di un'organizzazione. Se si desidera utilizzare Security Lake per un'organizzazione, è necessario utilizzare l'account di gestione Organizations per designare un amministratore delegato di Security Lake. Quindi, è necessario utilizzare le credenziali dell'amministratore delegato per abilitare

Security Lake, aggiungere account membro e abilitare Security Lake per tali account. Per ulteriori informazioni, consulta Gestione di più account con AWS Organizations.

In alternativa, puoi utilizzare Security Lake senza l'integrazione Organizations per un account autonomo che non fa parte di un'organizzazione.

Considerazioni sull'abilitazione di Amazon Security Lake

Prima di abilitare Security Lake, considera quanto segue:

- Security Lake offre funzionalità di gestione interregionale, il che significa che puoi creare il tuo data lake e configurare la raccolta dei log in tutto Regioni AWS il mondo. Per abilitare Security Lake in tutte le regioni supportate, puoi scegliere qualsiasi endpoint regionale supportato. Puoi anche aggiungere regioni di rollup per aggregare i dati di più regioni in un'unica regione.
- Ti consigliamo di attivare Security Lake in tutte le piattaforme supportate. Regioni AWS In questo modo, Security Lake può raccogliere dati collegati ad attività non autorizzate o insolite anche nelle regioni che non utilizzi attivamente. Se Security Lake non è attivato in tutte le regioni supportate, la sua capacità di raccogliere dati da altri servizi utilizzati in più regioni è ridotta.
- Quando abiliti Security Lake per la prima volta in qualsiasi regione, viene creato un ruolo collegato al servizio per il tuo account chiamato. `AWSServiceRoleForSecurityLake` Questo ruolo include le autorizzazioni per chiamare altre persone per tuo Servizi AWS conto e gestire il security data lake. Per ulteriori informazioni su come funzionano i ruoli collegati ai servizi, consulta Using service-linked roles nella IAM User Guide. Se abiliti Security Lake come amministratore delegato di Security Lake, Security Lake crea il ruolo collegato al servizio in ogni account membro dell'organizzazione.
- Security Lake non supporta Amazon S3 Object Lock. Quando vengono creati i bucket di data lake, S3 Object Lock è disabilitato per impostazione predefinita. L'abilitazione di Object Lock su un bucket interrompe la consegna di dati di log normalizzati al data lake.

Guida introduttiva alla console

Questo tutorial spiega come abilitare e configurare Security Lake tramite AWS Management Console. Come parte di AWS Management Console, la console Security Lake offre un processo semplificato per iniziare e crea tutti i ruoli AWS Identity and Access Management (IAM) necessari per creare il data lake.

Fase 1: Configurare le fonti

Security Lake raccoglie dati di log ed eventi da una varietà di fonti e da tutto il tuo Account AWS territorio. Regioni AWS Segui queste istruzioni per identificare quali dati vuoi che Security Lake raccolga. Puoi usare queste istruzioni solo per aggiungere una fonte supportata nativamente Servizio AWS . Per informazioni sull'aggiunta di una fonte personalizzata, consulta. Raccolta di dati da fonti personalizzate

Per configurare la raccolta di sorgenti di log

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, selezionate una regione. Puoi abilitare Security Lake nella regione corrente e in altre regioni durante l'onboarding.
3. Scegliere Iniziare.
4. Per Seleziona sorgenti di log ed eventi, scegli una delle seguenti opzioni:

    a. Inserisci AWS fonti predefinite: quando scegli l'opzione consigliata, gli eventi di dati CloudTrail S3 non sono inclusi per l'ingestione. Questo perché l'ingestione di un volume elevato di eventi di dati CloudTrail - S3 potrebbe influire in modo significativo sui costi di utilizzo. Per importare questa fonte, seleziona l'opzione Inserisci fonti specifiche. AWS

    b. Inserisci AWS fonti specifiche: con questa opzione, puoi selezionare una o più fonti di log ed eventi che desideri importare.

    > **Note**
    >
    > Quando abiliti Security Lake in un account per la prima volta, tutte le fonti di log ed eventi selezionate faranno parte di un periodo di prova gratuito di 15 giorni. Per ulteriori informazioni sulle statistiche di utilizzo, vedereAnalisi dell'utilizzo e dei costi stimati.

5. Per Versioni, scegli la versione dell'origine dati da cui desideri importare le fonti di registro e di eventi.

> **Important**
>
> Se non disponi delle autorizzazioni di ruolo necessarie per abilitare la nuova versione dell'origine del AWS registro nella regione specificata, contatta l'amministratore di Security Lake. Per ulteriori informazioni, consulta Aggiornare le autorizzazioni dei ruoli.

6. Per Select Regions, scegli se importare le fonti di log ed eventi da tutte le regioni supportate o da regioni specifiche. Se scegli Regioni specifiche, seleziona le regioni da cui importare i dati.
7. Per accedere al servizio, crea un nuovo ruolo IAM o utilizza un ruolo IAM esistente che autorizzi Security Lake a raccogliere dati dalle tue fonti e aggiungerli al tuo data lake. Un ruolo viene utilizzato in tutte le regioni in cui abiliti Security Lake.
8. Seleziona Avanti.

Fase 2: Definizione delle impostazioni di archiviazione e delle regioni di rollup (opzionale)

Puoi specificare la classe di storage Amazon S3 in cui desideri che Security Lake memorizzi i tuoi dati e per quanto tempo. Puoi anche specificare una regione di rollup per consolidare i dati provenienti da più regioni. Questi sono passaggi facoltativi. Per ulteriori informazioni, consulta Gestione del ciclo di vita in Security Lake.

Per configurare le impostazioni di archiviazione e rollup

1. Se desideri consolidare i dati di più regioni contribuenti in una regione di rollup, per Seleziona regioni di rollup, scegli Aggiungi regione di rollup. Specificate la regione di rollup e le regioni che vi contribuiranno. È possibile configurare una o più regioni di rollup.
2. Per le classi di storage Select, scegli una classe di storage Amazon S3. La classe di storage predefinita è S3 Standard. Fornisci un periodo di conservazione (in giorni) se desideri che i dati passino a un'altra classe di archiviazione dopo tale periodo e scegli Aggiungi transizione. Al termine del periodo di conservazione, gli oggetti scadono e Amazon S3 li elimina. Per ulteriori informazioni sulle classi di storage e sulla conservazione di Amazon S3, consulta. Gestione della conservazione
3. Se hai selezionato una regione di rollup nel primo passaggio, per l'accesso al servizio, crea un nuovo ruolo IAM o utilizza un ruolo IAM esistente che autorizzi Security Lake a replicare i dati su più regioni.

4. Seleziona Avanti.

Fase 3: Rivedi e crea un data lake

Controlla le fonti da cui Security Lake raccoglierà i dati, le tue regioni di rollup e le tue impostazioni di conservazione. Quindi, crea il tuo data lake.

Per rivedere e creare il data lake

1. Durante l'attivazione di Security Lake, esamina le sorgenti di log ed eventi, le regioni, le regioni di rollup e le classi di archiviazione.
2. Scegli Crea.

Dopo aver creato il data lake, verrà visualizzata la pagina di riepilogo sulla console di Security Lake. Questa pagina fornisce una panoramica del numero di regioni e aree di rollup, informazioni sugli abbonati e sui problemi.

Il menu Problemi mostra un riepilogo dei problemi degli ultimi 14 giorni che hanno avuto un impatto sul servizio Security Lake o sui bucket Amazon S3. Per ulteriori dettagli su ogni problema, puoi andare alla pagina Problemi della console Security Lake.

Passaggio 4: Visualizza e interroga i tuoi dati

Dopo aver creato il tuo data lake, puoi utilizzare Amazon Athena o servizi simili per visualizzare e interrogare i tuoi dati da AWS Lake Formation database e tabelle. Quando usi la console, Security Lake concede automaticamente le autorizzazioni di visualizzazione del database al ruolo che utilizzi per abilitare Security Lake. Come minimo, il ruolo deve disporre delle autorizzazioni di analista dei dati. Per ulteriori informazioni sui livelli di autorizzazione, consulta Lake Formation personas e IAM permissions reference. Per istruzioni sulla concessione *SELECT* delle autorizzazioni, consulta Concessione delle autorizzazioni di Data Catalog utilizzando il metodo della risorsa denominata nella Guida per gli sviluppatori. AWS Lake Formation

Fase 5: Creare abbonati

Dopo aver creato il data lake, puoi aggiungere abbonati per utilizzare i tuoi dati. Gli abbonati possono utilizzare i dati accedendo direttamente agli oggetti nei bucket Amazon S3 o interrogando il data lake. Per ulteriori informazioni sugli abbonati, consulta. Gestione degli abbonati in Amazon Security Lake

Iniziare a livello di programmazione

Questo tutorial spiega come abilitare e iniziare a utilizzare Security Lake a livello di codice. L'API Amazon Security Lake ti offre un accesso completo e programmatico al tuo account, ai dati e alle risorse di Security Lake. In alternativa, puoi utilizzare gli strumenti da riga di AWS comando, AWS Command Line Interfaceovvero gli AWS Strumenti per, PowerShell o gli AWS SDK per accedere a Security Lake.

Fase 1: Creare ruoli IAM

Se accedi a Security Lake in modo programmatico, è necessario creare alcuni ruoli AWS Identity and Access Management (IAM) per configurare il data lake.

> **Important**
>
> Non è necessario creare questi ruoli IAM se si utilizza la console Security Lake per abilitare e configurare Security Lake.

Devi creare ruoli in IAM se intendi intraprendere una o più delle seguenti azioni (scegli i link per visualizzare ulteriori informazioni sui ruoli IAM per ciascuna azione):

- Creazione di una fonte personalizzata: le fonti personalizzate sono fonti diverse da quelle supportate nativamente Servizi AWS che inviano dati a Security Lake.
- Creazione di un abbonato con accesso ai dati: gli abbonati con autorizzazioni possono accedere direttamente agli oggetti S3 dal data lake.
- Creazione di un abbonato con accesso tramite query: gli abbonati con autorizzazioni possono interrogare i dati da Security Lake utilizzando servizi come Amazon Athena.
- Configurazione di una regione di rollup: una regione di rollup consolida i dati provenienti da più regioni. Regioni AWS

Dopo aver creato i ruoli menzionati in precedenza, collega la policy AmazonSecurityLakeAdministrator AWS gestita al ruolo che stai utilizzando per abilitare Security Lake. Questa politica concede autorizzazioni amministrative che consentono a un preside di accedere a Security Lake e accedere a tutte le azioni di Security Lake.

Allega la policy AmazonSecurityLakeMetaStoreManager AWS gestita per creare il tuo data lake o interrogare i dati da Security Lake. Questa policy è necessaria affinché Security Lake supporti i

processi di estrazione, trasformazione e caricamento (ETL) su dati non elaborati di log ed eventi che riceve dalle fonti.

Passaggio 2: abilitare Amazon Security Lake

Per abilitare Security Lake a livello di codice, utilizza il CreateDataLakefunzionamento dell'API Security Lake. Se utilizzi il AWS CLI, esegui il comando. create-data-lake Nella richiesta, utilizzate il `region` campo dell'`configurations`oggetto per specificare il codice regionale per la regione in cui abilitare Security Lake. Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.

Esempio 1

Il comando di esempio seguente abilita Security Lake nelle `us-east-2` regioni `us-east-1` e. In entrambe le regioni, questo data lake è crittografato con chiavi gestite di Amazon S3. Gli oggetti scadono dopo 365 giorni e gli oggetti passano alla classe di storage `ONEZONE_IA` S3 dopo 60 giorni. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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"
```

Esempio 2

Il comando di esempio seguente abilita Security Lake nella `us-east-2` regione. Questo data lake è crittografato con una chiave gestita dal cliente creata in AWS Key Management Service (AWS KMS). Gli oggetti scadono dopo 500 giorni e gli oggetti passano alla classe di storage `GLACIER` S3 dopo 30 giorni. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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 hai già abilitato Security Lake e desideri aggiornare le impostazioni di configurazione per una regione o una fonte, usa l'UpdateDataLakeoperazione o, se usi il AWS CLI, il update-data-lakecomando. Non utilizzare l'`CreateDataLake`operazione.

Fase 3: Configurare le fonti

Security Lake raccoglie dati di log ed eventi da una varietà di fonti e da tutto il tuo Account AWS territorio. Regioni AWS Segui queste istruzioni per identificare quali dati vuoi che Security Lake raccolga. Puoi usare queste istruzioni solo per aggiungere una fonte supportata nativamente Servizio AWS . Per informazioni sull'aggiunta di una fonte personalizzata, consulta. Raccolta di dati da fonti personalizzate

Per definire una o più fonti di raccolta a livello di codice, utilizzate il CreateAwsLogSourcefunzionamento dell'API Security Lake. Per ogni fonte, specificate un valore unico a livello regionale per il parametro. `sourceName` Facoltativamente, utilizzate parametri aggiuntivi per limitare l'ambito della fonte a account specifici (`accounts`) o a una versione specifica (`sourceVersion`).

> **Note**
>
> Se non includi un parametro opzionale nella richiesta, Security Lake applica la richiesta a tutti gli account o a tutte le versioni della fonte specificata, a seconda del parametro che escludi. Ad esempio, se sei l'amministratore delegato di Security Lake di un'organizzazione ed escludi il `accounts` parametro, Security Lake applica la richiesta a tutti gli account dell'organizzazione. Analogamente, se si esclude il `sourceVersion` parametro, Security Lake applica la richiesta a tutte le versioni della fonte specificata.

Se la richiesta specifica una regione in cui non hai abilitato Security Lake, si verifica un errore. Per risolvere questo errore, assicurati che l'`regions`array specifichi solo le regioni in cui hai abilitato

Security Lake. In alternativa, puoi abilitare Security Lake nella regione e quindi inviare nuovamente la richiesta.

Quando abiliti Security Lake in un account per la prima volta, tutte le fonti di log ed eventi selezionate faranno parte di un periodo di prova gratuito di 15 giorni. Per ulteriori informazioni sulle statistiche di utilizzo, vedereAnalisi dell'utilizzo e dei costi stimati.

Fase 4: Configurazione delle impostazioni di archiviazione e delle regioni di rollup (opzionale)

Puoi specificare la classe di storage Amazon S3 in cui desideri che Security Lake memorizzi i tuoi dati e per quanto tempo. Puoi anche specificare una regione di rollup per consolidare i dati provenienti da più regioni. Questi sono passaggi facoltativi. Per ulteriori informazioni, consulta Gestione del ciclo di vita in Security Lake.

Per definire un obiettivo a livello di codice quando abiliti Security Lake, utilizza il CreateDataLakefunzionamento dell'API Security Lake. Se hai già abilitato Security Lake e desideri definire un obiettivo target, usa l'UpdateDataLakeoperazione, non l'`CreateDataLake`operazione.

Per entrambe le operazioni, utilizzate i parametri supportati per specificare le impostazioni di configurazione desiderate:

- Per specificare una regione di rollup, utilizzate il `region` campo per specificare la regione alla quale desiderate aggiungere dati alle regioni di rollup. Nell'`regions`array dell'`replicationConfiguration`oggetto, specificate il codice regionale per ogni regione di rollup. Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.
- Per specificare le impostazioni di conservazione dei dati, utilizza i `lifecycleConfiguration` parametri:
  - Per`transitions`, specifica il numero totale di giorni (`days`) in cui desideri archiviare gli oggetti S3 in una particolare classe `storageClass` di storage Amazon S3 ().
  - Per`expiration`, specifica il numero totale di giorni in cui desideri archiviare gli oggetti in Amazon S3, utilizzando qualsiasi classe di storage, dopo la creazione degli oggetti. Al termine di questo periodo di conservazione, gli oggetti scadono e Amazon S3 li elimina.

  Security Lake applica le impostazioni di conservazione specificate alla regione specificata nel `region` campo dell'oggetto. `configurations`

Ad esempio, il comando seguente crea un data lake con `ap-northeast-2` come regione di rollup. La `us-east-1` regione fornirà dati alla `ap-northeast-2` regione. Questo esempio stabilisce anche un periodo di scadenza di 10 giorni per gli oggetti che vengono aggiunti al 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"
```

Ora hai creato il tuo data lake. Utilizza il ListDataLakesfunzionamento dell'API Security Lake per verificare l'abilitazione di Security Lake e delle impostazioni del data lake in ogni regione.

Se si verificano problemi o errori nella creazione del data lake, è possibile visualizzare un elenco di eccezioni utilizzando l'ListDataLakeExceptionsoperazione e notificare agli utenti le eccezioni durante l'operazione. CreateDataLakeExceptionSubscription Per ulteriori informazioni, consulta Risoluzione dei problemi relativi allo stato del data lake.

Passaggio 5: Visualizza e interroga i tuoi dati

Dopo aver creato il tuo data lake, puoi utilizzare Amazon Athena o servizi simili per visualizzare e interrogare i tuoi dati da AWS Lake Formation database e tabelle. Quando abiliti Security Lake a livello di codice, le autorizzazioni di visualizzazione del database non vengono concesse automaticamente. L'account amministratore del data lake in AWS Lake Formation deve concedere `SELECT` le autorizzazioni al ruolo IAM che desideri utilizzare per interrogare i database e le tabelle pertinenti. Come minimo, il ruolo deve disporre delle autorizzazioni di analista dei dati. Per ulteriori informazioni sui livelli di autorizzazione, consulta Lake Formation personas e IAM permissions reference. Per istruzioni sulla concessione *`SELECT`* delle autorizzazioni, consulta Concessione delle autorizzazioni di Data Catalog utilizzando il metodo della risorsa denominata nella Guida per gli sviluppatori. AWS Lake Formation

Fase 6: Creare abbonati

Dopo aver creato il data lake, puoi aggiungere abbonati per utilizzare i tuoi dati. Gli abbonati possono utilizzare i dati accedendo direttamente agli oggetti nei bucket Amazon S3 o interrogando il data lake. Per ulteriori informazioni sugli abbonati, consulta. Gestione degli abbonati in Amazon Security Lake

Gestione di più account con AWS Organizations

Puoi utilizzare Amazon Security Lake per raccogliere log di sicurezza ed eventi da più Account AWS fonti. Per aiutare ad automatizzare e semplificare la gestione di più account, ti consigliamo vivamente di integrare Security Lake con. AWS Organizations

In Organizations, l'account utilizzato per creare l'organizzazione è chiamato account di gestione. Per integrare Security Lake con Organizations, l'account di gestione deve designare un account amministratore delegato di Security Lake per l'organizzazione.

L'amministratore delegato di Security Lake può abilitare Security Lake e configurare le impostazioni di Security Lake per gli account dei membri. L'amministratore delegato può raccogliere registri ed eventi in tutta l'organizzazione Regioni AWS ovunque sia abilitato Security Lake (indipendentemente dall'endpoint regionale attualmente utilizzato). L'amministratore delegato può anche configurare Security Lake per raccogliere automaticamente i dati di log ed eventi per i nuovi account dell'organizzazione.

L'amministratore delegato di Security Lake ha accesso ai dati di registro ed eventi per gli account dei membri associati. Di conseguenza, può configurare Security Lake per raccogliere i dati di proprietà degli account dei membri associati. Possono inoltre concedere agli abbonati il permesso di utilizzare i dati di proprietà degli account dei membri associati.

Per abilitare Security Lake per più account in un'organizzazione, l'account di gestione dell'organizzazione deve prima designare un account amministratore delegato di Security Lake per l'organizzazione. L'amministratore delegato può quindi abilitare e configurare Security Lake per l'organizzazione.

Per informazioni sulla configurazione di Organizations, vedere Creating and managing an organization nella AWS Organizations User Guide.

Considerazioni importanti per gli amministratori delegati di Security Lake

Prendi nota dei seguenti fattori che definiscono il comportamento di un amministratore delegato in Security Lake:

L'amministratore delegato è lo stesso in tutte le regioni.

Quando si crea l'amministratore delegato, questo diventa l'amministratore delegato per ogni regione in cui si abilita Security Lake.

Si consiglia di impostare l'account Log Archive come amministratore delegato di Security Lake.

L'account Log Archive è dedicato all'acquisizione e all'archiviazione di tutti i log relativi alla sicurezza. Account AWS L'accesso a questo account è in genere limitato a pochi utenti, come revisori e team di sicurezza per le indagini di conformità. Si consiglia di impostare l'account Log Archive come amministratore delegato di Security Lake in modo da poter visualizzare i log e gli eventi relativi alla sicurezza con un cambio di contesto minimo.

Inoltre, consigliamo che solo un numero minimo di utenti abbia accesso diretto all'account Log Archive. Al di fuori di questo gruppo selezionato, se un utente deve accedere ai dati raccolti da Security Lake, è possibile aggiungerlo come abbonato a Security Lake. Per informazioni sull'aggiunta di un abbonato, consulta. Gestione degli abbonati in Amazon Security Lake

Se non utilizzi il AWS Control Tower servizio, potresti non avere un account Log Archive. Per ulteriori informazioni sull'account Log Archive, vedere Security OU — Log Archive account nella AWS Security Reference Architecture.

Un'organizzazione può avere un solo amministratore delegato.

È possibile avere un solo amministratore delegato di Security Lake per ogni organizzazione.

L'account di gestione dell'organizzazione non può essere l'amministratore delegato.

In base alle migliori pratiche di AWS sicurezza e al principio del privilegio minimo, l'account di gestione dell'organizzazione non può essere l'amministratore delegato.

L'amministratore delegato deve far parte di un'organizzazione attiva.

Quando si elimina un'organizzazione, l'account amministratore delegato non può più gestire Security Lake. È necessario designare un amministratore delegato di un'altra organizzazione o utilizzare Security Lake con un account autonomo che non fa parte di un'organizzazione.

Autorizzazioni IAM necessarie per designare l'amministratore delegato

Quando si designa l'amministratore delegato di Security Lake, è necessario disporre delle autorizzazioni per abilitare Security Lake e utilizzare determinate operazioni AWS Organizations API elencate nella seguente dichiarazione politica.

È possibile aggiungere la seguente dichiarazione alla fine di una policy AWS Identity and Access Management (IAM) per concedere queste autorizzazioni.

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

Designazione dell'amministratore delegato di Security Lake e aggiunta degli account dei membri

Scegliete il metodo di accesso per designare l'account amministratore delegato di Security Lake per la vostra organizzazione. Solo l'account di gestione dell'organizzazione può designare l'account amministratore delegato per la propria organizzazione. L'account di gestione dell'organizzazione non può essere l'account amministratore delegato dell'organizzazione.

> **Note**
>
> - L'account di gestione dell'organizzazione deve utilizzare l'`RegisterDataLakeDelegatedAdministrator`operazione Security Lake per designare l'account amministratore delegato di Security Lake. La designazione dell'amministratore delegato di Security Lake tramite Organizations non è supportata.
> - Se si desidera modificare l'amministratore delegato dell'organizzazione, è necessario prima rimuovere l'amministratore delegato corrente. È quindi possibile designare un nuovo amministratore delegato.

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedi utilizzando le credenziali dell'account di gestione dell'organizzazione.

2. - Se Security Lake non è ancora abilitato, seleziona Inizia, quindi designa l'amministratore delegato di Security Lake nella pagina Abilita Security Lake.
   - Se Security Lake è già abilitato, designa l'amministratore delegato di Security Lake nella pagina Impostazioni.
3. In Delega l'amministrazione a un altro account, seleziona l'account che funge già da amministratore delegato per altri servizi di AWS sicurezza (scelta consigliata). In alternativa, inserisci l' Account AWS ID a 12 cifre dell'account che desideri designare come amministratore delegato di Security Lake.
4. Scegli Delega. Se Security Lake non è già abilitato, la designazione dell'amministratore delegato abiliterà Security Lake per quell'account nella regione corrente.

API

Per designare l'amministratore delegato a livello di codice, utilizza il RegisterDataLakeDelegatedAdministratorfunzionamento dell'API Security Lake. È necessario richiamare l'operazione dall'account di gestione dell'organizzazione. Se utilizzi il AWS CLI, esegui il register-data-lake-delegated-administratorcomando dall'account di gestione dell'organizzazione. Nella richiesta, utilizza il `accountId` parametro per specificare l'ID account a 12 cifre dell'account Account AWS da designare come amministratore delegato per l'organizzazione.

Ad esempio, il AWS CLI comando seguente designa l'amministratore delegato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

L'amministratore delegato può anche scegliere di automatizzare la raccolta di dati di AWS registro ed eventi per i nuovi account dell'organizzazione. Con questa configurazione, Security Lake viene automaticamente abilitato nei nuovi account quando gli account vengono aggiunti all'organizzazione in. AWS Organizations In qualità di amministratore delegato, puoi abilitare questa configurazione utilizzando l'CreateDataLakeOrganizationConfigurationoperazione dell'API Security Lake o, se utilizzi la CLI AWS, create-data-lake-organization-configurationeseguendo il comando. Nella richiesta, puoi anche specificare determinate impostazioni di configurazione per nuovi account.

Ad esempio, il AWS CLI comando seguente abilita automaticamente Security Lake e la raccolta di log di query del resolver Amazon Route 53, AWS Security Hub risultati e log di flusso di Amazon Virtual Private Cloud (Amazon VPC) nei nuovi account dell'organizzazione. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Dopo che l'account di gestione dell'organizzazione ha designato l'amministratore delegato, l'amministratore può abilitare e configurare Security Lake per l'organizzazione. Ciò include l'abilitazione e la configurazione di Security Lake per raccogliere dati di AWS log ed eventi per i singoli account dell'organizzazione. Per ulteriori informazioni, consulta Raccolta di dati dai AWS servizi.

È possibile utilizzare l'GetDataLakeOrganizationConfigurationoperazione per ottenere dettagli sulla configurazione corrente dell'organizzazione per gli account dei nuovi membri.

Rimozione dell'amministratore delegato di Security Lake

Solo l'account di gestione dell'organizzazione può rimuovere l'amministratore delegato di Security Lake dalla propria organizzazione. Se si desidera modificare l'amministratore delegato dell'organizzazione, rimuovere l'amministratore delegato corrente e quindi designare il nuovo amministratore delegato.

> **Important**
>
> La rimozione dell'amministratore delegato di Security Lake elimina il data lake e disabilita Security Lake per gli account dell'organizzazione.

Non è possibile modificare o rimuovere l'amministratore delegato utilizzando la console Security Lake. Queste attività possono essere eseguite solo a livello di codice.

Per rimuovere l'amministratore delegato a livello di codice, utilizza il DeregisterDataLakeDelegatedAdministratorfunzionamento dell'API Security Lake. È necessario richiamare l'operazione dall'account di gestione dell'organizzazione. Se si utilizza il AWS CLI, eseguire il deregister-data-lake-delegated-administratorcomando dall'account di gestione dell'organizzazione.

Ad esempio, il AWS CLI comando seguente rimuove l'amministratore delegato di Security Lake.

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

Per mantenere la designazione di amministratore delegato ma modificare le impostazioni di configurazione automatica dei nuovi account membro, usa il DeleteDataLakeOrganizationConfigurationfunzionamento dell'API Security Lake o, se stai usando il AWS CLI, il comando. delete-data-lake-organization-configuration Solo l'amministratore delegato può modificare queste impostazioni per l'organizzazione.

Ad esempio, il AWS CLI comando seguente interrompe la raccolta automatica dei risultati del Security Hub dai nuovi account membri che entrano a far parte dell'organizzazione. I nuovi account membro non contribuiranno ai risultati del Security Hub al data lake dopo che l'amministratore delegato avrà richiamato questa operazione. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securitylake delete-data-lake-organization-configuration \
```

```
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"SH_FINDINGS"}]}]'
```

Accesso affidabile a Security Lake

Dopo aver configurato Security Lake per un'organizzazione, l'account di AWS Organizations gestione può abilitare l'accesso affidabile con Security Lake. L'accesso affidabile consente a Security Lake di creare un ruolo collegato ai servizi IAM ed eseguire attività nell'organizzazione e nei relativi account per conto dell'utente. Per ulteriori informazioni, consulta Using AWS Organizations with other Servizi AWS nella Guida per l'AWS Organizations utente.

Come utente dell'account di gestione dell'organizzazione, puoi disabilitare l'accesso affidabile per Security Lake in AWS Organizations. Per istruzioni sulla disabilitazione dell'accesso affidabile, consulta Come abilitare o disabilitare l'accesso affidabile nella Guida per l'AWS Organizations utente.

Ti consigliamo di disabilitare l'accesso affidabile se quello dell'amministratore delegato Account AWS è sospeso, isolato o chiuso.

Gestione delle aree

Amazon Security Lake può raccogliere i log di sicurezza e gli eventi Regioni AWS in cui hai abilitato il servizio. Per ogni regione, i dati vengono archiviati in un bucket Amazon S3 diverso. Puoi specificare diverse configurazioni di data lake (ad esempio, diverse fonti e impostazioni di conservazione) per diverse regioni. È inoltre possibile definire una o più regioni di rollup per consolidare i dati provenienti da più regioni.

Verifica dello stato della regione

Security Lake può raccogliere dati su più siti Regioni AWS. Per tenere traccia dello stato del tuo data lake, può essere utile capire come è attualmente configurata ogni regione. Scegli il metodo di accesso preferito e segui questi passaggi per ottenere lo stato attuale di una regione.

Console

Per verificare lo stato della regione

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, scegli Regioni. Viene visualizzata la pagina Regioni, che fornisce una panoramica delle regioni in cui Security Lake è attualmente abilitato.
3. Seleziona una regione, quindi scegli Modifica per visualizzare i dettagli di quella regione.

API

Per conoscere lo stato della raccolta dei log nella regione corrente, utilizza il GetDataLakeSourcesfunzionamento dell'API Security Lake. Se stai usando AWS CLI, esegui il get-data-lake-sourcescomando. Per il `accounts` parametro, specificate uno o più Account AWS ID come elenco. Se la richiesta ha esito positivo, Security Lake restituisce un'istantanea per gli account nella regione corrente, incluse AWS le fonti da cui Security Lake raccoglie i dati e lo stato di ciascuna fonte. Se non si include il `accounts` parametro, la risposta include lo stato della raccolta dei log per tutti gli account in cui Security Lake è configurato nella regione corrente.

Ad esempio, il AWS CLI comando seguente recupera lo stato della raccolta dei registri per gli account specificati nella regione corrente. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Il AWS CLI comando seguente elenca lo stato della raccolta dei registri per tutti gli account e le fonti abilitate nella regione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Per determinare se hai abilitato Security Lake per una regione, usa l'ListDataLakesoperazione. Se stai usando AWS CLI, esegui il list-data-lakescomando. Per il `regions` parametro, specificate il codice regionale per la regione, `us-east-1` ad esempio per la regione Stati Uniti orientali (Virginia settentrionale). Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS. L'`ListDataLakes`operazione restituisce le impostazioni di configurazione del data lake per ogni regione specificata nella richiesta. Se non si specifica una regione, Security Lake restituisce lo stato e le impostazioni di configurazione del data lake in ogni regione in cui è disponibile Security Lake.

Ad esempio, il AWS CLI comando seguente mostra lo stato e le impostazioni di configurazione del data lake nella `eu-central-1` regione. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Modifica delle impostazioni della regione

Scegli il tuo metodo preferito e segui queste istruzioni per aggiornare le impostazioni del tuo data lake in uno o più Regioni AWS.

Console

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, scegli Regioni.
3. Seleziona una regione, quindi scegli Modifica.

4. Seleziona la casella di controllo Sostituisci le fonti per tutti gli account in per <Region>confermare che le tue selezioni qui sostituiscono le selezioni precedenti per questa regione.
5. Per Seleziona classi di archiviazione, scegli Aggiungi transizione per aggiungere nuove classi di archiviazione per i tuoi dati.
6. Per i tag, assegna o modifica facoltativamente i tag per la regione. Un tag è un'etichetta che puoi definire e assegnare a determinati tipi di AWS risorse, inclusa la configurazione del data lake per una particolare Account AWS regione. Per ulteriori informazioni, consulta Etichettatura delle risorse di Amazon Security Lake.
7. Per trasformare una regione in una regione di rollup, scegli Regioni di rollup (in Impostazioni) nel pannello di navigazione. Quindi scegliere Modify (Modifica). Nella sezione Seleziona aree di rollup, scegli Aggiungi regione di rollup. Seleziona le regioni che contribuiscono e fornisci a Security Lake l'autorizzazione a replicare i dati su più regioni. Al termine, scegli Salva per salvare le modifiche.

API

Per aggiornare le impostazioni regionali per il tuo data lake a livello di codice, utilizza il UpdateDataLakefunzionamento dell'API Security Lake. Se utilizzi il AWS CLI, esegui il comando. update-data-lake Per il `region` parametro, specificate il codice regionale per la regione di cui desiderate modificare le impostazioni, `us-east-1` ad esempio per la regione Stati Uniti orientali (Virginia settentrionale). Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.

Utilizza parametri aggiuntivi per specificare un nuovo valore per ogni impostazione che desideri modificare, ad esempio la chiave di crittografia (`encryptionConfiguration`) e le impostazioni di conservazione (). `lifecycleConfiguration`

Ad esempio, il AWS CLI comando seguente aggiorna le impostazioni di scadenza dei dati e di transizione della classe di archiviazione per la regione. `us-east-1` Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Configurazione delle regioni di rollup

Una regione di rollup consolida i dati di una o più regioni contribuenti. Specificare una regione di rollup può aiutarti a rispettare i requisiti di conformità regionali.

Prima di aggiungere una regione di rollup, devi prima creare due ruoli diversi in AWS Identity and Access Management (IAM):

- Ruolo IAM per la replica dei dati
- Ruolo IAM per registrare le partizioni AWS Glue

> **Note**
>
> Security Lake crea questi ruoli IAM o utilizza ruoli esistenti per tuo conto quando usi la console Security Lake. Tuttavia, è necessario creare questi ruoli quando si utilizza l'API Security Lake o AWS CLI.

Ruolo IAM per la replica dei dati

Questo ruolo IAM concede l'autorizzazione ad Amazon S3 per replicare i log e gli eventi di origine in più regioni.

Per concedere queste autorizzazioni, crea un ruolo IAM che inizi con il prefisso `SecurityLake` e allega la seguente policy di esempio al ruolo. Avrai bisogno dell'Amazon Resource Name (ARN) del ruolo quando crei una regione di rollup in Security Lake. In questa politica, `sourceRegions` sono regioni contributive e regioni `destinationRegions` cumulative.

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

Allega la seguente politica di affidabilità al tuo ruolo per consentire ad Amazon S3 di assumere il ruolo:

```
{
```

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

Se utilizzi una chiave gestita dal cliente proveniente da AWS Key Management Service (AWS KMS) per crittografare il tuo data lake Security Lake, devi concedere le seguenti autorizzazioni oltre alle autorizzazioni previste dalla politica di replica dei dati.

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

Per ulteriori informazioni sui ruoli di replica, consulta Configurazione delle autorizzazioni nella Guida per l'utente di Amazon Simple Storage Service.

Ruolo IAM per registrare le partizioni AWS Glue

Questo ruolo IAM concede le autorizzazioni per una AWS Lambda funzione di aggiornamento delle partizioni utilizzata da Security Lake per registrare AWS Glue le partizioni per gli oggetti S3 che sono stati replicati da altre regioni. Senza creare questo ruolo, i sottoscrittori non possono interrogare gli eventi da quegli oggetti.

Per concedere queste autorizzazioni, crea un ruolo denominato `AmazonSecurityLakeMetaStoreManager` (potresti averlo già creato durante l'onboarding su Security Lake). Per ulteriori informazioni su questo ruolo, inclusa una policy di esempio, consulta. Fase 1: Creare ruoli IAM

Nella console Lake Formation, devi anche concedere `AmazonSecurityLakeMetaStoreManager` le autorizzazioni come amministratore del data lake seguendo questi passaggi:

1. Aprire la console Lake Formation all'indirizzo https://console.aws.amazon.com/lakeformation/.
2. Accedi come utente amministrativo.
3. Se viene visualizzata la finestra Welcome to Lake Formation, scegli l'utente che hai creato o selezionato nel Passaggio 1, quindi scegli Inizia.

4. Se non vedi la finestra Welcome to Lake Formation, esegui i seguenti passaggi per configurare un Lake Formation Administrator.

    1. Nel pannello di navigazione, in Autorizzazioni, scegli Ruoli e attività amministrative. Nella sezione Amministratori di Data Lake della pagina della console, scegli Scegli amministratori.
    2. Nella finestra di dialogo Gestisci gli amministratori del data lake, per gli utenti e i ruoli IAM, scegli il ruolo AmazonSecurityLakeMetaStoreManagerIAM che hai creato, quindi scegli Salva.

Per ulteriori informazioni sulla modifica delle autorizzazioni per gli amministratori del data lake, consulta Create a data lake administrator nella Developer Guide.AWS Lake Formation

Aggiungere regioni di rollup

Scegli il tuo metodo di accesso preferito e segui questi passaggi per aggiungere una regione cumulativa.

> **Note**
>
> Una regione può fornire dati a più regioni di rollup. Tuttavia, una regione di rollup non può essere una regione contributrice per un'altra regione di rollup.

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel pannello di navigazione, in Impostazioni, scegli Regioni di rollup.
3. Scegli Modifica, quindi scegli Aggiungi area di rollup.
4. Specificate la regione di rollup e le regioni contributive. Ripeti questo passaggio se desideri aggiungere più regioni di rollup.
5. Se è la prima volta che aggiungi una regione di rollup, per l'accesso al servizio, crea un nuovo ruolo IAM o utilizza un ruolo IAM esistente che autorizzi Security Lake a replicare i dati su più regioni.
6. Al termine, scegli Salva.

Puoi anche aggiungere una regione di rollup quando effettui l'onboarding su Security Lake. Per ulteriori informazioni, consulta Guida introduttiva ad Amazon Security Lake.

API

Per aggiungere una regione di rollup a livello di codice, utilizza il UpdateDataLakefunzionamento dell'API Security Lake. Se utilizzi il AWS CLI, esegui il comando. update-data-lake Nella richiesta, utilizzate il `region` campo per specificare la regione in cui desiderate inserire i dati nella regione di rollup. Nell'`regions`sarray del `replicationConfiguration` parametro, specifica il codice regionale per ogni regione di rollup. Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.

Ad esempio, il comando seguente viene impostato `ap-northeast-2` come regione di rollup. La `us-east-1` Regione fornirà dati alla `ap-northeast-2` Regione. Questo esempio stabilisce anche un periodo di scadenza di 365 giorni per gli oggetti che vengono aggiunti al data lake. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Puoi anche aggiungere una regione di rollup quando accedi a Security Lake. Per fare ciò, usa l'CreateDataLakeoperazione (o, se usi il AWS CLI, il create-data-lakecomando). Per ulteriori informazioni sulla configurazione delle regioni di rollup durante l'onboarding, vedere. Guida introduttiva ad Amazon Security Lake

Aggiornamento o rimozione delle regioni di rollup

Scegli il metodo di accesso preferito e segui questi passaggi per aggiornare o rimuovere le regioni di rollup in Security Lake.

Console

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel pannello di navigazione, in Impostazioni, scegli Regioni di rollup.
3. Scegli Modifica.

4. Per modificare le regioni contributrici per una regione di rollup, specifica le regioni contributrici aggiornate nella riga relativa alla regione di rollup.
5. Per rimuovere una regione di rollup, scegli Rimuovi nella riga relativa all'area di rollup.
6. Al termine, scegli Salva.

API

Per configurare le regioni di rollup a livello di codice, utilizza il UpdateDataLakefunzionamento dell'API Security Lake. Se utilizzi il AWS CLI, esegui il comando. update-data-lake Nella richiesta, utilizza i parametri supportati per specificare le impostazioni di rollup:

- Per aggiungere una regione contribuente, utilizzate il `region` campo per specificare il codice regionale della regione da aggiungere. Nell'`regions`array dell'`replicationConfiguration`oggetto, specificate il codice regionale per ogni regione di rollup a cui fornire dati. Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.
- Per rimuovere una regione contribuente, utilizza il `region` campo per specificare il codice regionale della regione da rimuovere. Per i `replicationConfiguration` parametri, non specificate alcun valore.

Ad esempio, il comando seguente configura entrambe `us-east-1` e `us-east-2` come regioni contribuenti. Entrambe le regioni forniranno dati alla regione di `ap-northeast-3` rollup. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Gestione del codice in Amazon Security Lake

Le fonti sono registri ed eventi generati da un singolo sistema che corrispondono a una classe di eventi specifica nelloOpen Cybersecurity Schema Framework (OCSF) schema. Amazon Security Lake può raccogliere registri ed eventi da una varietà di fonti, tra cui fonti supportate in modo nativoServizi AWS e fonti personalizzate di terze parti.

Security Lake esegue processi di estrazione, trasformazione e caricamento (ETL) su dati di origine e li consente di convertire i dati nel formato Apache Parquet e nello schema OCSF. Dopo l'elaborazione, Security Lake archivia i dati di origine in un bucket Amazon Simple Storage Service (Amazon S3) all'Account AWSinterno inRegione AWS cui sono stati generati. Security Lake crea un bucket Amazon S3 per cui si abilita il servizio. Ogni fonte riceve un prefisso separato nel bucket S3 e Security Lake organizza i dati di ciascuna fonte in un set separato diAWS Lake Formation tabelle.

Argomenti

Raccolta di dati dai AWS servizi

Amazon Security Lake può raccogliere log ed eventi dai seguenti elementi supportati Servizi AWS nativamente:

- AWS CloudTrail gestione ed eventi relativi ai dati (S3, Lambda)
- Registri di controllo di Amazon Elastic Kubernetes Service (Amazon EKS)
- Log di query di Amazon Route 53 Resolver
- AWS Security Hub risultati
- Log di flusso Amazon Virtual Private Cloud (Amazon VPC)

Security Lake trasforma automaticamente questi dati nel Open Cybersecurity Schema Framework (OCSF) formato Apache Parquet.

> **Tip**
>
> Per aggiungere uno o più dei servizi precedenti come origine di registro in Security Lake, non è necessario configurare separatamente la registrazione in questi servizi, ad eccezione

degli eventi di gestione. CloudTrail Se la registrazione è configurata in questi servizi, non è necessario modificare la configurazione di registrazione per aggiungerli come sorgenti di registro in Security Lake. Security Lake estrae i dati direttamente da questi servizi attraverso un flusso di eventi indipendente e duplicato.

Prerequisito: verificare le autorizzazioni

Per aggiungere un file Servizio AWS come fonte in Security Lake, è necessario disporre delle autorizzazioni necessarie. Verifica che la policy AWS Identity and Access Management (IAM) allegata al ruolo che utilizzi per aggiungere una fonte sia autorizzata a eseguire le seguenti azioni:

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

È consigliabile che il ruolo soddisfi le condizioni e l'ambito di risorse seguenti per le `s3:PutObject` autorizzazioni `S3:getObject` e.

```
{
    "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}"
```

```
                }
            }
    }
    ]
}
```

Queste azioni consentono di raccogliere registri ed eventi da un utente e inviarli al AWS Glue database Servizio AWS e alla tabella corretti.

Se utilizzi una AWS KMS chiave per la crittografia lato server del tuo data lake, ti serve anche l'autorizzazione per. `kms:DescribeKey`

CloudTrail registri degli eventi

AWS CloudTrail fornisce una cronologia delle chiamate AWS API per il tuo account, incluse le chiamate API effettuate utilizzando gli AWS SDK AWS Management Console, gli strumenti da riga di comando e determinati AWS servizi. CloudTrail consente inoltre di identificare gli utenti e gli account chiamati AWS API per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono state effettuate le chiamate. Per ulteriori informazioni, consulta la AWS CloudTrail Guida per l'utente.

Security Lake può raccogliere i log associati agli eventi di CloudTrail gestione e agli eventi relativi ai CloudTrail dati per S3 e Lambda. CloudTrail gli eventi di gestione, gli eventi sui dati S3 e gli eventi sui dati Lambda sono tre fonti separate in Security Lake. Di conseguenza, hanno valori diversi `sourceName`se ne aggiungi uno come fonte di log importata. Gli eventi di gestione, noti anche come eventi del piano di controllo, forniscono informazioni dettagliate sulle operazioni di gestione eseguite sulle risorse dell'azienda. Account AWS CloudTrail gli eventi relativi ai dati, noti anche come operazioni sul piano dati, mostrano le operazioni relative alle risorse eseguite sulle risorse o all'interno di esse Account AWS. Queste operazioni sono spesso attività ad alto volume.

Per raccogliere gli eventi di CloudTrail gestione in Security Lake, è necessario disporre di almeno un percorso organizzativo CloudTrail multiregionale che raccolga gli eventi di gestione di lettura e scrittura CloudTrail . La registrazione deve essere abilitata per il percorso. Se la registrazione è configurata negli altri servizi, non è necessario modificare la configurazione di registrazione per aggiungerli come fonti di registro in Security Lake. Security Lake estrae i dati direttamente da questi servizi attraverso un flusso di eventi indipendente e duplicato.

Un percorso multiregionale fornisce file di log da più regioni a un singolo bucket Amazon Simple Storage Service (Amazon S3) per un singolo bucket. Account AWS Se disponi già di un percorso

multiregionale gestito tramite CloudTrail console oppure non sono AWS Control Tower necessarie ulteriori azioni.

- Per informazioni sulla creazione e la gestione di un itinerario CloudTrail, consulta Creazione di un itinerario per un'organizzazione nella Guida per l'AWS CloudTrail utente.
- Per informazioni sulla creazione e la gestione di un percorso AWS Control Tower, consulta Logging AWS Control Tower actions with AWS CloudTrail nella Guida per l'AWS Control Tower utente.

Quando aggiungi CloudTrail eventi come fonte, Security Lake inizia immediatamente a raccogliere i registri CloudTrail degli eventi. Utilizza gli eventi di CloudTrail gestione e dati direttamente da CloudTrail un flusso di eventi indipendente e duplicato.

Security Lake non gestisce gli CloudTrail eventi né influisce sulle configurazioni esistenti CloudTrail . Per gestire direttamente l'accesso e la conservazione degli CloudTrail eventi, è necessario utilizzare la console di CloudTrail servizio o l'API. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

L'elenco seguente fornisce i collegamenti del GitHub repository ai riferimenti di mappatura relativi al modo in cui Security Lake normalizza CloudTrail gli eventi in OCSF.

GitHub CloudTrail Archivio OCSF per eventi

- Versione sorgente 1 (v1.0.0-rc.2)
- Versione sorgente 2 (v1.1.0)

Registri di controllo di Amazon EKS

Quando aggiungi Amazon EKS Audit Logs come fonte, Security Lake inizia a raccogliere informazioni approfondite sulle attività eseguite sulle risorse Kubernetes in esecuzione nei cluster Elastic Kubernetes Service (EKS). I registri di controllo EKS consentono di rilevare attività potenzialmente sospette nei cluster EKS all'interno di Amazon Elastic Kubernetes Service.

Security Lake utilizza gli eventi EKS Audit Log direttamente dalla funzionalità di registrazione del piano di controllo di Amazon EKS attraverso un flusso indipendente e duplicato di log di audit. Questo processo non richiede alcuna configurazione aggiuntiva né influisce sulle configurazioni di registrazione del piano di controllo (control-plane) Amazon EKS esistenti che potresti avere. Per ulteriori informazioni, consulta la registrazione del piano di controllo di Amazon EKS nella Guida per l'utente di Amazon EKS.

Per informazioni su come Security Lake normalizza gli eventi EKS Audit Logs in OCSF, consulta il riferimento alla mappatura nel GitHub repository OCSF per gli eventi di Amazon EKS Audit Logs.

Log delle query di Route 53 Resolver

I log delle query del resolver Route 53 tengono traccia delle query DNS effettuate dalle risorse all'interno del tuo Amazon Virtual Private Cloud (Amazon VPC). Questo ti aiuta a capire come funzionano le tue applicazioni e a individuare le minacce alla sicurezza.

Quando aggiungete i log delle query del resolver Route 53 come origine in Security Lake, Security Lake inizia immediatamente a raccogliere i log delle query del resolver direttamente da Route 53 attraverso un flusso di eventi indipendente e duplicato.

Security Lake non gestisce i log di Route 53 né influisce sulle configurazioni di registrazione delle query del resolver esistenti. Per gestire i log delle interrogazioni del resolver, è necessario utilizzare la console di servizio Route 53. Per ulteriori informazioni, consulta Managing Resolver Query Logging configurations nella Amazon Route 53 Developer Guide.

L'elenco seguente fornisce collegamenti ai GitHub repository ai riferimenti di mappatura su come Security Lake normalizza i log di Route 53 in OCSF.

GitHub Archivio OCSF per i log di Route 53

- Versione sorgente 1 (v1.0.0-rc.2)
- Versione sorgente 2 (v1.1.0)

Risultati del Security Hub

I risultati di Security Hub ti aiutano a comprendere la tua posizione in materia di sicurezza AWS e ti consentono di verificare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Security Hub raccoglie i risultati da varie fonti, comprese le integrazioni con altre Servizi AWS integrazioni di prodotti di terze parti e i controlli del Security Hub. Security Hub elabora i risultati in un formato standard chiamato AWS Security Finding Format (ASFF).

Quando aggiungi i risultati di Security Hub come fonte in Security Lake, Security Lake inizia immediatamente a raccogliere i risultati direttamente da Security Hub attraverso un flusso di eventi indipendente e duplicato. Security Lake trasforma anche i risultati da ASFF a Open Cybersecurity Schema Framework (OCSF) (OCSF).

Security Lake non gestisce i risultati del Security Hub né influisce sulle impostazioni del Security Hub. Per gestire i risultati di Security Hub, è necessario utilizzare la console del servizio Security Hub, l'API o AWS CLI. Per ulteriori informazioni, consulta Findings AWS Security Hub nella Guida AWS Security Hub per l'utente.

L'elenco seguente fornisce collegamenti al GitHub repository al riferimento di mappatura su come Security Lake normalizza i risultati del Security Hub in OCSF.

GitHub Archivio OCSF per i risultati del Security Hub

- Versione sorgente 1 (v1.0.0-rc.2)
- Versione sorgente 2 (v1.1.0)

Log di flusso VPC

La funzionalità VPC Flow Logs di Amazon VPC acquisisce informazioni sul traffico IP da e verso le interfacce di rete all'interno del tuo ambiente.

Quando aggiungi i log di flusso VPC come origine in Security Lake, Security Lake inizia immediatamente a raccogliere i log di flusso VPC. Utilizza i log di flusso VPC direttamente da Amazon VPC attraverso un flusso indipendente e duplicato di Flow Logs.

Security Lake non gestisce i log di flusso VPC né influisce sulle configurazioni di Amazon VPC. Per gestire i tuoi Flow Logs, devi utilizzare la console di servizio Amazon VPC. Per ulteriori informazioni, consulta Work with Flow Logs nella Amazon VPC Developer Guide.

L'elenco seguente fornisce i collegamenti del GitHub repository al riferimento di mappatura su come Security Lake normalizza i log di flusso VPC in OCSF.

GitHub Archivio OCSF per i log di flusso VPC

- Versione sorgente 1 (v1.0.0-rc.2)
- Versione sorgente 2 (v1.1.0)

Aggiungere un file Servizio AWS come fonte

Dopo aver aggiunto un file Servizio AWS come fonte, Security Lake inizia automaticamente a raccogliere i registri di sicurezza e gli eventi da esso. Queste istruzioni spiegano come aggiungere

una sorgente supportata in modo nativo in Security Servizio AWS Lake. Per istruzioni sull'aggiunta di una fonte personalizzata, consulta. Raccolta di dati da fonti personalizzate

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Scegli Sorgenti dal pannello di navigazione.
3. Seleziona Servizio AWS quello da cui desideri raccogliere i dati e scegli Configura.
4. Nella sezione Impostazioni della fonte, abilita la fonte e seleziona la versione dell'origine dati che desideri utilizzare per l'ingestione dei dati. Per impostazione predefinita, la versione più recente dell'origine dati viene acquisita da Security Lake.

   > **Important**
   >
   > Se non disponi delle autorizzazioni di ruolo necessarie per abilitare la nuova versione dell'origine del AWS registro nella regione specificata, contatta l'amministratore di Security Lake. Per ulteriori informazioni, consulta Aggiornare le autorizzazioni dei ruoli.

   Affinché i tuoi abbonati possano importare la versione selezionata dell'origine dati, devi anche aggiornare le impostazioni degli abbonati. Per i dettagli su come modificare un abbonato, consulta Gestione degli abbonati in Amazon Security Lake.

   Facoltativamente, puoi scegliere di importare solo la versione più recente e disabilitare tutte le versioni di origine precedenti utilizzate per l'inserimento dei dati.
5. Nella sezione Regioni, seleziona le regioni in cui desideri raccogliere i dati per l'origine. Security Lake raccoglierà i dati dalla fonte da tutti gli account nelle regioni selezionate.
6. Scegli Abilita .

API

Per aggiungere un file Servizio AWS come fonte a livello di codice, utilizza il CreateAwsLogSourcefunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il create-aws-log-sourcecomando. I parametri `sourceName` e `regions` sono obbligatori. Facoltativamente, puoi limitare l'ambito della fonte a uno specifico `accounts` o a uno specifico`sourceVersion`.

> **Important**
>
> Quando non si fornisce un parametro nel comando, Security Lake presuppone che il parametro mancante si riferisca all'intero set. Ad esempio, se non si fornisce il `accounts` parametro, il comando si applica all'intero set di account dell'organizzazione.

L'esempio seguente aggiunge i log di flusso VPC come origine negli account e nelle regioni designati. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

> **Note**
>
> Se applichi questa richiesta a una regione in cui non hai abilitato Security Lake, riceverai un errore. Puoi risolvere l'errore abilitando Security Lake in quella regione o utilizzando il `regions` parametro per specificare solo le regioni in cui hai abilitato Security Lake.

```
$ aws securitylake create-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions=["us-east-2"],sourceVersion="1.0"
```

Aggiornamento delle autorizzazioni dei ruoli

Console

Se non disponi delle autorizzazioni di ruolo necessarie per importare dati da una versione dell'origine dati, devi aggiornare le autorizzazioni di `AmazonSecurityLakeMetaStoreManagerV2` ruolo per elaborare i dati dalle tue fonti.

Segui i passaggi per aggiornare le autorizzazioni del ruolo per elaborare i dati da una nuova versione dell'origine di AWS registro in una regione specificata. Si tratta di un'azione unica, poiché le autorizzazioni vengono applicate automaticamente alle future versioni delle origini dati.

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

Accedi con le credenziali dell'amministratore delegato di Security Lake.

2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere General (Generali).
3. Scegli Aggiorna le autorizzazioni del ruolo.
4. Nella sezione Accesso al servizio, esegui una delle seguenti operazioni:
   - Creare e utilizzare un nuovo ruolo di servizio: è possibile utilizzare il ruolo AmazonSecurityLakeMetaStoreManagerV2 creato da Security Lake.
   - Usa un ruolo di servizio esistente: puoi scegliere un ruolo di servizio esistente dall'elenco dei nomi del ruolo di servizio.
5. Scegli Applica.

API

Se non disponi delle autorizzazioni di ruolo necessarie per importare dati da una versione dell'origine dati, devi aggiornare le autorizzazioni del `AmazonSecurityLakeMetaStoreManagerV2` ruolo per elaborare i dati dalle tue fonti. Si tratta di un'azione unica, poiché le autorizzazioni vengono applicate automaticamente alle future versioni delle origini dati.

Per aggiornare le autorizzazioni a livello di codice, utilizza il UpdateDataLakefunzionamento dell'API Security Lake. Per aggiornare le autorizzazioni utilizzando AWS CLI, esegui il comando. update-data-lake

Per aggiornare le autorizzazioni del ruolo, è necessario allegare la AmazonSecurityLakeMetastoreManagerpolicy al ruolo.

Eliminazione del ruolo AmazonSecurityLakeMetaStoreManager

Important

Dopo aver aggiornato le autorizzazioni del ruolo a`AmazonSecurityLakeMetaStoreManagerV2`, verifica che il data lake funzioni correttamente prima di rimuovere il vecchio `AmazonSecurityLakeMetaStoreManager` ruolo. Si consiglia di attendere almeno 4 ore prima di rimuovere il ruolo.

Se decidi di rimuovere il ruolo, devi prima eliminare il `AmazonSecurityLakeMetaStoreManager` ruolo da AWS Lake Formation.

Segui questi passaggi per rimuovere il `AmazonSecurityLakeMetaStoreManager` ruolo dalla console di Lake Formation.

1. Accedi a e apri AWS Management Console la console Lake Formation all'indirizzo https://console.aws.amazon.com/lakeformation/.
2. Nella console di Lake Formation, dal riquadro di navigazione, scegli Ruoli e attività amministrative.
3. Rimuovi `AmazonSecurityLakeMetaStoreManager` da ogni regione.

Rimuovere un Servizio AWS file come fonte

Scegli il tuo metodo di accesso e segui questi passaggi per rimuovere una fonte Security Lake supportata Servizio AWS nativamente. Puoi rimuovere una fonte per una o più regioni. Quando rimuovi la fonte, Security Lake interrompe la raccolta di dati da tale fonte nelle regioni e negli account specificati e gli abbonati non possono più consumare nuovi dati dalla fonte. Tuttavia, gli abbonati possono comunque utilizzare i dati raccolti da Security Lake dalla fonte prima della rimozione. È possibile utilizzare queste istruzioni solo per rimuovere una fonte supportata in modo nativo Servizio AWS . Per informazioni sulla rimozione di una fonte personalizzata, consulta. Raccolta di dati da fonti personalizzate

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Scegli Sorgenti dal pannello di navigazione.
3. Seleziona una fonte e scegli Disattiva.
4. Seleziona una o più regioni in cui desideri interrompere la raccolta di dati da questa fonte. Security Lake smetterà di raccogliere dati dalla fonte da tutti gli account nelle regioni selezionate.

API

Per rimuovere un file Servizio AWS come fonte a livello di codice, utilizza il DeleteAwsLogSourcefunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il delete-aws-log-sourcecomando. I parametri `sourceName` e

`regions` sono obbligatori. Facoltativamente, puoi limitare l'ambito della rimozione a uno specifico `accounts` o a uno specifico`sourceVersion`.

> **Important**
>
> Quando non si fornisce un parametro nel comando, Security Lake presuppone che il parametro mancante si riferisca all'intero set. Ad esempio, se non si fornisce il `accounts` parametro, il comando si applica all'intero set di account dell'organizzazione.

L'esempio seguente rimuove i log di flusso VPC come origine negli account e nelle regioni designati.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="1.0"
```

L'esempio seguente rimuove Route 53 come origine nell'account e nelle regioni designati.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-
east-2"]',sourceVersion="1.0"
```

Gli esempi precedenti sono formattati per Linux, macOS o Unix e utilizzano il carattere di continuazione di riga (\) per migliorare la leggibilità.

Ottenere lo stato della raccolta di sorgenti

Scegli il tuo metodo di accesso e segui i passaggi per ottenere un'istantanea degli account e delle fonti per i quali è abilitata la raccolta dei log nella regione corrente.

Console

Per conoscere lo stato della raccolta dei log nella regione corrente

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, scegli Account.

3. Posiziona il cursore sul numero nella colonna Sorgenti per vedere quali registri sono abilitati per l'account selezionato.

API

Per conoscere lo stato della raccolta dei log nella regione corrente, utilizza il GetDataLakeSourcesfunzionamento dell'API Security Lake. Se stai usando AWS CLI, esegui il get-data-lake-sourcescomando. Per il `accounts` parametro, puoi specificare uno o più Account AWS ID come elenco. Se la richiesta ha esito positivo, Security Lake restituisce un'istantanea per gli account nella regione corrente, incluse AWS le fonti da cui Security Lake raccoglie i dati e lo stato di ciascuna fonte. Se non si include il `accounts` parametro, la risposta include lo stato della raccolta dei log per tutti gli account in cui Security Lake è configurato nella regione corrente.

Ad esempio, il AWS CLI comando seguente recupera lo stato della raccolta dei registri per gli account specificati nella regione corrente. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Raccolta di dati da fonti personalizzate

Amazon Security Lake può raccogliere log ed eventi da fonti personalizzate di terze parti. Per ogni fonte personalizzata, Security Lake gestisce quanto segue:

- Fornisce un prefisso univoco per l'origine nel bucket Amazon S3.
- Crea un ruolo in AWS Identity and Access Management (IAM) che consente a una fonte personalizzata di scrivere dati nel data lake. Il limite delle autorizzazioni per questo ruolo è impostato da una politica AWS gestita chiamata. `AmazonSecurityLakePermissionsBoundary`
- Crea una AWS Lake Formation tabella per organizzare gli oggetti che l'origine scrive su Security Lake.
- Imposta un AWS Glue crawler per partizionare i dati di origine. Il crawler compila il file con la tabella. AWS Glue Data Catalog Inoltre, rileva automaticamente i nuovi dati di origine ed estrae le definizioni degli schemi.

Per aggiungere una fonte personalizzata a Security Lake, deve soddisfare i seguenti requisiti:

1. Destinazione: l'origine personalizzata deve essere in grado di scrivere dati su Security Lake come set di oggetti S3 sotto il prefisso assegnato all'origine. Per le fonti che contengono più categorie di dati, è necessario fornire ogni classe di eventi Open Cybersecurity Schema Framework (OCSF) unica come fonte separata. Security Lake crea un ruolo IAM che consente all'origine personalizzata di scrivere nella posizione specificata nel bucket S3.

   > **Note**
   >
   > Utilizza lo strumento di convalida OCSF per verificare se la fonte personalizzata è compatibile con. `OCSF Schema 1.1`

2. Formato: ogni oggetto S3 raccolto dall'origine personalizzata deve essere formattato come file Apache Parquet.
3. Schema: la stessa classe di eventi OCSF deve essere applicata a ogni record all'interno di un oggetto in formato Parquet.

Le migliori pratiche per l'acquisizione di fonti personalizzate

Per facilitare l'elaborazione e l'interrogazione efficienti dei dati, consigliamo di seguire queste best practice quando si aggiunge una fonte personalizzata a Security Lake:

Partizionamento

Gli oggetti devono essere partizionati per posizione di origine, Regione AWS, Account AWS e data. Il percorso dei dati della partizione è formattato come. *`bucket-name`*`/`*`source-location`*`/region=`*`region`*`/accountId=`*`accountID`*`/eventDay=`*`YYYYMMDD`*

Una partizione di esempio è. `aws-security-data-lake-`*`us-west-2-lake-uid`*`/`*`source-location`*`/region=`*`us-west-2`*`/accountId=`*`123456789012`*`/eventDay=`*`20230428`*`/`

- `bucket-name`— Il nome del bucket Amazon S3 in cui Security Lake archivia i dati di origine personalizzati.
- `source-location`— Prefisso per l'origine personalizzata nel tuo bucket S3. Security Lake archivia tutti gli oggetti S3 per una determinata fonte con questo prefisso e il prefisso è unico per quella determinata fonte.
- `region`— Regione AWS su cui vengono scritti i dati.
- `accountId`— Account AWS ID a cui appartengono i record nella partizione di origine.

- `eventDay`— Data in cui si è verificato l'evento, formattata come una stringa di otto caratteri (). `YYYYMMDD`

Dimensioni e frequenza dell'oggetto

Gli oggetti scritti su Security Lake devono memorizzare i record nel buffer per 5 minuti. Se il periodo di buffer include troppi dati per essere interrogati in modo efficiente, le fonti personalizzate possono scrivere più record nella finestra di 5 minuti, purché la dimensione media di tali file rimanga inferiore a 256 MB. Le fonti personalizzate con velocità effettiva ridotta possono scrivere oggetti più piccoli ogni 5 minuti per mantenere una latenza di inserimento di 5 minuti e memorizzare i record nel buffer per periodi più lunghi.

Impostazioni del parquet

Security Lake supporta le versioni 1.x e 2.x di Parquet. La dimensione della pagina dati deve essere limitata a 1 MB (non compressa). La dimensione del gruppo di righe non deve superare i 256 MB (compressi). Per la compressione all'interno dell'oggetto Parquet, è preferibile zstandard.

Ordinamento

All'interno di ogni oggetto in formato Parquet, i record devono essere ordinati per tempo per ridurre il costo dell'interrogazione dei dati.

Prerequisiti per aggiungere una fonte personalizzata

Quando si aggiunge un'origine personalizzata, Security Lake crea un ruolo IAM che consente alla fonte di scrivere i dati nella posizione corretta nel data lake. Il nome del ruolo segue il formato`AmazonSecurityLake-Provider-{name of the custom source}-{region}`, `region` dov'è il formato Regione AWS in cui stai aggiungendo l'origine personalizzata. Security Lake attribuisce una policy al ruolo che consente l'accesso al data lake. Se hai crittografato il data lake con una AWS KMS chiave gestita dal cliente, Security Lake allega anche una policy `kms:Decrypt` e `kms:GenerateDataKey` autorizzazioni al ruolo. Il limite delle autorizzazioni per questo ruolo è impostato da una AWS politica gestita chiamata. `AmazonSecurityLakePermissionsBoundary`

Argomenti

- Verificare le autorizzazioni
- Crea un ruolo IAM per consentire l'accesso in scrittura alla posizione del bucket di Security Lake (API e AWS CLI passaggio solo)

Verificare le autorizzazioni

Prima di aggiungere una fonte personalizzata, verifica di disporre delle autorizzazioni necessarie per eseguire le seguenti azioni.

Per verificare le tue autorizzazioni, usa IAM per esaminare le policy IAM allegate alla tua identità IAM. Quindi, confronta le informazioni contenute in tali policy con il seguente elenco di azioni che devi essere autorizzato a eseguire per aggiungere una fonte personalizzata.

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

Queste azioni consentono di raccogliere log ed eventi da un'origine personalizzata, inviarli al AWS Glue database e alla tabella corretti e archiviarli in Amazon S3.

Se utilizzi una AWS KMS chiave per la crittografia lato server del tuo data lake, hai bisogno anche dell'autorizzazione per`kms:CreateGrant`, e. `kms:DescribeKey` `kms:GenerateDataKey`

> **Important**
>
> Se prevedi di utilizzare la console Security Lake per aggiungere un abbonato, puoi saltare il passaggio successivo e procedere con. Aggiungere una fonte personalizzata La console

Security Lake offre un processo semplificato per iniziare e crea tutti i ruoli IAM necessari o utilizza i ruoli esistenti per tuo conto.
Se prevedi di utilizzare l'API Security Lake o di AWS CLI aggiungere un abbonato, continua con il passaggio successivo per creare un ruolo IAM per consentire l'accesso in scrittura alla posizione del bucket di Security Lake.

Crea un ruolo IAM per consentire l'accesso in scrittura alla posizione del bucket di Security Lake (API e AWS CLI passaggio solo)

Se utilizzi l'API Security Lake o vuoi AWS CLI aggiungere una fonte personalizzata, aggiungi questo ruolo IAM per concedere l' AWS Glue autorizzazione alla scansione dei dati di origine personalizzati e identificare le partizioni nei dati. Queste partizioni sono necessarie per organizzare i dati e creare e aggiornare tabelle nel Data Catalog.

Dopo aver creato questo ruolo IAM, avrai bisogno dell'Amazon Resource Name (ARN) del ruolo per aggiungere una fonte personalizzata.

È necessario allegare la policy `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS gestita.

Per concedere le autorizzazioni necessarie, devi anche creare e incorporare la seguente politica in linea nel tuo ruolo per consentire Crawler di AWS Glue la lettura dei file di dati dall'origine personalizzata e la creazione/aggiornamento delle tabelle in Data Catalog. AWS Glue

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

```
}
```

Allega la seguente politica di fiducia per consentire e Account AWS utilizzando la quale può assumere il ruolo in base all'ID esterno:

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

Se il bucket S3 nella regione in cui stai aggiungendo la fonte personalizzata è crittografato con un file gestito dal cliente AWS KMS key, devi inoltre allegare la seguente politica al ruolo e alla tua politica chiave 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}}"
    ]
}
```

Aggiungere una fonte personalizzata

Dopo aver creato il ruolo IAM per richiamare il AWS Glue crawler, segui questi passaggi per aggiungere una fonte personalizzata in Security Lake.

Console

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, selezionate la regione in cui desiderate creare l'origine personalizzata.
3. Scegli Origini personalizzate nel riquadro di navigazione, quindi scegli Crea fonte personalizzata.
4. Nella sezione Dettagli della fonte personalizzata, inserisci un nome univoco a livello globale per la tua fonte personalizzata. Quindi, selezionate una classe di eventi OCSF che descriva il tipo di dati che l'origine personalizzata invierà a Security Lake.
5. Se Account AWS sei autorizzato a scrivere dati, inserisci l'Account AWS ID e l'ID esterno dell'origine personalizzata che scriverà i log e gli eventi nel data lake.
6. Per Service Access, create e utilizzate un nuovo ruolo di servizio o utilizzate un ruolo di servizio esistente che autorizzi Security Lake a richiamare AWS Glue.
7. Scegli Crea.

API

Per aggiungere una fonte personalizzata a livello di codice, utilizza il CreateCustomLogSourcefunzionamento dell'API Security Lake. Usa l'operazione nel Regione AWS punto in cui desideri creare l'origine personalizzata. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il create-custom-log-sourcecomando.

Nella tua richiesta, usa i parametri supportati per specificare le impostazioni di configurazione per l'origine personalizzata:

- `sourceName`— Specificate un nome per la fonte. Il nome deve essere un valore unico a livello regionale.
- `eventClasses`— Specificare una o più classi di eventi OCSF per descrivere il tipo di dati che la fonte invierà a Security Lake. Per un elenco delle classi di eventi OCSF supportate come origine in Security Lake, vedere Open Cybersecurity Schema Framework (OCSF).

- `sourceVersion`— Facoltativamente, specificare un valore per limitare la raccolta dei log a una versione specifica dei dati di origine personalizzati.
- `crawlerConfiguration`— Specificate l'Amazon Resource Name (ARN) del ruolo IAM che avete creato per richiamare il crawler. AWS Glue Per i passaggi dettagliati per creare un ruolo IAM, consulta Prerequisiti per aggiungere una fonte personalizzata
- `providerIdentity`— Specificare l' AWS identità e l'ID esterno che l'origine utilizzerà per scrivere log ed eventi nel data lake.

L'esempio seguente aggiunge un'origine personalizzata come origine di registro nell'account del provider di log designato nelle regioni designate. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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”]
```

Mantenere aggiornati i dati di origine personalizzati in AWS Glue

Dopo aver aggiunto una fonte personalizzata in Security Lake, Security Lake crea un AWS Glue crawler. Il crawler si connette all'origine personalizzata, determina le strutture dei dati e popola il AWS Glue Data Catalog con tabelle.

Ti consigliamo di eseguire manualmente il crawler per mantenere aggiornato lo schema sorgente personalizzato e mantenere la funzionalità di interrogazione in Athena e in altri servizi di interrogazione. In particolare, è consigliabile eseguire il crawler se si verifica una delle seguenti modifiche nel set di dati di input per un'origine personalizzata:

- Il set di dati ha una o più nuove colonne di primo livello.
- Il set di dati contiene uno o più nuovi campi in una colonna con un tipo di `struct` dati.

Per istruzioni sull'esecuzione di un crawler, consulta Scheduling an AWS Glue crawler nella Developer Guide.AWS Glue

Security Lake non può eliminare o aggiornare i crawler esistenti nel tuo account. Se elimini un'origine personalizzata, ti consigliamo di eliminare il crawler associato se prevedi di creare un'origine personalizzata con lo stesso nome in futuro.

Eliminazione di una fonte personalizzata

Eliminare una fonte personalizzata per interrompere l'invio di dati dalla sorgente a Security Lake.

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, selezionate la regione da cui desiderate rimuovere la fonte personalizzata.
3. Nel riquadro di navigazione, scegli Fonti personalizzate.
4. Seleziona la fonte personalizzata che desideri rimuovere.
5. Scegli Annulla registrazione della fonte personalizzata, quindi scegli Elimina per confermare l'azione.

API

Per eliminare una fonte personalizzata a livello di codice, utilizza il DeleteCustomLogSourcefunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il delete-custom-log-sourcecomando. Utilizzate l'operazione nel Regione AWS punto in cui desiderate eliminare la fonte personalizzata.

Nella richiesta, utilizzate il `sourceName` parametro per specificare il nome dell'origine personalizzata da eliminare. Oppure specifica il nome dell'origine personalizzata e utilizza il `sourceVersion` parametro per limitare l'ambito dell'eliminazione solo a una versione specifica dei dati dell'origine personalizzata.

L'esempio seguente elimina un'origine di registro personalizzata da Security Lake.

Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

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

Gestione degli abbonati in Amazon Security Lake

Un abbonato ad Amazon Security Lake utilizza i log e gli eventi di Security Lake. Per controllare i costi e aderire alle migliori pratiche di accesso con privilegi minimi, fornisci agli abbonati l'accesso ai dati in base alla fonte. Per ulteriori informazioni sulle origini, consulta Gestione del codice in Amazon Security Lake.

Security Lake supporta due tipi di accesso per gli abbonati:

- Accesso ai dati: gli abbonati ricevono una notifica dei nuovi oggetti Amazon S3 per un'origine man mano che gli oggetti vengono scritti nel data lake Security Lake. Gli abbonati possono accedere direttamente agli oggetti S3 e ricevere notifiche di nuovi oggetti tramite un endpoint di sottoscrizione o eseguendo il polling di una coda Amazon Simple Queue Service (Amazon SQS). Questo tipo di abbonamento è identificato come `S3` nel parametro dell'API. `accessTypes` CreateSubscriber
- Accesso tramite query: gli abbonati interrogano i dati di origine dalle AWS Lake Formation tabelle del bucket S3 utilizzando servizi come Amazon Athena. Questo tipo di abbonamento è identificato `LAKEFORMATION` nel `accessTypes` parametro dell'API. CreateSubscriber

Gli abbonati hanno accesso solo ai dati di origine selezionati al Regione AWS momento della creazione dell'abbonato. Per consentire a un abbonato di accedere ai dati di più regioni, puoi specificare la regione in cui creare l'abbonato come regione di rollup e fare in modo che altre regioni forniscano i dati ad essa. Per ulteriori informazioni sulle regioni cumulative e sulle regioni contributrici, consulta. Gestione delle aree

> **Important**
>
> Il numero massimo di sorgenti che Security Lake consente di aggiungere per abbonato è 10. Potrebbe trattarsi di una combinazione di AWS fonti e fonti personalizzate.

Argomenti

- Gestione dell'accesso ai dati per gli abbonati a Security Lake
- Gestione dell'accesso alle query per gli abbonati a Security Lake

Gestione dell'accesso ai dati per gli abbonati a Security Lake

Gli abbonati con accesso ai dati di origine in Amazon Security Lake ricevono una notifica della presenza di nuovi oggetti per l'origine non appena i dati vengono scritti nel bucket S3. Per impostazione predefinita, gli abbonati ricevono notifiche sui nuovi oggetti tramite un endpoint HTTPS da loro fornito. In alternativa, gli abbonati possono ricevere notifiche sui nuovi oggetti eseguendo il polling di una coda Amazon Simple Queue Service (Amazon SQS).

Prerequisiti per la creazione di un abbonato con accesso ai dati

È necessario completare i seguenti prerequisiti prima di poter creare un abbonato con accesso ai dati in Security Lake.

Argomenti

Verificare le autorizzazioni

Per verificare le tue autorizzazioni, usa IAM per esaminare le policy IAM allegate alla tua identità IAM. Quindi, confronta le informazioni contenute in tali policy con il seguente elenco di azioni (autorizzazioni) necessarie per notificare agli abbonati quando vengono scritti nuovi dati nel data lake.

È necessaria l'autorizzazione per eseguire le seguenti azioni:

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

- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

Oltre all'elenco precedente, è necessaria anche l'autorizzazione per eseguire le seguenti azioni:

- `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`

Ottieni l'ID esterno dell'abbonato

Per creare un abbonato, oltre all' Account AWS ID dell'abbonato, dovrai anche ottenere il suo ID esterno. L'ID esterno è un identificatore univoco che l'abbonato ti fornisce. Security Lake aggiunge l'ID esterno al ruolo IAM del sottoscrittore che crea. Si utilizza l'ID esterno quando si crea un abbonato nella console di Security Lake, tramite l'API, oppure. AWS CLI

Per ulteriori informazioni sugli ID esterni, consulta Come utilizzare un ID esterno per concedere l'accesso alle tue AWS risorse a una terza parte nella Guida per l'utente IAM.

> **Important**
>
> Se prevedi di utilizzare la console Security Lake per aggiungere un abbonato, puoi saltare il passaggio successivo e procedere con. Creazione di un abbonato con accesso ai dati

La console Security Lake offre un processo semplificato per iniziare e crea tutti i ruoli IAM necessari o utilizza i ruoli esistenti per tuo conto.
Se prevedi di utilizzare l'API Security Lake o di AWS CLI aggiungere un abbonato, continua con il passaggio successivo per creare un ruolo IAM per richiamare EventBridge le destinazioni API.

Crea un ruolo IAM per richiamare le destinazioni EventBridge API (API e AWS CLI - only step)

Se utilizzi Security Lake tramite API oppure AWS CLI crea un ruolo in AWS Identity and Access Management (IAM) che conceda ad Amazon EventBridge le autorizzazioni per richiamare destinazioni API e inviare notifiche di oggetti agli endpoint HTTPS corretti.

Dopo aver creato questo ruolo IAM, avrai bisogno dell'Amazon Resource Name (ARN) del ruolo per creare il sottoscrittore. Questo ruolo IAM non è necessario se l'abbonato esegue il polling dei dati da una coda di Amazon Simple Queue Service (Amazon SQS) o interroga direttamente i dati da. AWS Lake Formation Per ulteriori informazioni su questo tipo di metodo di accesso ai dati (tipo di accesso), consulta. Gestione dell'accesso alle query per gli abbonati a Security Lake

Allega la seguente policy al tuo ruolo IAM:

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

Allega la seguente policy di fiducia al tuo ruolo IAM per EventBridge consentirti di assumere il ruolo:

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

Security Lake crea automaticamente un ruolo IAM che consente al sottoscrittore di leggere i dati dal data lake (o di interrogare gli eventi da una coda Amazon SQS se questo è il metodo di notifica preferito). Questo ruolo è protetto da una policy gestita chiamata. AWS `AmazonSecurityLakePermissionsBoundary`

Creazione di un abbonato con accesso ai dati

Scegli uno dei seguenti metodi di accesso per creare un abbonato con accesso ai dati nella versione corrente. Regione AWS

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, selezionate la regione in cui desiderate creare l'abbonato.
3. Nel riquadro di navigazione, scegli Abbonati.
4. Nella pagina Iscritti, scegli Crea sottoscrittore.
5. Per i dettagli dell'abbonato, inserisci il nome dell'abbonato e una descrizione opzionale.

   La regione viene compilata automaticamente come quella attualmente selezionata Regione AWS e non può essere modificata.
6. Per le sorgenti di log ed eventi, scegli quali fonti l'abbonato è autorizzato a utilizzare.
7. Per il metodo di accesso ai dati, scegli S3 per configurare l'accesso ai dati per l'abbonato.
8. Per le credenziali dell'abbonato, fornisci l'ID dell'abbonato e l'ID esterno. Account AWS

9. (Facoltativo) Per i dettagli sulle notifiche, se desideri che Security Lake crei una coda Amazon SQS che l'abbonato possa controllare per le notifiche degli oggetti, seleziona la coda SQS. Se desideri che Security Lake invii notifiche a un endpoint HTTPS, seleziona EventBridge Endpoint di sottoscrizione.

   Se selezioni Subscription endpoint, procedi anche come segue:

   a. Inserisci l'endpoint dell'abbonamento. Alcuni esempi di formati di endpoint validi includono. **`http://example.com`** Facoltativamente, puoi anche fornire un nome di chiave HTTPS e un valore di chiave HTTPS.

   b. Per Service Access, crea un nuovo ruolo IAM o utilizza un ruolo IAM esistente che EventBridge autorizzi a richiamare le destinazioni API e inviare notifiche sugli oggetti agli endpoint corretti.

      Per informazioni sulla creazione di un nuovo ruolo IAM, consulta Creare un ruolo IAM per richiamare EventBridge le destinazioni API.

10. (Facoltativo) Per i tag, inserisci fino a 50 tag da assegnare al sottoscrittore.

    Un tag è un'etichetta che puoi definire e assegnare a determinati tipi di risorse. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi. Per ulteriori informazioni, vedi Etichettatura delle risorse di Amazon Security Lake.

11. Scegli Crea.

API

Per creare un abbonato con accesso programmatico ai dati, utilizza il CreateSubscriberfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando create-subscriber.

Nella richiesta, utilizzate questi parametri per specificare le seguenti impostazioni per l'abbonato:

- Per`sources`, specifica ogni fonte a cui desideri che l'abbonato acceda.
- Per`subscriberIdentity`, specifica l'ID dell' AWS account e l'ID esterno che l'abbonato utilizzerà per accedere ai dati di origine.
- Per`subscriber-name`, specificare il nome del sottoscrittore.
- Per `accessTypes`, specificare `S3`.

Esempio 1

L'esempio seguente crea un sottoscrittore con accesso ai dati nella AWS regione corrente per l'identità di sottoscrittore specificata per un'origine. AWS

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{awsLogSource: {sourceName: VPC_FLOW, sourceVersion: 1.0}}] \
--subscriber-name subscriber name \
--access-types S3
```

Esempio 2

L'esempio seguente crea un abbonato con accesso ai dati nella AWS regione corrente per l'identità di sottoscrittore specificata per un'origine personalizzata.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{customLogSource: {sourceName: custom-source-name, sourceVersion: 1.0}}]
 \
--subscriber-name subscriber name
--access-types S3
```

Gli esempi precedenti sono formattati per Linux, macOS o Unix e utilizzano il carattere di continuazione di riga rovesciata (\) per migliorare la leggibilità.

(Facoltativo) Dopo aver creato un sottoscrittore, utilizzate l'CreateSubscriberNotificationoperazione per specificare come notificare al sottoscrittore quando vengono scritti nuovi dati nel data lake per le fonti a cui desiderate che l'abbonato acceda. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando. create-subscriber-notification

- Per sovrascrivere il metodo di notifica predefinito (endpoint HTTPS) e creare una coda Amazon SQS, specifica i valori per i parametri. `sqsNotificationConfiguration`
- Se preferisci la notifica con un endpoint HTTPS, specifica i valori per i parametri. `httpsNotificationConfiguration`
- Per il `targetRoleArn` campo, specifica l'ARN del ruolo IAM che hai creato per richiamare EventBridge le destinazioni 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"}
```

Per ottenerlo`subscriberID`, utilizza il ListSubscribersfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando list-subscriber.

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

Per modificare successivamente il metodo di notifica (coda Amazon SQS o endpoint HTTPS) per l'abbonato, utilizza l'UpdateSubscriberNotificationoperazione o, se utilizzi il, esegui il AWS CLI comando. update-subscriber-notification Puoi anche modificare il metodo di notifica utilizzando la console Security Lake: seleziona l'abbonato nella pagina Sottoscrittori, quindi scegli Modifica.

Esempio di messaggio di notifica dell'oggetto

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

```
  }
}
```

Aggiornamento di un abbonato ai dati

È possibile aggiornare un abbonato modificando le fonti da cui l'abbonato consuma. Puoi anche assegnare o modificare i tag per un abbonato. Un tag è un'etichetta che puoi definire e assegnare a determinati tipi di AWS risorse, inclusi gli abbonati. Per ulteriori informazioni, vedi Etichettatura delle risorse di Amazon Security Lake.

Scegli uno dei metodi di accesso e segui questi passaggi per definire nuove fonti per un abbonamento esistente.

Console

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, scegli Abbonati.
3. Seleziona l'abbonato.
4. Scegli Modifica, quindi esegui una delle seguenti operazioni:
   - Per aggiornare le fonti per l'abbonato, inserisci le nuove impostazioni nella sezione Registri e fonti di eventi.
   - Per assegnare o modificare i tag per l'abbonato, modificali se necessario nella sezione Tag.
5. Al termine, scegli Salva.

API

Per aggiornare le fonti di accesso ai dati per un abbonato in modo programmatico, utilizza il UpdateSubscriberfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando update-subscriber. Nella richiesta, utilizzate i `sources` parametri per specificare ogni fonte a cui desiderate che l'abbonato acceda.

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

Per un elenco di abbonati associati a una specifica Account AWS o organizzazione, usa l'ListSubscribersoperazione. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando list-subscribers.

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

Per rivedere le impostazioni correnti per un particolare abbonato, usa l'GetSubscriberoperazione. esegui il comando get-subscriber. Security Lake restituisce quindi il nome e la descrizione dell'abbonato, l'ID esterno e informazioni aggiuntive. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando get-subscriber.

Per aggiornare il metodo di notifica per un sottoscrittore, utilizzate l'operazione. UpdateSubscriberNotification Se stai usando il AWS Command Line Interface (AWS CLI), esegui il update-subscriber-notificationcomando. Ad esempio, puoi specificare un nuovo endpoint HTTPS per l'abbonato o passare da un endpoint HTTPS a una coda Amazon SQS.

Rimuovere un abbonato ai dati

Se non desideri più che un abbonato utilizzi i dati di Security Lake, puoi rimuovere l'abbonato seguendo questi passaggi.

Console

1. Apri la console di Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, scegli Abbonati.
3. Seleziona l'abbonato che desideri rimuovere.
4. Scegliere Elimina e confermare l'operazione. Questo eliminerà l'abbonato e tutte le impostazioni di notifica associate.

API

In base allo scenario, esegui una delle seguenti operazioni:

- Per eliminare il sottoscrittore e tutte le impostazioni di notifica associate, utilizza il DeleteSubscriberfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando delete-subscriber.
- Per mantenere l'abbonato ma interrompere le future notifiche all'abbonato, utilizza il DeleteSubscriberNotificationfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando run the delete-subscriber-notification.

Gestione dell'accesso alle query per gli abbonati a Security Lake

Gli abbonati con accesso alle query possono interrogare i dati raccolti da Security Lake. Questi abbonati interrogano direttamente AWS Lake Formation le tabelle nel tuo bucket S3 con servizi come Amazon Athena. Sebbene il motore di query principale per Security Lake sia Athena, puoi utilizzare anche altri servizi, come Amazon Redshift Spectrum e Spark SQL, che si integrano con. AWS Glue Data Catalog

> **Note**
>
> Questa sezione spiega come concedere l'accesso alle query a un abbonato di terze parti. Per informazioni sull'esecuzione di query sul tuo data lake, consulta. Passaggio 4: Visualizza e interroga i tuoi dati

Prerequisiti per la creazione di un sottoscrittore con accesso alle query

È necessario completare i seguenti prerequisiti prima di poter creare un abbonato con accesso ai dati in Security Lake.

Argomenti

- Verificare le autorizzazioni
- Crea un ruolo IAM per interrogare i dati di Security Lake (API e fase solo AWS CLI)
- Concedi le autorizzazioni di amministratore di Lake Formation

Verificare le autorizzazioni

Prima di creare un abbonato con accesso tramite query, verificate di disporre dell'autorizzazione per eseguire il seguente elenco di azioni.

Per verificare le tue autorizzazioni, usa IAM per esaminare le policy IAM allegate alla tua identità IAM. Quindi, confronta le informazioni contenute in tali policy con il seguente elenco di azioni che devi essere autorizzato a eseguire per creare un abbonato con accesso tramite query.

- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`

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

> **Important**
>
> Dopo aver verificato le autorizzazioni:
>
> - Se prevedi di utilizzare la console Security Lake per aggiungere un abbonato con accesso alle query, puoi saltare il passaggio successivo e procedere con. Concedi le autorizzazioni di amministratore di Lake Formation Security Lake crea tutti i ruoli IAM necessari o utilizza i ruoli esistenti per tuo conto.
> - Se prevedi di utilizzare l'API o la CLI di Security Lake per aggiungere un sottoscrittore con accesso alle query, continua con il passaggio successivo per creare un ruolo IAM per interrogare i dati di Security Lake.

Crea un ruolo IAM per interrogare i dati di Security Lake (API e fase solo AWS CLI)

Quando si utilizza l'API Security Lake o AWS CLI si concede l'accesso alle query a un abbonato, è necessario creare un ruolo denominato. `AmazonSecurityLakeMetaStoreManager` Security Lake utilizza questo ruolo per registrare le AWS Glue partizioni e aggiornare AWS Glue le tabelle. Potresti aver già creato questo ruolo durante la creazione dei ruoli IAM necessari.

Concedi le autorizzazioni di amministratore di Lake Formation

Dovrai anche aggiungere le autorizzazioni di amministratore di Lake Formation al ruolo IAM che usi per accedere alla console di Security Lake e aggiungere abbonati.

Puoi concedere le autorizzazioni di amministratore di Lake Formation per il tuo ruolo seguendo questi passaggi:

1. Aprire la console Lake Formation all'indirizzo https://console.aws.amazon.com/lakeformation/.
2. Accedi come utente amministrativo.
3. Se viene visualizzata la finestra Welcome to Lake Formation, scegli l'utente che hai creato o selezionato nel Passaggio 1, quindi scegli Inizia.
4. Se non vedi la finestra Welcome to Lake Formation, esegui i seguenti passaggi per configurare un Lake Formation Administrator.

    1. Nel pannello di navigazione, in Autorizzazioni, scegli Ruoli e attività amministrative. Nella sezione Amministratori di Data lake, scegli Scegli amministratori.
    2. Nella finestra di dialogo Gestisci gli amministratori del data lake, per gli utenti e i ruoli IAM, scegli il ruolo di amministratore utilizzato per accedere alla console di Security Lake, quindi scegli Salva.

Per ulteriori informazioni sulla modifica delle autorizzazioni per gli amministratori del data lake, consulta Create a data lake administrator nella Developer Guide. AWS Lake Formation

Il ruolo IAM deve disporre di `SELECT` privilegi sul database e sulle tabelle a cui desideri concedere l'accesso a un sottoscrittore. Per istruzioni su come eseguire questa operazione, consulta Concessione delle autorizzazioni di Data Catalog utilizzando il metodo della risorsa denominata nella Guida per gli sviluppatori. AWS Lake Formation

Creazione di un abbonato con accesso tramite query

Scegli il tuo metodo preferito per creare un abbonato con accesso alle query tra quelli correnti. Regione AWS Un sottoscrittore può interrogare i dati solo dai dati in Regione AWS cui è stato creato. Per creare un abbonato, è necessario disporre dell' Account AWS ID e dell'ID esterno dell'abbonato. L'ID esterno è un identificatore univoco che l'abbonato ti fornisce. Per ulteriori informazioni sugli ID esterni, consulta Come utilizzare un ID esterno per concedere l'accesso alle tue AWS risorse a una terza parte nella Guida per l'utente IAM.

> **Note**
>
> Security Lake non supporta la versione 1 di condivisione dei dati tra account di Lake Formation. È necessario aggiornare la condivisione dei dati tra account di Lake Formation alla versione 2 o alla versione 3. Per i passaggi per aggiornare le impostazioni della versione di Cross Account tramite la AWS Lake Formation console o la AWS CLI, consulta Abilitare la nuova versione nella AWS Lake Formation Developer Guide.

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedere all'account amministratore delegato.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri creare l'abbonato.
3. Nel riquadro di navigazione, scegli Abbonati.
4. Nella pagina Iscritti, scegli Crea sottoscrittore.
5. Per i dettagli dell'abbonato, inserisci il nome dell'abbonato e una descrizione opzionale.

   La regione viene compilata automaticamente come quella attualmente selezionata Regione AWS e non può essere modificata.
6. Per le sorgenti di log ed eventi, scegli quali fonti desideri che Security Lake includa quando restituisci i risultati delle query.
7. Per Metodo di accesso ai dati, scegli Lake Formation per creare l'accesso alle query per l'abbonato.
8. Per le credenziali dell'abbonato, fornisci l' Account AWS ID dell'abbonato e l'ID esterno.
9. (Facoltativo) Per i tag, inserisci fino a 50 tag da assegnare all'abbonato.

   Un tag è un'etichetta che puoi definire e assegnare a determinati tipi di risorse. AWS Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi. Per ulteriori informazioni, vedi Etichettatura delle risorse di Amazon Security Lake.
10. Scegli Crea.

API

Per creare un abbonato con accesso alle query a livello di codice, utilizza il CreateSubscriberfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando create-subscriber.

Nella richiesta, utilizzate questi parametri per specificare le seguenti impostazioni per l'abbonato:

- Per `accessTypes`, specificare `LAKEFORMATION`.
- Per`sources`, specifica ogni fonte che desideri che Security Lake includa quando restituisce i risultati delle query.

- Per `subscriberIdentity`, specifica l' AWS identità e l'ID esterno utilizzati dal sottoscrittore per interrogare i dati di origine.

L'esempio seguente crea un sottoscrittore con accesso tramite query nella AWS regione corrente per l'identità di sottoscrittore specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 129345678912,"externalId": 123456789012} \
--sources [{awsLogSource: {sourceName: VPC_FLOW, sourceVersion: 1.0}}] \
--subscriber-name subscriber name \
--access-types LAKEFORMATION
```

Configurazione della condivisione delle tabelle tra account (fase di sottoscrizione)

Security Lake utilizza la condivisione di tabelle tra account di Lake Formation per supportare l'accesso alle query degli abbonati. Quando si crea un sottoscrittore con accesso alle query nella console, nell'API o nell'API di Security Lake AWS CLI, Security Lake condivide le informazioni sulle tabelle pertinenti di Lake Formation con l'abbonato creando una condivisione di risorse in AWS Resource Access Manager ()AWS RAM.

Quando si apportano determinati tipi di modifiche a un abbonato con accesso tramite query, Security Lake crea una nuova condivisione di risorse. Per ulteriori informazioni, consulta Modifica di un abbonato con accesso tramite interrogazione.

L'abbonato deve seguire questi passaggi per consumare i dati dalle tabelle di Lake Formation:

1. Accetta la condivisione di risorse: il sottoscrittore deve accettare la condivisione di risorse che contiene `resourceShareArn` e `resourceShareName` che viene generata quando crei o modifichi il sottoscrittore. Scegli uno dei seguenti metodi di accesso:
   - Per console e AWS CLI, vedi Accettazione di un invito alla condivisione di risorse da AWS RAM.
   - Per l'API, richiama l'GetResourceShareInvitationsAPI. Filtra per `resourceShareArn` e `resourceShareName` per trovare la condivisione di risorse corretta. Accetta l'invito con l'AcceptResourceShareInvitationAPI.

L'invito alla condivisione delle risorse scade tra 12 ore, quindi devi convalidarlo e accettarlo entro 12 ore. Se l'invito scade, continui a vederlo in uno `PENDING` stato, ma accettandolo non avrai accesso alle risorse condivise. Trascorse più di 12 ore, elimina l'abbonato Lake Formation e ricrea l'abbonato per ricevere un nuovo invito alla condivisione di risorse.

2. Creare un collegamento di risorse alle tabelle condivise: l'abbonato deve creare un collegamento di risorsa alle tabelle condivise di Lake Formation in uno AWS Lake Formation (se utilizza la console) o AWS Glue (se utilizza API/AWS CLI). Questo collegamento alle risorse indirizza l'account dell'abbonato alle tabelle condivise. Scegli uno dei seguenti metodi di accesso:
   - Per console e AWS CLI, consulta Creazione di un collegamento di risorsa a una tabella condivisa del catalogo dati nella Guida per gli AWS Lake Formation sviluppatori.
   - Per l'API, richiama l' AWS Glue CreateTableAPI. Consigliamo agli abbonati di creare anche un database unico con l'CreateDatabaseAPI per archiviare le tabelle dei link alle risorse.
3. Interroga le tabelle condivise: servizi come Amazon Athena possono fare riferimento direttamente alle tabelle e i nuovi dati raccolti da Security Lake sono automaticamente disponibili per le query. Le query vengono eseguite presso l'abbonato e i costi sostenuti per esse vengono fatturati all'abbonato. Account AWS Puoi controllare l'accesso in lettura alle risorse nel tuo account Security Lake.

Per ulteriori informazioni sulla concessione delle autorizzazioni su più account, consulta Condivisione dei dati tra account in Lake Formation nella Developer Guide. AWS Lake Formation

Modifica di un abbonato con accesso tramite interrogazione

Security Lake supporta la modifica di un abbonato con accesso tramite query. È possibile modificare il nome, la descrizione, l'ID esterno, il principale (Account AWS ID) dell'abbonato e le fonti di registro che l'abbonato è in grado di utilizzare. Scegli il tuo metodo preferito e segui i passaggi per modificare un abbonato con accesso alle query tra quelli correnti. Regione AWS

> **Note**
>
> Security Lake non supporta la versione 1 di condivisione dei dati tra account di Lake Formation. È necessario aggiornare la condivisione dei dati tra account di Lake Formation alla versione 2 o alla versione 3. Per i passaggi per aggiornare le impostazioni della versione di Cross Account tramite la AWS Lake Formation console o la AWS CLI, consulta Abilitare la nuova versione nella AWS Lake Formation Developer Guide.

Console

In base ai dettagli che desideri modificare, segui i passaggi forniti solo per quell'azione.

Per modificare il nome dell'abbonato

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedere all'account amministratore delegato.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri modificare i dettagli dell'abbonato.
3. Nel riquadro di navigazione, scegli Abbonati.
4. Nella pagina Iscritti, utilizza il pulsante di opzione per selezionare l'abbonato che desideri modificare. Il metodo di accesso ai dati per l'abbonato selezionato deve essere LAKEFORMATION.
5. Scegli Modifica.
6. Inserisci il nuovo nome del sottoscrittore e scegli Salva.

Per modificare la descrizione dell'abbonato

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedere all'account amministratore delegato.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri modificare l'abbonato.
3. Nel riquadro di navigazione, scegli Sottoscrittori.
4. Nella pagina Iscritti, utilizza il pulsante di opzione per selezionare l'abbonato che desideri modificare. Il metodo di accesso ai dati per l'abbonato selezionato deve essere LAKEFORMATION.
5. Scegli Modifica.
6. Inserisci la nuova descrizione per l'abbonato e scegli Salva.

Per modificare un ID esterno

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedere all'account amministratore delegato.

2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri modificare i dettagli dell'abbonato.
3. Nel riquadro di navigazione, scegli Abbonati.
4. Nella pagina Iscritti, utilizza il pulsante di opzione per selezionare l'abbonato che desideri modificare. Il metodo di accesso ai dati per l'abbonato selezionato deve essere LAKEFORMATION.
5. Scegli Modifica.
6. Inserisci il nuovo ID esterno fornito dall'abbonato e scegli Salva.

   Il salvataggio del nuovo ID esterno rimuove automaticamente la condivisione di AWS RAM risorse precedente e crea una nuova condivisione di risorse per l'abbonato.
7. Il sottoscrittore deve accettare la nuova condivisione di risorse seguendo il passaggio 1 di. Configurazione della condivisione delle tabelle tra account (fase di sottoscrizione) Assicurati che l'Amazon Resource Name (ARN) visualizzato nei dettagli dell'abbonato sia lo stesso della console Lake Formation. Il collegamento della risorsa alle tabelle condivise rimane invariato, quindi l'abbonato non deve creare un nuovo collegamento alla risorsa.

Per modificare il principale (Account AWS ID)

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedere all'account amministratore delegato.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri modificare i dettagli dell'abbonato.
3. Nel riquadro di navigazione, scegli Abbonati.
4. Nella pagina Iscritti, utilizza il pulsante di opzione per selezionare l'abbonato che desideri modificare. Il metodo di accesso ai dati per l'abbonato selezionato deve essere LAKEFORMATION.
5. Scegli Modifica.
6. Inserisci il nuovo Account AWS ID dell'abbonato e scegli Salva.

   Il salvataggio del nuovo ID account rimuove automaticamente la condivisione di AWS RAM risorse precedente, in modo che il principale precedente non possa utilizzare i registri e le fonti degli eventi. Security Lake crea una nuova condivisione di risorse.

7. Utilizzando le credenziali del nuovo principale, il sottoscrittore deve accettare la nuova condivisione di risorse e creare un collegamento di risorsa alle tabelle condivise. Ciò consente al nuovo principale di accedere alle risorse condivise. Per istruzioni, vedere i passaggi 1 e 2 di seguitoConfigurazione della condivisione delle tabelle tra account (fase di sottoscrizione). Assicurati che l'ARN visualizzato nei dettagli dell'abbonato sia lo stesso della console Lake Formation.

Per modificare le sorgenti di log ed eventi

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

   Accedere all'account amministratore delegato.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri modificare i dettagli dell'abbonato.
3. Nel riquadro di navigazione, scegli Abbonati.
4. Nella pagina Iscritti, utilizza il pulsante di opzione per selezionare l'abbonato che desideri modificare. Il metodo di accesso ai dati per l'abbonato selezionato deve essere LAKEFORMATION.
5. Scegli Modifica.
6. Deseleziona le fonti esistenti o seleziona le fonti che desideri aggiungere. Se deselezionate una fonte, non sono necessarie ulteriori azioni da parte vostra. Se si sceglie di aggiungere una fonte, non viene creato alcun nuovo invito alla condivisione delle risorse. Tuttavia, Security Lake aggiorna le tabelle condivise di Lake Formation in base alle fonti aggiunte. Il sottoscrittore deve creare un collegamento di risorsa alle tabelle condivise aggiornate in modo da poter interrogare i dati di origine. Per istruzioni, consulta la fase 2 diConfigurazione della condivisione delle tabelle tra account (fase di sottoscrizione).
7. Selezionare Salva.

API

Per modificare un sottoscrittore con accesso alle query a livello di programmazione, utilizza il UpdateSubscriberfunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando update-subscriber. Nella richiesta, utilizzate i parametri supportati per specificare le seguenti impostazioni per l'abbonato:

- `PersubscriberName`, specifica il nome del nuovo abbonato.
- `PersubscriberDescription`, specifica la nuova descrizione.
- `PersubscriberIdentity`, specifica il principale (Account AWS ID) e l'ID esterno che il sottoscrittore utilizzerà per interrogare i dati di origine. È necessario fornire sia l'ID principale che l'ID esterno. Se vuoi mantenere invariato uno di questi valori, inserisci il valore corrente.
  - Aggiornamento solo dell'ID esterno: questa azione rimuove la condivisione di AWS RAM risorse precedente e crea una nuova condivisione di risorse per l'abbonato. Il sottoscrittore deve accettare la nuova condivisione di risorse seguendo il passaggio 1 di. Configurazione della condivisione delle tabelle tra account (fase di sottoscrizione) Il collegamento della risorsa alle tabelle condivise rimane invariato, quindi il sottoscrittore non deve creare un nuovo collegamento alla risorsa.
  - Aggiornamento solo del principale: questa azione rimuove la condivisione di AWS RAM risorse precedente in modo che il principale precedente non possa utilizzare i registri e le fonti degli eventi. Security Lake crea una nuova condivisione di risorse. Utilizzando le credenziali del nuovo principale, il sottoscrittore deve accettare la nuova condivisione di risorse e creare un collegamento di risorsa alle tabelle condivise. Ciò consente al nuovo principale di accedere alle risorse condivise. Per istruzioni, vedere i passaggi 1 e 2 di seguitoConfigurazione della condivisione delle tabelle tra account (fase di sottoscrizione).

  Per aggiornare l'ID esterno e il principale, segui i passaggi 1 e 2 di cui sopraConfigurazione della condivisione delle tabelle tra account (fase di sottoscrizione).
- `Persources`, rimuovi le fonti esistenti o specifica le fonti che desideri aggiungere. Se rimuovi una fonte, non sono necessarie ulteriori azioni da parte tua. Se aggiungi una fonte, non viene creato alcun nuovo invito alla condivisione delle risorse. Tuttavia, Security Lake aggiorna le tabelle condivise di Lake Formation in base alle fonti aggiunte. Il sottoscrittore deve creare un collegamento di risorsa alle tabelle condivise aggiornate in modo da poter interrogare i dati di origine. Per istruzioni, consulta la fase 2 diConfigurazione della condivisione delle tabelle tra account (fase di sottoscrizione).

Domande su Security Lake

È possibile interrogare i dati archiviati da Security Lake in AWS Lake Formation database e tabelle. Puoi anche creare abbonati di terze parti nella console, nell'API di Security Lake o AWS CLI. Gli abbonati di terze parti possono anche interrogare i dati di Lake Formation dalle fonti specificate.

L'amministratore del data lake Lake Formation deve concedere `SELECT` le autorizzazioni per i database e le tabelle pertinenti all'identità IAM che interroga i dati. È inoltre necessario creare un sottoscrittore in Security Lake prima di poter interrogare i dati. Per ulteriori informazioni su come creare un sottoscrittore con accesso alle query, vedere. Gestione dell'accesso alle query per gli abbonati a Security Lake

Argomenti

Interrogazioni di Security Lake per la versione sorgente 1

La sezione seguente fornisce indicazioni sull'interrogazione dei dati da Security Lake e include alcuni esempi di query per fonti supportate nativamente. AWS Queste interrogazioni sono progettate per recuperare dati in un ambiente specifico. Regione AWS Questi esempi utilizzano us-east-1 (Stati Uniti orientali (Virginia settentrionale)). Inoltre, le query di esempio utilizzano un `LIMIT 25` parametro che restituisce fino a 25 record. È possibile omettere questo parametro o modificarlo in base alle proprie preferenze. Per altri esempi, consulta la directory delle query GitHub OCSF di Amazon Security Lake.

Tabella dei sorgenti dei log

Quando si interrogano i dati di Security Lake, è necessario includere il nome della tabella Lake Formation in cui risiedono i dati.

```
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
```

I valori comuni per la tabella delle sorgenti dei log includono quanto segue:

- `cloud_trail_mgmt_1_0`— eventi AWS CloudTrail di gestione
- `lambda_execution_1_0`— eventi CloudTrail relativi ai dati per Lambda
- `s3_data_1_0`— eventi CloudTrail relativi ai dati per S3
- `route53_1_0`— Registri delle query del resolver Amazon Route 53
- `sh_findings_1_0` AWS Security Hub — risultati
- `vpc_flow_1_0`— Registri di flusso di Amazon Virtual Private Cloud (Amazon VPC)

Esempio: tutti i risultati del Security Hub nella tabella **`sh_findings_1_0`** della regione 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
```

Regione del database

Quando si interrogano i dati di Security Lake, è necessario includere il nome della regione del database da cui si eseguono le query sui dati. Per un elenco completo delle regioni di database in cui Security Lake è attualmente disponibile, consulta Amazon Security Lake endpoints.

Esempio: elenca AWS CloudTrail l'attività dall'IP di origine

L'esempio seguente elenca tutte le CloudTrail attività dell'IP di origine 192.0.2.1 che sono state registrate dopo 20230301 (1 marzo 2023), nella tabella cloud_trail_mgmt_1_0 from the 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 della partizione

Partizionando i dati, è possibile limitare la quantità di dati analizzati da ciascuna query, migliorando così le prestazioni e riducendo i costi. Security Lake implementa il partizionamento tramite, e parametri. `eventDay` `region` `accountid` `eventDay`le partizioni utilizzano il formato. `YYYYMMDD`

Questo è un esempio di query che utilizza la `eventDay` partizione:

```
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
```

I valori comuni `eventDay` includono quanto segue:

Eventi verificatisi nell'ultimo anno

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

Eventi verificatisi nell'ultimo mese

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

Eventi verificatisi negli ultimi 30 giorni

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

Eventi che si sono verificati nelle ultime 12 ore

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

Eventi che si sono verificati negli ultimi 5 minuti

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

Eventi avvenuti tra 7 e 14 giorni fa

```
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)
```

Eventi che si verificano a partire da una data specifica

```
>= '20230301'
```

Esempio: elenco di tutte le CloudTrail attività dall'IP **`192.0.2.1`** di origine a partire dal 1° marzo 2023 o dopo tale data nella tabella **`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
```

Esempio: elenco di tutte le CloudTrail attività dall'IP di origine **`192.0.2.1`** negli ultimi 30 giorni nella tabella **`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
```

Esempi di interrogazioni relative ai dati CloudTrail

AWS CloudTrail tiene traccia dell'attività degli utenti e dell'utilizzo delle API in Servizi AWS. Gli abbonati possono interrogare CloudTrail i dati per conoscere i seguenti tipi di informazioni:

Ecco alcuni esempi di interrogazioni relative ai dati: CloudTrail

Tentativi non autorizzati Servizi AWS negli ultimi 7 giorni

```
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
```

Elenco di tutte le CloudTrail attività effettuate dall'IP di origine **`192.0.2.1`** negli ultimi 7 giorni

```
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
```

Elenco di tutte le attività IAM negli ultimi 7 giorni

```
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
```

Istanze in cui la credenziale **`AIDACKCEVSQ6C2EXAMPLE`** è stata utilizzata negli ultimi 7 giorni

```
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
```

Elenco dei CloudTrail record non riusciti negli ultimi 7 giorni

```
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
```

Query di esempio per i log delle query del resolver Route 53

I log delle query resolver di Amazon Route 53 tengono traccia delle query DNS effettuate dalle risorse all'interno del tuo Amazon VPC. Gli abbonati possono interrogare i log delle query del resolver Route 53 per conoscere i seguenti tipi di informazioni:

Ecco alcuni esempi di query relative ai log delle query del resolver Route 53:

Elenco delle query DNS degli ultimi 7 giorni CloudTrail

```
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
```

Elenco delle query DNS corrispondenti **`s3.amazonaws.com`** negli ultimi 7 giorni

```
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
```

Elenco di query DNS che non sono state risolte negli ultimi 7 giorni

```
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
```

Elenco delle query DNS risolte **`192.0.2.1`** negli ultimi 7 giorni

```
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
```

Query di esempio per i risultati del Security Hub

Security Hub ti offre una visione completa dello stato di sicurezza AWS e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Security Hub produce risultati per i controlli di sicurezza e riceve risultati da servizi di terze parti.

Ecco alcuni esempi di interrogazioni relative ai risultati del Security Hub:

Nuovi risultati con gravità maggiore o uguale **`MEDIUM`** a quella degli ultimi 7 giorni

```
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
```

Risultati duplicati negli ultimi 7 giorni

```
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
```

Tutti i risultati non informativi degli ultimi 7 giorni

```
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
```

Risultati in cui la risorsa è un bucket Amazon S3 (nessuna limitazione di 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 = 'AwsS3Bucket')
   LIMIT 25
```

I risultati ottenuti con un Common Vulnerability Scoring System (CVSS) hanno ottenuto un punteggio superiore a (nessuna limitazione di tempo) **1**

```
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
```

Risultati che corrispondono a Common Vulnerabilities and Exposures (CVE) (nessuna limitazione di tempo) **`CVE-0000-0000`**

```
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
```

Numero di prodotti che hanno inviato risultati da Security Hub negli ultimi 7 giorni

```
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
```

Numero di tipi di risorse nei risultati degli ultimi 7 giorni

```
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
```

Pacchetti vulnerabili in base ai risultati degli ultimi 7 giorni

```
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
```

Risultati che sono cambiati negli ultimi 7 giorni

```
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
```

Query di esempio per Amazon VPC Flow Logs

Amazon Virtual Private Cloud (Amazon VPC) fornisce dettagli sul traffico IP in entrata e in uscita dalle interfacce di rete nel tuo VPC.

Ecco alcuni esempi di query di Amazon VPC Flow Logs:

Traffico specifico Regioni AWS negli ultimi 7 giorni

```
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
```

Elenco delle attività dall'IP di origine **`192.0.2.1`** e dalla porta di origine **22** negli ultimi 7 giorni

```
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
```

Numero di indirizzi IP di destinazione distinti negli ultimi 7 giorni

```
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
```

Traffico proveniente da 198.51.100.0/24 negli ultimi 7 giorni

```
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
```

Tutto il traffico HTTPS negli ultimi 7 giorni

```
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
```

Ordina per numero di pacchetti per le connessioni destinate alla porta **443** negli ultimi 7 giorni

```
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
```

Tutto il traffico tra IP **192.0.2.1** e **192.0.2.2** negli ultimi 7 giorni

```
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
```

Tutto il traffico in entrata negli ultimi 7 giorni

```
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
```

Tutto il traffico in uscita negli ultimi 7 giorni

```
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
```

Tutto il traffico rifiutato negli ultimi 7 giorni

```
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
```

Interrogazioni di Security Lake per la versione sorgente 2

È possibile interrogare i dati archiviati da Security Lake in AWS Lake Formation database e tabelle. Puoi anche creare abbonati di terze parti nella console, nell'API di Security Lake o AWS CLI. Gli abbonati di terze parti possono anche interrogare i dati di Lake Formation dalle fonti specificate.

L'amministratore del data lake Lake Formation deve concedere `SELECT` le autorizzazioni per i database e le tabelle pertinenti all'identità IAM che interroga i dati. È inoltre necessario creare un sottoscrittore in Security Lake prima di poter interrogare i dati. Per ulteriori informazioni su come creare un sottoscrittore con accesso alle query, vedere. Gestione dell'accesso alle query per gli abbonati a Security Lake

La sezione seguente fornisce indicazioni sull'interrogazione dei dati da Security Lake e include alcuni esempi di query per fonti supportate in modo nativo AWS . Queste interrogazioni sono progettate per recuperare dati in un ambiente specifico. Regione AWS Questi esempi utilizzano us-east-1 (Stati Uniti orientali (Virginia settentrionale)). Inoltre, le query di esempio utilizzano un `LIMIT 25` parametro che restituisce fino a 25 record. È possibile omettere questo parametro o modificarlo in base alle proprie preferenze. Per altri esempi, consulta la directory delle query GitHub OCSF di Amazon Security Lake.

Tabella dei sorgenti dei log

Quando si interrogano i dati di Security Lake, è necessario includere il nome della tabella Lake Formation in cui risiedono i dati.

```
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
```

I valori comuni per la tabella delle sorgenti dei log includono quanto segue:

- `cloud_trail_mgmt_2_0`— eventi AWS CloudTrail di gestione
- `lambda_execution_2_0`— eventi CloudTrail relativi ai dati per Lambda
- `s3_data_2_0`— eventi CloudTrail relativi ai dati per S3
- `route53_2_0`— Registri delle query del resolver Amazon Route 53
- `sh_findings_2_0` AWS Security Hub — risultati
- `vpc_flow_2_0`— Registri di flusso di Amazon Virtual Private Cloud (Amazon VPC)
- `eks_audit_2_0`— Registri di controllo di Amazon Elastic Kubernetes Service (Amazon EKS)

Esempio: tutti i risultati del Security Hub nella tabella **`sh_findings_2_0`** della regione 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
```

Regione del database

Quando si interrogano i dati di Security Lake, è necessario includere il nome della regione del database da cui si eseguono le query sui dati. Per un elenco completo delle regioni di database in cui Security Lake è attualmente disponibile, consulta Amazon Security Lake endpoints.

Esempio: elenca l'attività di Amazon Virtual Private Cloud dall'IP di origine

L'esempio seguente elenca tutte le attività Amazon VPC dall'IP di origine 192.0.2.1 che sono state registrate dopo 20230301 (1 marzo 2023), nella tabella vpc_flow_2_0 da 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 della partizione

Partizionando i dati, è possibile limitare la quantità di dati analizzati da ciascuna query, migliorando così le prestazioni e riducendo i costi. Le partizioni funzionano in modo leggermente diverso in Security Lake 2.0 rispetto a Security Lake 1.0. Security Lake ora implementa il partizionamento tramite`time_dt`, e. `region` `accountid` Security Lake 1.0 ha invece implementato il partizionamento tramite`eventDay`, e parametri. `region` `accountid`

L'interrogazione `time_dt` produrrà automaticamente le partizioni di data da S3 e può essere interrogata proprio come qualsiasi campo basato sull'ora in Athena.

Questo è un esempio di query che utilizza la `time_dt` partizione per interrogare i log dopo il 1° marzo 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
```

I valori comuni `time_dt` includono quanto segue:

Eventi verificatisi nell'ultimo anno

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

Eventi verificatisi nell'ultimo mese

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

Eventi verificatisi negli ultimi 30 giorni

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

Eventi verificatisi nelle ultime 12 ore

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

Eventi che si sono verificati negli ultimi 5 minuti

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

Eventi avvenuti tra 7 e 14 giorni fa

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

Eventi che si verificano a partire da una data specifica

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

Esempio: elenco di tutte le CloudTrail attività dall'IP **`192.0.2.1`** di origine a partire dal 1° marzo 2023 o dopo tale data nella tabella **`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
```

Esempio: elenco di tutte le CloudTrail attività dall'IP di origine **`192.0.2.1`** negli ultimi 30 giorni nella tabella **`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
```

Interrogazione degli osservabili di Security Lake

Observables è una nuova funzionalità ora disponibile in Security Lake 2.0. L'oggetto osservabile è un elemento pivot che contiene informazioni correlate che si trovano in molti punti dell'evento. L'interrogazione degli osservabili consente agli utenti di ricavare informazioni di sicurezza di alto livello da tutti i loro set di dati.

Interrogando elementi specifici all'interno degli osservabili, puoi limitare i set di dati a cose come nomi utente specifici, UID di risorse, IP, hash e altre informazioni di tipo IOC

Questa è una query di esempio che utilizza l'array observables per interrogare i log nelle tabelle VPC Flow e Route53 contenenti il valore IP '172.01.02.03'

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

```
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip')
SELECT * FROM a
LEFT JOIN b ON a.value=b.value and a.name=b.name
LIMIT 25
```

CloudTrail Esempi di interrogazioni per i dati

AWS CloudTrail tiene traccia dell'attività degli utenti e dell'utilizzo delle API in Servizi AWS. Gli abbonati possono interrogare CloudTrail i dati per conoscere i seguenti tipi di informazioni:

Ecco alcuni esempi di interrogazioni di CloudTrail dati:

Tentativi non autorizzati Servizi AWS negli ultimi 7 giorni

```
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
```

Elenco di tutte le CloudTrail attività effettuate dall'IP di origine **192.0.2.1** negli ultimi 7 giorni

```
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
```

Elenco di tutte le attività IAM negli ultimi 7 giorni

```
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
```

Istanze in cui la credenziale **AIDACKCEVSQ6C2EXAMPLE** è stata utilizzata negli ultimi 7 giorni

```
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
```

Elenco dei CloudTrail record non riusciti negli ultimi 7 giorni

```
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
```

Query di esempio per i log delle query del resolver Route 53

I log delle query resolver di Amazon Route 53 tengono traccia delle query DNS effettuate dalle risorse all'interno del tuo Amazon VPC. Gli abbonati possono interrogare i log delle query del resolver Route 53 per conoscere i seguenti tipi di informazioni:

Elenco delle query DNS degli ultimi 7 giorni CloudTrail

```
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
```

Elenco delle query DNS corrispondenti **`s3.amazonaws.com`** negli ultimi 7 giorni

```
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
```

Elenco di query DNS che non sono state risolte negli ultimi 7 giorni

```
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
```

Elenco delle query DNS risolte **`192.0.2.1`** negli ultimi 7 giorni

```
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
```

Domande di esempio per i risultati del Security Hub

Security Hub ti offre una visione completa dello stato di sicurezza AWS e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Security Hub produce risultati per i controlli di sicurezza e riceve risultati da servizi di terze parti.

Ecco alcuni esempi di interrogazioni relative ai risultati del Security Hub:

Nuovi risultati con gravità maggiore o uguale **`MEDIUM`** a quella degli ultimi 7 giorni

```
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
```

Risultati duplicati negli ultimi 7 giorni

```
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
```

Tutti i risultati non informativi degli ultimi 7 giorni

```
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
```

Risultati in cui la risorsa è un bucket Amazon S3 (nessuna limitazione di 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 = 'AwsS3Bucket')
LIMIT 25
```

I risultati ottenuti con un Common Vulnerability Scoring System (CVSS) hanno ottenuto un punteggio superiore a (nessuna limitazione di tempo) **1**

```
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
```

Risultati che corrispondono a Common Vulnerabilities and Exposures (CVE) (nessuna limitazione di tempo) **`CVE-0000-0000`**

```
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
```

Numero di prodotti che hanno inviato risultati da Security Hub negli ultimi 7 giorni

```
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
```

Numero di tipi di risorse nei risultati degli ultimi 7 giorni

```
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
```

Pacchetti vulnerabili in base ai risultati degli ultimi 7 giorni

```
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
```

Risultati che sono cambiati negli ultimi 7 giorni

```
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
```

Query di esempio per Amazon VPC Flow Logs

Amazon Virtual Private Cloud (Amazon VPC) fornisce dettagli sul traffico IP da e verso le interfacce di rete nel tuo VPC.

Ecco alcuni esempi di query di Amazon VPC Flow Logs:

Traffico specifico Regioni AWS negli ultimi 7 giorni

```
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
```

Elenco delle attività dall'IP di origine **`192.0.2.1`** e dalla porta di origine **22** negli ultimi 7 giorni

```
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
```

Numero di indirizzi IP di destinazione distinti negli ultimi 7 giorni

```
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
```

Traffico proveniente da 198.51.100.0/24 negli ultimi 7 giorni

```
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
```

Tutto il traffico HTTPS negli ultimi 7 giorni

```
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
```

Ordina per numero di pacchetti per le connessioni destinate alla porta **443** negli ultimi 7 giorni

```
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
```

Tutto il traffico tra IP **192.0.2.1** e **192.0.2.2** negli ultimi 7 giorni

```
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
```

Tutto il traffico in entrata negli ultimi 7 giorni

```
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
```

Tutto il traffico in uscita negli ultimi 7 giorni

```
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
```

Tutto il traffico rifiutato negli ultimi 7 giorni

```
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
```

Query di esempio per Amazon EKS

I log di Amazon EKS tracciano l'attività del piano di controllo fornisce log di audit e diagnostica direttamente dal piano di controllo di Amazon CloudWatch EKS ai log del tuo account. Questi log semplificano la protezione e la gestione dei cluster. Gli abbonati possono interrogare i log EKS per conoscere i seguenti tipi di informazioni:

Ecco alcuni esempi di interrogazioni relative ai registri EKS:

Richieste a un URL specifico negli ultimi 7 giorni

```
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
```

Richieste di aggiornamento provenienti da '10.0.97.167' negli ultimi 7 giorni

```
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
```

Richieste e risposte associate alla risorsa 'kube-controller-manager' negli ultimi 7 giorni

```
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
```

Gestione del ciclo di vita in Security Lake

Puoi personalizzare Security Lake per archiviare i dati nella tua cartella preferita Regioni AWS per il periodo di tempo che preferisci. La gestione del ciclo di vita può aiutarti a rispettare diversi requisiti di conformità.

Gestione della conservazione

Per gestire i dati in modo che vengano archiviati a costi contenuti, puoi configurare le impostazioni di conservazione dei dati. Poiché Security Lake archivia i dati come oggetti nei bucket Amazon Simple Storage Service (Amazon S3), le impostazioni di conservazione corrispondono a una configurazione del ciclo di vita di Amazon S3. Configurando queste impostazioni, puoi specificare la tua classe di storage Amazon S3 preferita e il periodo di tempo in cui gli oggetti S3 devono rimanere in quella classe di storage prima che passino a una classe di storage diversa o scadano. Per ulteriori informazioni sulle configurazioni del ciclo di vita di Amazon S3, consulta Managing your storage lifecycle nella Amazon Simple Storage Service User Guide.

In Security Lake, specifichi le impostazioni di conservazione a livello di regione. Ad esempio, puoi scegliere di trasferire tutti gli oggetti S3 in uno specifico Regione AWS alla classe di storage S3 Standard-IA 30 giorni dopo la loro scrittura nel data lake. La classe di storage predefinita di Amazon S3 è S3 Standard.

> **Important**
>
> Security Lake non supporta Amazon S3 Object Lock. Quando vengono creati i bucket di data lake, S3 Object Lock è disabilitato per impostazione predefinita. L'abilitazione di S3 Object Lock con la modalità di conservazione predefinita interrompe la consegna dei dati di registro normalizzati al data lake.

Configurazione delle impostazioni di conservazione quando si abilita Security Lake

Segui queste istruzioni per configurare le impostazioni di conservazione per una o più regioni durante l'onboarding su Security Lake. Se non configuri le impostazioni di conservazione, Security Lake utilizza le impostazioni predefinite per una configurazione del ciclo di vita di Amazon S3: archivia i dati a tempo indeterminato utilizzando la classe di storage S3 Standard.

Console

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Quando raggiungi la Fase 2: Definisci l'obiettivo del flusso di lavoro di onboarding, scegli Aggiungi transizione in Seleziona classi di archiviazione. Quindi scegli la classe di storage Amazon S3 a cui desideri trasferire gli oggetti S3. (La classe di storage predefinita non in elenco è S3 Standard.) Specificate anche un periodo di conservazione (in giorni) per quella classe di archiviazione. Per trasferire gli oggetti in un'altra classe di archiviazione dopo tale periodo, scegli Aggiungi transizione e inserisci le impostazioni per la classe di archiviazione e il periodo di conservazione successivi.
3. Per specificare quando vuoi che gli oggetti S3 scadano, scegli Aggiungi transizione. Quindi, per la classe di archiviazione, scegli Scadenza. Per il periodo di conservazione, inserisci il numero totale di giorni in cui desideri archiviare gli oggetti in Amazon S3, utilizzando qualsiasi classe di storage, dopo la creazione degli oggetti. Al termine di questo periodo di tempo, gli oggetti scadono e Amazon S3 li elimina.
4. Al termine, selezionare Next (Avanti).

Le modifiche verranno applicate a tutte le regioni in cui hai abilitato Security Lake durante le precedenti fasi di onboarding.

API

Per configurare le impostazioni di conservazione in modo programmatico durante l'onboarding su Security Lake, utilizza il CreateDataLakefunzionamento dell'API Security Lake. Se stai usando, esegui il comando AWS CLI. create-data-lake Specificate le impostazioni di conservazione desiderate nei `lifecycleConfiguration` parametri come segue:

- Per`transitions`, specifica il numero totale di giorni (`days`) in cui desideri archiviare gli oggetti S3 in una particolare classe `storageClass` di storage Amazon S3 ().
- Per`expiration`, specifica il numero totale di giorni in cui desideri archiviare gli oggetti in Amazon S3, utilizzando qualsiasi classe di storage, dopo la creazione degli oggetti. Al termine di questo periodo di tempo, gli oggetti scadono e Amazon S3 li elimina.

Security Lake applica le impostazioni alla regione specificata nel `region` campo dell'oggetto. `configurations`

Ad esempio, il comando seguente abilita Security Lake nella `us-east-1` regione. In questa regione, gli oggetti scadono dopo 365 giorni e gli oggetti passano alla classe di storage `ONEZONE_IA` S3 dopo 60 giorni. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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"
```

Aggiornamento delle impostazioni di conservazione

Segui queste istruzioni per aggiornare le impostazioni di conservazione per una o più regioni dopo aver abilitato Security Lake.

Console

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, scegli Regioni
3. Seleziona una regione, quindi scegli Modifica.
4. Nella sezione Seleziona le classi di archiviazione, inserisci le impostazioni desiderate. Per la classe di storage, scegli la classe di storage Amazon S3 a cui vuoi trasferire gli oggetti S3. (La classe di storage predefinita non in elenco è S3 Standard.) Per il periodo di conservazione, inserisci il numero di giorni in cui desideri archiviare gli oggetti in quella classe di archiviazione. È possibile specificare più transizioni.

   Per specificare anche quando vuoi che gli oggetti S3 scadano, scegli Scadenza per la classe di archiviazione. Quindi, per il periodo di conservazione, inserisci il numero totale di giorni in cui desideri archiviare gli oggetti in Amazon S3, utilizzando qualsiasi classe di storage, dopo la creazione degli oggetti. Al termine di questo periodo di tempo, gli oggetti scadono e Amazon S3 li elimina.
5. Al termine, scegli Salva.

API

Per aggiornare le impostazioni di conservazione a livello di codice, utilizza il UpdateDataLakefunzionamento dell'API Security Lake. Se utilizzi la, esegui il comando. AWS CLIupdate-data-lake Nella richiesta, utilizzate il `lifecycleConfiguration` parametro per specificare le nuove impostazioni:

- Per modificare le impostazioni di transizione, utilizza i `transitions` parametri per specificare ogni nuovo periodo di tempo in giorni (`days`) in cui desideri archiviare gli oggetti S3 in una particolare classe `storageClass` di storage Amazon S3 ().
- Per modificare il periodo di conservazione complessivo, utilizza il `expiration` parametro per specificare il numero totale di giorni in cui desideri archiviare gli oggetti S3, utilizzando qualsiasi classe di storage, dopo la creazione degli oggetti. Al termine di questo periodo di conservazione, gli oggetti scadono e Amazon S3 li elimina.

Security Lake applica le impostazioni alla regione specificata nel `region` campo dell'oggetto. `configurations`

Ad esempio, il AWS CLI comando seguente aggiorna le impostazioni di scadenza dei dati e le impostazioni di transizione di archiviazione per la `us-east-1` regione. In questa regione, gli oggetti scadono dopo 500 giorni e gli oggetti passano alla classe di storage `ONEZONE_IA` S3 dopo 30 giorni. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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"
```

Regioni di rollup

Una regione cumulativa consolida i dati di una o più regioni contributori. Questo può aiutarti a rispettare i requisiti regionali di conformità dei dati.

Per istruzioni sulla configurazione delle regioni di rollup, consulta. Configurazione delle regioni di rollup

Open Cybersecurity Schema Framework (OCSF)

Che cos'è OCSF?

L'Open Cybersecurity Schema Framework (OCSF) è uno sforzo collaborativo AWS e open source di partner leader nel settore della sicurezza informatica. OCSF fornisce uno schema standard per gli eventi di sicurezza più comuni, definisce i criteri di controllo delle versioni per facilitare l'evoluzione dello schema e include un processo di autogoverno per produttori e consumatori di registri di sicurezza. Il codice sorgente pubblico per OCSF è ospitato su. GitHub

Security Lake converte automaticamente i log e gli eventi che provengono dallo schema supportato nativamente Servizi AWS allo schema OCSF. Dopo la conversione in OCSF, Security Lake archivia i dati in un bucket Amazon Simple Storage Service (Amazon S3) (un bucket per) nel tuo. Regione AWS Account AWS I log e gli eventi scritti su Security Lake da fonti personalizzate devono rispettare lo schema OCSF e il formato Apache Parquet. Gli abbonati possono trattare i log e gli eventi come record Parquet generici o applicare la classe di eventi dello schema OCSF per interpretare più accuratamente le informazioni contenute in un record.

Classi di eventi OCSF

I log e gli eventi di una determinata origine di Security Lake corrispondono a una classe di eventi specifica definita in OCSF. L'attività DNS, l'attività SSH e l'autenticazione sono esempi di classi di eventi in OCSF. È possibile specificare a quale classe di eventi corrisponde una particolare fonte.

Identificazione della fonte OCSF

OCSF utilizza una varietà di campi per aiutarti a determinare da dove ha avuto origine uno specifico set di log o eventi. Questi sono i valori dei campi pertinenti Servizi AWS che sono supportati nativamente come sorgenti in Security Lake.

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

Origine	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	nome_classe	metadati.versione
CloudTrail Eventi relativi ai dati Lambda	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail Eventi di gestione	CloudTrail	AWS	Management	API Activity, Authentication o Account Change	1.0.0-rc.2
CloudTrail Eventi relativi ai dati S3	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.0.0-rc.2
Security Hub	Security Hub	AWS	Corrisponde al ProductName valore del Security Hub	Security Finding	1.0.0-rc.2
Log di flusso 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.

Origine	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	nome_classe	metadati.versione
CloudTrail Eventi relativi ai dati Lambda	`CloudTrail`	`AWS`	`Data`	`API Activity`	`1.1.0`
CloudTrail Eventi di gestione	`CloudTrail`	`AWS`	`Management`	`API Activity, Authentication o Account Change`	`1.1.0`
CloudTrail Eventi relativi ai dati S3	`CloudTrail`	`AWS`	`Data`	`API Activity`	`1.1.0`
Route 53	`Route 53`	`AWS`	`Resolver Query Logs`	`DNS Activity`	`1.1.0`
Security Hub	Corrisponde al valore del AWS Security Finding Format (ASFF) `ProductName`	Corrisponde al valore del AWS Security Finding Format (ASFF) `CompanyName`	Corrisponde `featureName` al valore di ASFF `ProductFields`	`Vulnerability Finding, Compliance Finding, or Detection Finding`	`1.1.0`
Log di flusso VPC	`Amazon VPC`	`AWS`	`Flowlogs`	`Network Activity`	`1.1.0`

Origine	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	nome_classe	metadati.versione
Registri di controllo EKS	`Amazon EKS`	`AWS`	`Elastic Kubernetes Service`	`API Activity`	`1.1.0`

Integrazioni con Security Lake

Amazon Security Lake si integra con altri prodotti Servizi AWS e di terze parti. Le integrazioni possono inviare dati a Security Lake come fonte o consumare dati in Security Lake come abbonato. I seguenti argomenti spiegano quali prodotti Servizi AWS e quelli di terze parti si integrano con Security Lake.

Argomenti

Servizio AWS integrazioni con Security Lake

Amazon Security Lake si integra con altri Servizi AWS. Un servizio può funzionare come integrazione del codice sorgente, integrazione degli abbonati o entrambe le opzioni.

Le integrazioni di origine hanno le seguenti proprietà:

- Invia dati a Security Lake
- I dati arrivano in formato Apache Parquet
- I dati arrivano nello schema Open Cybersecurity Schema Framework (OCSF)

Le integrazioni degli abbonati hanno le seguenti proprietà:

- Leggi i dati di origine da Security Lake su un endpoint HTTPS o una coda Amazon Simple Queue Service (Amazon SQS) o interrogando direttamente i dati di origine da AWS Lake Formation
- In grado di leggere i dati in formato Apache Parquet (Security Lake lo gestisce automaticamente per Security Hub e altre fonti supportate nativamente)
- In grado di leggere i dati nello schema OCSF (Security Lake lo gestisce automaticamente per Security Hub e altre fonti supportate nativamente)

La sezione seguente spiega con cosa si integra Servizi AWS Security Lake e come funziona ciascuna integrazione.

Integrazione con AWS AppFabric

Tipo di integrazione: Source

AWS AppFabricè un servizio senza codice che collega le applicazioni SaaS (Software as a Service) in tutta l'organizzazione, in modo che i team IT e di sicurezza possano gestire e proteggere le applicazioni utilizzando uno schema standard e un archivio centrale.

In che modo Security Lake riceve i risultati AppFabric

Puoi inviare i dati dei log di AppFabric controllo a Security Lake selezionando Amazon Kinesis Data Firehose come destinazione e configurando Kinesis Data Firehose per fornire dati nello schema OCSF e in formato Apache Parquet a Security Lake.

Prerequisiti

Prima di poter inviare i log di AppFabric controllo a Security Lake, è necessario inviare i log di controllo normalizzati OCSF a un flusso Kinesis Data Firehose. Puoi quindi configurare Kinesis Data Firehose per inviare l'output al tuo bucket Security Lake Amazon S3. Per ulteriori informazioni, consulta Scegli Amazon S3 come destinazione nella Amazon Kinesis Developer Guide.

Invia i AppFabric risultati a Security Lake

Per inviare i log di AppFabric controllo a Security Lake dopo aver completato il prerequisito precedente, è necessario abilitare entrambi i servizi e aggiungerli AppFabric come origine personalizzata in Security Lake. Per istruzioni sull'aggiunta di una fonte personalizzata, vedere. Raccolta di dati da fonti personalizzate

Smetti di ricevere AppFabric i log in Security Lake

Per interrompere la ricezione AppFabric dei registri di controllo, è possibile utilizzare la console di Security Lake, l'API Security Lake o AWS CLI eliminarli AppFabric come origine personalizzata. Per istruzioni, consulta Eliminazione di una fonte personalizzata.

Integrazione con AWS Security Hub

Tipo di integrazione: Source

AWS Security Huboffre una visione completa dello stato di sicurezza AWS e consente di verificare la conformità dell'ambiente agli standard e alle best practice del settore della sicurezza. Security

Hub raccoglie dati sulla sicurezza da tutti Account AWS i servizi e dai prodotti partner di terze parti supportati e ti aiuta ad analizzare le tendenze della sicurezza e identificare i problemi di sicurezza con la massima priorità.

Quando integri Amazon Security Lake e Security Hub, ricevi i risultati di Security Hub in Security Lake. I risultati di Security Hub diventano una fonte a cui gli abbonati a Security Lake possono attingere, aiutandoti ad analizzare il tuo livello di sicurezza.

In che modo Security Lake riceve i risultati del Security Hub

Nella Centrale di sicurezza, i problemi di sicurezza vengono monitorati come esiti. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub dispone anche di una serie di regole chiamate controlli che utilizza per rilevare problemi di sicurezza e generare risultati.

Tutti i risultati in Security Hub utilizzano un formato JSON standard denominato AWS Security Finding Format (ASFF).

Security Lake riceve i risultati del Security Hub e li trasforma in. Open Cybersecurity Schema Framework (OCSF)

Prerequisiti

Quando si abilita Security Hub e si aggiungono i risultati di Security Hub come origine in Security Lake, Security Hub inizia a inviare nuovi risultati e aggiornamenti ai risultati esistenti a Security Lake.

Se desideri che Security Hub generi i risultati del controllo e li invii a Security Lake, devi abilitare gli standard di sicurezza pertinenti e attivare la registrazione delle risorse su base regionale in AWS Config. Per ulteriori informazioni, vedere Abilitazione e configurazione AWS Config nella Guida per l'AWS Security Hub utente.

Invia i risultati del Security Hub a Security Lake

Per inviare i risultati di Security Hub a Security Lake, è necessario abilitare entrambi i servizi e aggiungere i risultati di Security Hub come fonte in Security Lake. Per istruzioni sull'aggiunta di una AWS fonte, vedereAggiungere un file Servizio AWS come fonte.

Smetti di ricevere i risultati del Security Hub in Security Lake

Per interrompere la ricezione dei risultati di Security Hub, puoi utilizzare la console Security Hub, l'API Security Hub o AWS CLI.

Consulta Disabilitazione e abilitazione del flusso di risultati da un'integrazione (console) o Disabilitazione del flusso di risultati da un'integrazione (API Security Hub, AWS CLI) nella Guida per l'utente.AWS Security Hub

Integrazioni di terze parti con Security Lake

Amazon Security Lake si integra con diversi provider di terze parti. Un provider può offrire un'integrazione del codice sorgente, un'integrazione con gli abbonati o un'integrazione di servizi. I provider possono offrire uno o più tipi di integrazione.

Le integrazioni di origine hanno le seguenti proprietà:

- Invia dati a Security Lake
- I dati arrivano in formato Apache Parquet
- I dati arrivano nello schema Open Cybersecurity Schema Framework (OCSF)

Le integrazioni degli abbonati hanno le seguenti proprietà:

- Leggi i dati di origine da Security Lake su un endpoint HTTPS o una coda Amazon Simple Queue Service (Amazon SQS) o interrogando direttamente i dati di origine da AWS Lake Formation
- In grado di leggere i dati in formato Apache Parquet
- In grado di leggere i dati nello schema OCSF

Le integrazioni di servizi possono aiutarti a implementare Security Lake e altro Servizi AWS nella tua organizzazione. Possono anche fornire assistenza per la reportistica, l'analisi e altri casi d'uso.

Per cercare un fornitore partner specifico, consulta il Partner Solutions Finder. Per acquistare un prodotto di terze parti, consulta AWS Marketplace.

Per richiedere di essere aggiunto come partner di integrazione o diventare partner di Security Lake, invia un'email a <securitylake-partners@amazon.com>.

Se utilizzi integrazioni di terze parti che inviano i risultati a AWS Security Hub, puoi anche esaminarli in Security Lake se l'integrazione del Security Hub per Security Lake è abilitata. Per istruzioni su come abilitare l'integrazione, consultaIntegrazione con AWS Security Hub. Per un elenco delle integrazioni di terze parti che inviano i risultati a Security Hub, consulta Integrazioni di prodotti di partner di terze parti disponibili nella Guida per l'AWS Security Hub utente.

Prima di configurare gli abbonati, verifica il supporto dei log OCSF dell'abbonato. Per i dettagli più recenti, consulta la documentazione del tuo abbonato.

Accenture – MxDR

Tipo di integrazione: abbonato, servizio

Accenture'sL'integrazione di MxDR con Security Lake offre l'inserimento di dati in tempo reale di log ed eventi, il rilevamento gestito delle anomalie, la ricerca delle minacce e le operazioni di sicurezza. Ciò facilita l'analisi e il rilevamento e la risposta gestiti (MDR).

Come integrazione dei servizi, Accenture può anche aiutarti a implementare Security Lake nella tua organizzazione.

Documentazione sull'integrazione

Aqua Security

Tipo di integrazione: fonte

Aqua Securitypuò essere aggiunto come fonte personalizzata per inviare eventi di controllo a Security Lake. Gli eventi di controllo vengono convertiti nello schema OCSF e nel formato Parquet.

Documentazione sull'integrazione

Barracuda – Email Protection

Tipo di integrazione: fonte

Barracuda Email Protectionpuò inviare eventi a Security Lake quando vengono rilevati nuovi attacchi e-mail di phishing. Puoi ricevere questi eventi insieme ad altri dati di sicurezza nel tuo data lake.

Documentazione sull'integrazione

Booz Allen Hamilton

Tipo di integrazione: Servizio

Come integrazione di servizi, Booz Allen Hamilton utilizza un approccio alla sicurezza informatica basato sui dati fondendo dati e analisi con il servizio Security Lake.

Link per i partner

ChaosSearch

Tipo di integrazione: abbonato

ChaosSearchoffre l'accesso ai dati multimodello agli utenti con API aperte come Elasticsearch e SQL o con le interfacce utente Kibana e Superset incluse in modo nativo. È possibile utilizzare i dati di Security Lake ChaosSearch senza limiti di conservazione per monitorare, avvisare e individuare le minacce. Questo ti aiuta ad affrontare gli ambienti di sicurezza complessi e le minacce persistenti di oggi.

Documentazione sull'integrazione

Cisco Security – Secure Firewall

Tipo di integrazione: fonte

Grazie all'integrazione Cisco Secure Firewall con Security Lake, è possibile archiviare i log del firewall in modo strutturato e scalabile. Il client enCore di Cisco trasmette i log del firewall dal Firewall Management Center, esegue la conversione dello schema in schema OCSF e li archivia in Security Lake.

Documentazione sull'integrazione

Claroty – xDome

Tipo di integrazione: fonte

Claroty xDomeinvia gli avvisi rilevati all'interno delle reti a Security Lake con una configurazione minima. Le opzioni di implementazione flessibili e rapide aiutano a xDome proteggere gli asset Internet of Things (XIoT) estesi, costituiti da risorse IoT, IIoT e BMS, all'interno della rete, rilevando automaticamente i primi indicatori di minaccia.

Documentazione sull'integrazione

CMD Solutions

Tipo di integrazione: Servizio

CMD Solutionsaiuta le aziende ad aumentare la loro agilità integrando la sicurezza in modo tempestivo e continuo attraverso processi di progettazione, automazione e garanzia continua.

Come integrazione dei servizi, CMD Solutions può aiutarti a implementare Security Lake nella tua organizzazione.

Link al partner

Confluent – Amazon S3 Sink Connector

Tipo di integrazione: fonte

Confluentconnette, configura e orchestra automaticamente le integrazioni di dati con connettori predefiniti e completamente gestiti. Confluent S3 Sink ConnectorConsente di prelevare dati grezzi e inserirli in Security Lake su larga scala in formato parquet nativo.

Documentazione sull'integrazione

Contrast Security

Tipo di integrazione: fonte

Prodotto partner per l'integrazione: Contrast Assess

Contrast Security Assessè uno strumento IAST che offre il rilevamento delle vulnerabilità in tempo reale in app Web, API e microservizi. Assess si integra con Security Lake per aiutarti a fornire visibilità centralizzata per tutti i carichi di lavoro.

Documentazione sull'integrazione

Cribl – Search

Tipo di integrazione: abbonato

È possibile utilizzarlo Cribl Search per cercare i dati di Security Lake.

Documentazione sull'integrazione

Cribl – Stream

Tipo di integrazione: fonte

È possibile utilizzare Cribl Stream per inviare dati da qualsiasi fonte di terze parti Cribl supportata a Security Lake nello schema OCSF.

Documentazione di integrazione

CrowdStrike – Falcon Data Replicator

Tipo di integrazione: fonte

Questa integrazione estrae i dati da un CrowdStrike Falcon Data Replicator sistema di streaming continuo, li trasforma in uno schema OCSF e li invia a Security Lake.

Documentazione sull'integrazione

CyberArk – Unified Identify Security Platform

Tipo di integrazione: fonte

CyberArk Audit Adapter, una AWS Lambda funzione, raccoglie gli eventi di sicurezza CyberArk Identity Security Platform e invia i dati a Security Lake nello schema OCSF.

Documentazione di integrazione

Darktrace – Cyber AI Loop

Tipo di integrazione: fonte

L'Darktraceintegrazione con Security Lake apporta la potenza dell'Darktraceautoapprendimento a Security Lake. Le informazioni provenienti da Cyber AI Loop possono essere correlate ad altri flussi di dati ed elementi dello stack di sicurezza dell'organizzazione. L'integrazione registra le violazioni del Darktrace modello come rilevazioni di sicurezza.

Documentazione sull'integrazione (accedi al Darktrace portale per consultare la documentazione)

Datadog

Tipo di integrazione: Abbonato

Datadog Cloud SIEMrileva le minacce in tempo reale al tuo ambiente cloud, inclusi i dati in Security Lake, e unifica DevOps i team di sicurezza in un'unica piattaforma.

Documentazione sull'integrazione

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

Tipo di integrazione: abbonato, servizio

Deloitte MXDR CAEconsente di archiviare, analizzare e visualizzare rapidamente i dati di sicurezza standardizzati. La suite CAE di funzionalità analitiche, AI e ML personalizzate fornisce automaticamente informazioni utili basate su modelli eseguiti sui dati in formato OCSF di Security Lake.

Come integrazione di servizi, Deloitte può anche aiutarti a implementare Security Lake nella tua organizzazione.

Documentazione sull'integrazione

Devo

Tipo di integrazione: abbonato

Il Devo raccoglitore di AWS supporti per l'importazione da Security Lake. Questa integrazione può aiutarti ad analizzare e affrontare una varietà di casi d'uso della sicurezza, come il rilevamento delle minacce, le indagini e la risposta agli incidenti.

Documentazione sull'integrazione

DXC – SecMon

Tipo di integrazione: abbonato, servizio

DXC SecMonraccoglie gli eventi di sicurezza da Security Lake e li monitora per rilevare e segnalare potenziali minacce alla sicurezza. Questo aiuta le organizzazioni a comprendere meglio il loro livello di sicurezza e a identificare e rispondere in modo proattivo alle minacce.

Come integrazione dei servizi, DXC può anche aiutarti a implementare Security Lake nella tua organizzazione.

Documentazione sull'integrazione

Eviden— AIsaac (in precedenzaAtos)

Tipo di integrazione: abbonato

La AIsaac MDR piattaforma utilizza i log di flusso VPC inseriti nello schema OCSF in Security Lake e utilizza modelli di intelligenza artificiale per rilevare le minacce.

Documentazione sull'integrazione

ExtraHop – Reveal(x) 360

Tipo di integrazione: fonte

È possibile migliorare la sicurezza del carico di lavoro e delle applicazioni integrando i dati di rete, compresi i rilevamenti di IOCExtraHop Reveal(x) 360, da e verso Security Lake nello schema OCSF

Documentazione sull'integrazione

Falcosidekick

Tipo di integrazione: fonte

Falcosidekickraccoglie e invia gli eventi Falco a Security Lake. Questa integrazione esporta gli eventi di sicurezza utilizzando lo schema OCSF.

Documentazione di integrazione

Gigamon – Application Metadata Intelligence

Tipo di integrazione: fonte

Gigamon Application Metadata Intelligence (AMI)potenzia gli strumenti di monitoraggio dell'osservabilità, del SIEM e delle prestazioni di rete con attributi critici dei metadati. Ciò consente di fornire una visibilità più approfondita delle applicazioni in modo da individuare i punti deboli delle prestazioni, i problemi di qualità e i potenziali rischi per la sicurezza della rete.

Documentazione sull'integrazione

Hoop Cyber

Tipo di integrazione: Servizio

Hoop Cyber FastStartinclude una valutazione delle fonti di dati, l'assegnazione delle priorità e l'onboarding delle fonti di dati e aiuta i clienti a interrogare i propri dati con gli strumenti e le integrazioni esistenti offerti tramite Security Lake.

Link per i partner

IBM – QRadar

Tipo di integrazione: abbonato

IBM Security QRadar SIEM with UAXintegra Security Lake con una piattaforma di analisi che identifica e previene le minacce nei cloud ibridi. Questa integrazione supporta sia l'accesso ai dati che l'accesso alle query.

Documentazione di integrazione sull'utilizzo dei AWS CloudTrail log

Documentazione di integrazione sull'uso di Amazon Athena per le query

Infosys

Tipo di integrazione: Servizio

Infosysti aiuta a personalizzare l'implementazione di Security Lake in base alle tue esigenze organizzative e fornisce informazioni personalizzate.

Link al partner

Insbuilt

Tipo di integrazione: Servizio

Insbuiltè specializzato in servizi di consulenza cloud e può aiutarti a capire come implementare Security Lake nella tua organizzazione.

Link per i partner

Kyndryl – AIOps

Tipo di integrazione: abbonato, servizio

Kyndrylsi integra con Security Lake per fornire l'interoperabilità dei dati informatici, dell'intelligence sulle minacce e dell'analisi basata sull'intelligenza artificiale. In qualità di abbonato all'accesso ai dati, Kyndryl acquisisce AWS CloudTrail Management Events da Security Lake per scopi di analisi.

Come integrazione di servizi, Kyndryl può anche aiutarti a implementare Security Lake nella tua organizzazione.

Documentazione sull'integrazione

Lacework – Polygraph

Tipo di integrazione: fonte

Lacework Polygraph® Data Platformsi integra con Security Lake come fonte di dati e fornisce risultati di sicurezza su vulnerabilità, configurazioni errate e minacce note e sconosciute in tutto l'ambiente. AWS

Documentazione sull'integrazione

Laminar

Tipo di integrazione: fonte

Laminarinvia gli eventi di sicurezza dei dati a Security Lake nello schema OCSF, rendendoli disponibili per ulteriori casi d'uso di analisi, come la risposta agli incidenti e le indagini.

Documentazione sull'integrazione

MegazoneCloud

Tipo di integrazione: Servizio

MegazoneCloudè specializzato in servizi di consulenza cloud e può aiutarti a capire come implementare Security Lake nella tua organizzazione. Colleghiamo Security Lake a soluzioni ISV integrate per creare attività personalizzate e creare approfondimenti personalizzati in base alle esigenze dei clienti.

Documentazione sull'integrazione

Monad

Tipo di integrazione: fonte

Monadtrasforma automaticamente i dati in uno schema OCSF e li invia al data lake Security Lake.

Documentazione sull'integrazione

NETSCOUT – Omnis Cyber Intelligence

Tipo di integrazione: fonte

Grazie all'integrazione con Security Lake, NETSCOUT diventa una fonte personalizzata di risultati di sicurezza e informazioni dettagliate sulla sicurezza su ciò che accade nella tua azienda, come le

minacce informatiche, i rischi per la sicurezza e le modifiche della superficie di attacco. Questi risultati vengono prodotti nell'account del cliente da NETSCOUT CyberStreams e Omnis Cyber Intelligence quindi inviati a Security Lake nello schema OCSF. I dati acquisiti soddisfano anche altri requisiti e best practice per una fonte Security Lake, tra cui formato, schema, partizionamento e aspetti relativi alle prestazioni.

Documentazione sull'integrazione

Netskope – CloudExchange

Tipo di integrazione: fonte

Netskopeti aiuta a rafforzare il tuo livello di sicurezza condividendo i log relativi alla sicurezza e le informazioni sulle minacce con Security Lake. Netskopei risultati vengono inviati a Security Lake con un CloudExchange plug-in, che può essere avviato come ambiente basato su docker all'interno AWS o in un data center locale.

Documentazione sull'integrazione

New Relic ONE

Tipo di integrazione: abbonato

New Relic ONEè un'applicazione per abbonati basata su Lambda. Viene distribuito nel tuo account, attivato da Amazon SQS e invia i dati New Relic utilizzando le chiavi di licenza New Relic

Documentazione sull'integrazione

Okta – Workforce Identity Cloud

Tipo di integrazione: fonte

Oktainvia i log di identità a Security Lake nello schema OCSF tramite un'integrazione Amazon. EventBridge Okta System Logslo schema in OCSF aiuterà i team di data scientist e addetti alla sicurezza a interrogare gli eventi di sicurezza utilizzando uno standard open source. La generazione di log OCSF standardizzati da Okta consente di eseguire attività di controllo e generare report relativi all'autenticazione, all'autorizzazione, alle modifiche dell'account e alle modifiche delle entità secondo uno schema coerente.

Documentazione sull'integrazione

[AWS CloudFormation modello da aggiungere Okta come fonte personalizzata in Security Lake]

Orca – Cloud Security Platform

Tipo di integrazione: fonte

La piattaforma di sicurezza cloud Orca agentless che AWS si integra con Security Lake inviando eventi Cloud Detection and Response (CDR) nello schema OCSF.

[Documentazione sull'integrazione (accedi al portale per consultare la Orca documentazione)]

Palo Alto Networks – Prisma Cloud

Tipo di integrazione: fonte

Palo Alto Networks Prisma Cloudaggrega i dati di rilevamento delle vulnerabilità tra le macchine virtuali negli ambienti nativi del cloud e li invia a Security Lake.
<Per abilitare l'integrazione, invia un'e-mail a securitylake-partners@amazon.co

[Documentazione sull'integrazione]

Ping Identity – PingOne

Tipo di integrazione: fonte

PingOneinvia avvisi di modifica dell'account a Security Lake nello schema OCSF e nel formato Parquet, consentendoti di scoprire e intervenire in base alle modifiche dell'account.

[Documentazione sull'integrazione]

PwC – Fusion center

Tipo di integrazione: abbonato, servizio

PwC offre conoscenze e competenze per aiutare i clienti a implementare un centro di fusione per soddisfare le loro esigenze individuali. Basato su Amazon Security Lake, un centro di fusione offre la possibilità di combinare dati provenienti da diverse fonti per creare una visione centralizzata e quasi in tempo reale.

[Documentazione sull'integrazione]

Rapid7 – InsightIDR

Tipo di integrazione: abbonato

InsightIDR, la soluzione Rapid7 SIEM/XDR, può inserire i log in Security Lake per il rilevamento delle minacce e l'indagine di attività sospette.

Documentazione sull'integrazione

RipJar – Labyrinth for Threat Investigations

Tipo di integrazione: abbonato

Labyrinth for Threat Investigationsoffre un approccio a livello aziendale all'esplorazione delle minacce su larga scala basato sulla fusione dei dati, con sicurezza granulare, flussi di lavoro adattabili e reportistica.

Documentazione sull'integrazione

Sailpoint

Tipo di integrazione: fonte

Prodotto partner per l'integrazione: SailPoint IdentityNow

Questa integrazione consente ai clienti di trasformare i dati degli eventi daSailPoint IdentityNow. L'integrazione ha lo scopo di fornire un processo automatizzato per portare le attività IdentityNow degli utenti e gli eventi di governance in Security Lake per migliorare le informazioni provenienti dai prodotti di monitoraggio degli incidenti di sicurezza e degli eventi.

Documentazione sull'integrazione

Securonix

Tipo di integrazione: abbonato

Securonix Next-Gen SIEMsi integra con Security Lake, consentendo ai team di sicurezza di inserire i dati più rapidamente e di espandere le proprie capacità di rilevamento e risposta.

Documentazione sull'integrazione

SentinelOne

Tipo di integrazione: abbonato

La SentinelOne Singularity™ XDR piattaforma estende il rilevamento e la risposta in tempo reale ai carichi di lavoro di endpoint, identità e cloud in esecuzione su infrastrutture locali e cloud pubbliche, tra cui Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Kubernetes Service (Amazon EKS).

Documentazione sull'integrazione (accedi al portale per consultare la documentazione) SentinelOne

Sentra – Data Lifecyle Security Platform

Tipo di integrazione: fonte

Dopo aver implementato l'infrastruttura di Sentra scansione nel tuo account, Sentra recupera i risultati e li inserisce nel tuo SaaS. Questi risultati sono metadati che vengono Sentra archiviati e successivamente trasmessi a Security Lake nello schema OCSF per l'esecuzione di interrogazioni.

Documentazione sull'integrazione

SOC Prime

Tipo di integrazione: abbonato

SOC Primesi integra con Security Lake tramite Amazon OpenSearch Service e Amazon Athena per facilitare l'orchestrazione intelligente dei dati e la caccia alle minacce sulla base di obiettivi Zero Trust. SOC Primeconsente ai team di sicurezza di aumentare la visibilità delle minacce e indagare sugli incidenti senza un volume eccessivo di avvisi. Puoi risparmiare tempo di sviluppo con regole e query riutilizzabili che sono automaticamente convertibili in Athena e OpenSearch Service nello schema OCSF.

Documentazione sull'integrazione

Splunk

Tipo di integrazione: abbonato

Il Splunk AWS componente aggiuntivo per Amazon Web Services (AWS) supporta l'importazione da Security Lake. Questa integrazione consente di accelerare il rilevamento, l'indagine e la risposta alle minacce sottoscrivendo i dati nello schema OCSF di Security Lake.

Documentazione sull'integrazione

Stellar Cyber

Tipo di integrazione: abbonato

Stellar Cyberutilizza i log di Security Lake e aggiunge i record al Stellar Cyber data lake. Questo connettore utilizza lo schema OCSF.

Documentazione di integrazione

Sumo Logic

Tipo di integrazione: abbonato

Sumo Logicutilizza i dati di Security Lake e offre un'ampia visibilità in ambienti cloud AWS ibridi e on-premise. Sumo Logic offre ai team di sicurezza visibilità, automazione e monitoraggio delle minacce completi su tutti i loro strumenti di sicurezza.

Documentazione sull'integrazione

Swimlane – Turbine

Tipo di integrazione: abbonato

Swimlaneinserisce i dati da Security Lake nello schema OCSF e li invia tramite playbook low-code e gestione dei casi per facilitare il rilevamento, l'indagine e la risposta agli incidenti più rapidi delle minacce.

Documentazione sull'integrazione (accedi al Swimlane portale per consultare la documentazione)

Sysdig Secure

Tipo di integrazione: fonte

Sysdig Secure'sLa piattaforma di protezione delle applicazioni native per il cloud (CNAPP) invia eventi di sicurezza a Security Lake per massimizzare la supervisione, semplificare le indagini e semplificare la conformità.

Documentazione sull'integrazione

Talon

Tipo di integrazione: fonte

Prodotto partner per l'integrazione: Talon Enterprise Browser

Talon's Enterprise Browser, un ambiente endpoint sicuro e isolato basato su browser, invia Talon Access, protezione dei dati, azioni SaaS ed eventi di sicurezza a Security Lake fornendo visibilità e opzioni per correlare in modo incrociato gli eventi per il rilevamento, l'analisi forense e le indagini.

Documentazione sull'integrazione (accedi al portale per consultare la documentazione) Talon

Tanium

Tipo di integrazione: fonte

Tanium Unified Cloud Endpoint Detection, Management, and SecurityLa piattaforma fornisce dati di inventario a Security Lake nello schema OCSF.

Documentazione sull'integrazione

TCS

Tipo di integrazione: Servizio

TCS AWS Business UnitOffre innovazione, esperienza e talento. Questa integrazione è alimentata da un decennio di creazione di valore congiunta, profonda conoscenza del settore, esperienza tecnologica e saggezza nella fornitura. Come integrazione dei servizi, TCS può aiutarti a implementare Security Lake nella tua organizzazione.

Documentazione sull'integrazione

Tego Cyber

Tipo di integrazione: abbonato

Tego Cybersi integra con Security Lake per aiutarti a rilevare e indagare rapidamente su potenziali minacce alla sicurezza. Correlando diversi indicatori di minaccia su ampi intervalli di tempo e fonti di registro, Tego Cyber scopre le minacce nascoste. La piattaforma è arricchita con informazioni sulle minacce altamente contestuali, che forniscono precisione e informazioni dettagliate nel rilevamento e nelle indagini sulle minacce.

Documentazione sull'integrazione

Tines – No-code security automation

Tipo di integrazione: abbonato

Tines No-code security automationti aiuta a prendere decisioni più accurate sfruttando i dati di sicurezza centralizzati in Security Lake.

Documentazione sull'integrazione

Torq – Enterprise Security Automation Platform

Tipo di integrazione: fonte, abbonato

Torqsi integra perfettamente con Security Lake sia come fonte personalizzata che come abbonato. Torqti aiuta a implementare l'automazione e l'orchestrazione su scala aziendale con una semplice piattaforma senza codice.

Documentazione sull'integrazione

Trellix – XDR

Tipo di integrazione: fonte, abbonato

Essendo una piattaforma XDR aperta, Trellix XDR supporta l'integrazione di Security Lake. Trellix XDRpuò sfruttare i dati nello schema OCSF per casi d'uso di analisi della sicurezza. Puoi anche ampliare il tuo data lake Security Lake con oltre 1.000 fonti di eventi di sicurezza. Trellix XDR Ciò consente di estendere le capacità di rilevamento e risposta per il proprio ambiente. AWS I dati acquisiti sono correlati ad altri rischi per la sicurezza e forniscono gli strumenti necessari per rispondere a un rischio in modo tempestivo.

Documentazione sull'integrazione

Trend Micro – CloudOne

Tipo di integrazione: fonte

Trend Micro CloudOne Workload Securityinvia le seguenti informazioni a Security Lake dalle tue istanze Amazon Elastic Compute Cloud (EC2):

- attività di interrogazione DNS

- Attività sui file
- Attività di rete
- Attività di processo
- Attività di Registry Value
- Attività dell'account utente

Documentazione sull'integrazione

Uptycs – Uptycs XDR

Tipo di integrazione: fonte

Uptycsinvia una grande quantità di dati nello schema OCSF da risorse locali e cloud a Security Lake. I dati includono rilevamenti di minacce comportamentali da endpoint e carichi di lavoro cloud, rilevamenti di anomalie, violazioni delle policy, policy rischiose, configurazioni errate e vulnerabilità.

Documentazione sull'integrazione

Vectra AI – Vectra Detect for AWS

Tipo di integrazione: fonte

UtilizzandoVectra Detect for AWS, puoi inviare avvisi ad alta fedeltà a Security Lake come fonte personalizzata utilizzando un modello dedicato. AWS CloudFormation

Documentazione sull'integrazione

VMware Aria Automation for Secure Clouds

Tipo di integrazione: fonte

Con questa integrazione, puoi rilevare le configurazioni errate del cloud e inviarle a Security Lake per un'analisi avanzata.

Documentazione sull'integrazione

Wazuh

Tipo di integrazione: abbonato

Wazuhmira a gestire in modo sicuro i dati degli utenti, fornire l'accesso alle query per ogni fonte e ottimizzare i costi di interrogazione.

Documentazione sull'integrazione

Wipro

Tipo di integrazione: fonte, servizio

Questa integrazione consente di raccogliere dati dalla Wipro Cloud Application Risk Governance (CARG) piattaforma per fornire una visione unificata delle applicazioni cloud e delle posizioni di conformità in tutta l'azienda.

Come integrazione di servizi, Wipro può anche aiutarti a implementare Security Lake nella tua organizzazione.

Documentazione sull'integrazione

Wiz – CNAPP

Tipo di integrazione: fonte

L'integrazione tra Wiz e Security Lake facilita la raccolta dei dati di sicurezza del cloud in un unico data lake di sicurezza sfruttando lo schema OCSF, uno standard open source progettato per lo scambio di dati di sicurezza estensibile e normalizzato.

Documentazione sull'integrazione (accedi al portale per consultare la Wiz documentazione)

Zscaler – Zscaler Posture Control

Tipo di integrazione: fonte

Zscaler Posture Control™, una piattaforma di protezione delle applicazioni nativa per il cloud, invia i risultati di sicurezza a Security Lake nello schema OCSF.

Documentazione sull'integrazione

Sicurezza in Amazon Security Lake

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il modello di responsabilità condivisa fa riferimento ad una sicurezza del cloud e nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS in Cloud AWS. AWS fornisce inoltre i servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon Security Lake, consulta AWSServices in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, le leggi e le normative applicabili.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Security Lake. I seguenti argomenti mostrano come configurare Security Lake per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di Security Lake.

Argomenti

Gestione delle identità e degli accessi per Amazon Security Lake

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Security Lake. IAM è un Servizio AWS software che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Security Lake.

Utente del servizio: se utilizzi il servizio Security Lake per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Security Lake per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Security Lake, vediRisoluzione dei problemi relativi all'identità e all'accesso ad Amazon Security Lake.

Amministratore del servizio: se sei responsabile delle risorse di Security Lake della tua azienda, probabilmente hai pieno accesso a Security Lake. Spetta a te determinare a quali funzionalità e risorse di Security Lake devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Security Lake, consultaCome funziona Amazon Security Lake con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a Security Lake. Per visualizzare esempi di policy basate sull'identità di Security Lake che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon Security Lake

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWSaccesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane.

Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
- Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La

maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire

da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Security Lake con IAM

Prima di utilizzare IAM per gestire l'accesso a Security Lake, scopri quali funzionalità IAM sono disponibili per l'uso con Security Lake.

Funzionalità IAM che puoi utilizzare con Amazon Security Lake

Funzionalità IAM	Supporto per Security Lake
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Security Lake e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Security Lake

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Security Lake supporta politiche basate sull'identità. Per ulteriori informazioni, consulta Esempi di policy basate sull'identità per Amazon Security Lake.

Politiche basate sulle risorse all'interno di Security Lake

Supporta le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Il servizio Security Lake crea policy basate sulle risorse per i bucket Amazon S3 che archiviano i tuoi dati. Non colleghi queste politiche basate sulle risorse ai tuoi bucket S3. Security Lake crea automaticamente queste politiche per tuo conto.

Una risorsa di esempio è un bucket S3 con un Amazon Resource Name (ARN) di. `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}` In questo esempio, `region` è specifico in Regione AWS cui hai abilitato Security Lake ed `bucket-identifier` è una stringa alfanumerica unica a livello regionale che Security Lake assegna al bucket. Security Lake crea il bucket S3 per archiviare i dati di quella regione. La politica delle risorse definisce quali principali possono eseguire azioni sul bucket. Ecco un esempio di policy basata sulle risorse (bucket policy) che Security Lake allega al bucket:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        },
        {
            "Sid": "PutSecurityLakeObject",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "securitylake.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-east-1:{DA-AccountID}:*"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sulle politiche basate sulle risorse, consulta le politiche basate sull'identità e le politiche basate sulle risorse nella Guida per l'utente IAM.

Azioni politiche per Security Lake

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per un elenco delle azioni di Security Lake, consulta Azioni definite da Amazon Security Lake nel Service Authorization Reference.

Le azioni politiche in Security Lake utilizzano il seguente prefisso prima dell'azione:

```
securitylake
```

Ad esempio, per concedere a un utente l'autorizzazione ad accedere alle informazioni su un sottoscrittore specifico, includi l'`securitylake:GetSubscriber`azione nella politica assegnata a quell'utente. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Security Lake definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "securitylake:action1",
      "securitylake:action2"
]
```

Per visualizzare esempi di politiche basate sull'identità di Security Lake, vedere. Esempi di policy basate sull'identità per Amazon Security Lake

Risorse politiche per Security Lake

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Security Lake definisce i seguenti tipi di risorse: sottoscrittore e configurazione del data lake per un Account AWS particolare utente. Regione AWS È possibile specificare questi tipi di risorse nelle politiche utilizzando gli ARN.

Per un elenco dei tipi di risorse di Security Lake e la sintassi ARN per ciascuno di essi, consulta Tipi di risorse definiti da Amazon Security Lake nel Service Authorization Reference. Per sapere quali azioni è possibile specificare per ogni tipo di risorsa, consulta Azioni definite da Amazon Security Lake nel Service Authorization Reference.

Per visualizzare esempi di politiche basate sull'identità di Security Lake, consulta. Esempi di policy basate sull'identità per Amazon Security Lake

Chiavi relative alle condizioni delle policy per Security Lake

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per un elenco delle chiavi di condizione di Security Lake, consulta Chiavi di condizione per Amazon Security Lake nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon Security Lake nel Service Authorization Reference. Per esempi di politiche che utilizzano chiavi di condizione, consultaEsempi di policy basate sull'identità per Amazon Security Lake.

Liste di controllo degli accessi (ACL) in Security Lake

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Security Lake non supporta gli ACL, il che significa che non è possibile collegare un ACL a una risorsa Security Lake.

Controllo degli accessi basato sugli attributi (ABAC) con Security Lake

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

È possibile allegare tag alle risorse di Security Lake, agli abbonati e alla configurazione del data lake per un singolo individuo. Account AWS Regioni AWS È inoltre possibile controllare l'accesso a questi tipi di risorse fornendo informazioni sui tag nell'elemento di una policy. `Condition` Per informazioni sull'etichettatura delle risorse di Security Lake, consultaEtichettatura delle risorse di Amazon Security Lake. Per un esempio di politica basata sull'identità che controlla l'accesso a una risorsa in base ai tag di quella risorsa, vedi. Esempi di policy basate sull'identità per Amazon Security Lake

Utilizzo di credenziali temporanee con Security Lake

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Security Lake supporta l'uso di credenziali temporanee.

Sessioni di accesso diretto per Security Lake

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Alcune azioni di Security Lake richiedono autorizzazioni per azioni aggiuntive e dipendenti in altre. Servizi AWS Per un elenco di queste azioni, consulta Azioni definite da Amazon Security Lake nel Service Authorization Reference.

Ruoli di servizio per Security Lake

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

Security Lake non assume né utilizza ruoli di servizio. Tuttavia, i servizi correlati come Amazon EventBridge e Amazon S3 assumono ruoli di servizio quando si utilizza Security Lake. AWS Lambda Per eseguire azioni per tuo conto, Security Lake utilizza un ruolo collegato al servizio.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio può creare problemi operativi con l'utilizzo di Security Lake. Modifica i ruoli di servizio solo quando Security Lake fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Security Lake

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Security Lake utilizza un ruolo collegato al servizio IAM denominato. `AWSServiceRoleForAmazonSecurityLake` Il ruolo collegato al servizio Security Lake concede le autorizzazioni per gestire un servizio Security Data Lake per conto dei clienti. Questo ruolo collegato ai servizi è un ruolo IAM collegato direttamente a Security Lake. È predefinito da Security Lake e include tutte le autorizzazioni richieste da Security Lake per chiamare altri Servizi AWS utenti per tuo conto. Security Lake utilizza questo ruolo collegato ai servizi in tutti i paesi in Regioni AWS cui Security Lake è disponibile.

Per i dettagli sulla creazione o la gestione del ruolo collegato ai servizi di Security Lake, consulta. Ruolo collegato ai servizi per Amazon Security Lake

Esempi di policy basate sull'identità per Amazon Security Lake

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse di Security Lake. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Security Lake, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Security Lake nel Service Authorization Reference.

Argomenti

- Best practice per le policy

- Utilizzo della console Security Lake
- Esempio: consentire agli utenti di visualizzare le loro autorizzazioni
- Esempio: consentire all'account di gestione dell'organizzazione di designare e rimuovere un amministratore delegato
- Esempio: consenti agli utenti di recensire gli abbonati in base ai tag

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Security Lake nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Security Lake

Per accedere alla console Amazon Security Lake, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse di Security Lake presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano utilizzare la console Security Lake, crea policy IAM che forniscano loro l'accesso alla console. Per ulteriori informazioni, consulta Identità IAM nella Guida per l'utente IAM.

Se crei una policy che consente agli utenti o ai ruoli di utilizzare la console Security Lake, assicurati che la policy includa le azioni appropriate per le risorse a cui tali utenti o ruoli devono accedere sulla console. Altrimenti, non saranno in grado di navigare o visualizzare i dettagli su tali risorse sulla console.

Ad esempio, per aggiungere una fonte personalizzata utilizzando la console, a un utente deve essere consentito di eseguire le seguenti azioni:

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StartCrawlerSchedule`
- `iam:GetRole`

- iam:PutRolePolicy
- iam:DeleteRolePolicy
- iam:PassRole
- lakeformation:RegisterResource
- lakeformation:GrantPermissions
- s3:ListBucket
- s3:PutObject

Esempio: consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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": "*"
        }
    ]
}
```

Esempio: consentire all'account di gestione dell'organizzazione di designare e rimuovere un amministratore delegato

Questo esempio mostra come è possibile creare una politica che consenta a un utente di un account di AWS Organizations gestione di designare e rimuovere l'amministratore delegato di Security Lake per la propria organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "securitylake:RegisterDataLakeDelegatedAdministrator",
                "securitylake:DeregisterDataLakeDelegatedAdministrator"
            ],
            "Resource": "arn:aws:securitylake:*:*:*"
        }
    ]
}
```

Esempio: consenti agli utenti di recensire gli abbonati in base ai tag

Nelle politiche basate sull'identità, è possibile utilizzare le condizioni per controllare l'accesso alle risorse di Security Lake in base ai tag. Questo esempio mostra come è possibile creare una policy che consenta a un utente di esaminare gli abbonati utilizzando la console di Security Lake o l'API di Security Lake. Tuttavia, l'autorizzazione viene concessa solo se il valore del `Owner` tag per un abbonato è il nome utente dell'utente.

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

In questo esempio, se un utente con il nome utente `richard-roe` tenta di esaminare i dettagli dei singoli abbonati, un abbonato deve essere taggato o. `0wner=richard-roe` `owner=richard-roe` In caso contrario, a questo utente viene negato l'accesso. La chiave di tag di condizione `0wner` corrisponde sia a `0wner` che a `owner` perché i nomi delle chiavi di condizione non distinguono tra maiuscole e minuscole. Per ulteriori informazioni sull'utilizzo delle chiavi di condizione, consulta IAM JSON Policy elements: Condition nella IAM User Guide. Per informazioni sull'etichettatura delle risorse di Security Lake, consulta. Etichettatura delle risorse di Amazon Security Lake

AWS politiche gestite per Amazon Security Lake

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo

pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AmazonSecurityLakeMetastoreManager

Amazon Security Lake utilizza una AWS Lambda funzione per gestire i metadati nel tuo data lake. Tramite l'uso di questa funzione, Security Lake può indicizzare le partizioni Amazon Simple Storage Service (Amazon S3) che contengono i dati e i file di dati nelle AWS Glue tabelle del Data Catalog. Questa policy gestita contiene tutte le autorizzazioni per la funzione Lambda per indicizzare le partizioni e i file di dati S3 nelle tabelle. AWS Glue

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `logs`— Consente ai responsabili di registrare l'output della funzione Lambda in Amazon CloudWatch Logs.
- `glue`— Consente ai principali di eseguire azioni di scrittura specifiche per le tabelle di Data Catalog. AWS Glue Ciò consente inoltre ai AWS Glue crawler di identificare le partizioni nei dati.
- `sqs`— Consente ai principali di eseguire azioni di lettura e scrittura specifiche per le code Amazon SQS che inviano notifiche di eventi quando gli oggetti vengono aggiunti o aggiornati nel tuo data lake.
- `s3`— Consente ai responsabili di eseguire azioni di lettura e scrittura specifiche per il bucket Amazon S3 che contiene i tuoi dati.

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

```
            "Sid": "AllowWriteLambdaLogs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
                "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowGlueManage",
            "Effect": "Allow",
            "Action": [
                "glue:CreatePartition",
                "glue:BatchCreatePartition",
                "glue:GetTable",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
                "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
                "arn:aws:glue:*:*:catalog"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowToReadFromSqs",
            "Effect": "Allow",
            "Action": [
                "sqs:ReceiveMessage",
                "sqs:DeleteMessage",
                "sqs:GetQueueAttributes"
```

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

AWS politica gestita: AmazonSecurityLakePermissionsBoundary

Amazon Security Lake crea ruoli IAM per fonti personalizzate di terze parti per scrivere dati nel data lake e per consentire agli abbonati personalizzati di terze parti di utilizzare i dati dal data lake e utilizza questa politica durante la creazione di questi ruoli per definire i limiti delle loro autorizzazioni. Non è necessario agire per utilizzare questa policy. Se il data lake è crittografato con una AWS KMS chiave gestita dal cliente `kms:Decrypt` e vengono aggiunte `kms:GenerateDataKey` le autorizzazioni.

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

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

```
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "kms:ViaService": [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": [
```

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

AWS politica gestita: AmazonSecurityLakeAdministrator

Puoi collegare la `AmazonSecurityLakeAdministrator` policy a un principale prima che abiliti Amazon Security Lake per il proprio account. Questa politica concede autorizzazioni amministrative che consentono l'accesso completo e principale a tutte le azioni di Security Lake. Il responsabile può quindi effettuare l'onboarding su Security Lake e successivamente configurare sorgenti e abbonati in Security Lake.

Questa politica include le azioni che gli amministratori di Security Lake possono eseguire su altri AWS servizi tramite Security Lake.

La `AmazonSecurityLakeAdministrator` policy non supporta la creazione di ruoli di utilità richiesti da Security Lake per gestire la replica interregionale di Amazon S3, la registrazione di nuove partizioni di dati, l' AWS Glueesecuzione di un crawler Glue sui dati aggiunti a fonti personalizzate o la notifica di nuovi dati agli abbonati agli endpoint HTTPS. Puoi creare questi ruoli in anticipo, come descritto in. Guida introduttiva ad Amazon Security Lake

Oltre alla policy `AmazonSecurityLakeAdministrator` gestita, Security Lake richiede `lakeformation:PutDataLakeSettings` le autorizzazioni per le funzioni di onboarding e configurazione. `PutDataLakeSettings`consente di impostare un responsabile IAM come amministratore per tutte le risorse regionali di Lake Formation nell'account. Questo `iam:CreateRole permission` ruolo deve essere accompagnato da una `AmazonSecurityLakeAdministrator` politica.

Gli amministratori di Lake Formation hanno pieno accesso alla console di Lake Formation e controllano la configurazione iniziale dei dati e le autorizzazioni di accesso. Security Lake assegna il principale che abilita Security Lake e il `AmazonSecurityLakeMetaStoreManager` ruolo (o altro ruolo specificato) come amministratori di Lake Formation in modo che possano creare tabelle, aggiornare lo schema delle tabelle, registrare nuove partizioni e configurare le autorizzazioni sulle tabelle. È necessario includere le seguenti autorizzazioni nella politica per l'utente o il ruolo di amministratore di Security Lake:

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

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `securitylake`— Consente ai responsabili l'accesso completo a tutte le azioni di Security Lake.
- `organizations`— Consente ai responsabili di recuperare informazioni da AWS Organizations sugli account di un'organizzazione. Se un account appartiene a un'organizzazione, queste autorizzazioni consentono alla console di Security Lake di visualizzare nomi e numeri di account.
- `iam`— Consente ai responsabili di creare ruoli collegati ai servizi per Security Lake e AWS Lake Formation, come passaggio obbligatorio Amazon EventBridge, di abilitare tali servizi. Consente inoltre la creazione e la modifica di politiche per i ruoli di sottoscrittore e di origine personalizzati, con le autorizzazioni di tali ruoli limitate a quanto consentito dalla politica. `AmazonSecurityLakePermissionsBoundary`
- `ram`— Consente ai responsabili di configurare l'accesso Lake Formation basato sulle query da parte degli abbonati alle sorgenti di Security Lake.
- `s3`— Consente ai responsabili di creare e gestire i bucket Security Lake e di leggerne il contenuto.
- `lambda`— Consente ai principali di gestire le partizioni di tabella Lambda utilizzate per aggiornare le partizioni di AWS Glue tabella dopo la distribuzione del AWS codice sorgente e la replica tra regioni.
- `glue`— Consente ai responsabili di creare e gestire il database e le tabelle di Security Lake.
- `lakeformation`— Consente ai responsabili di gestire le Lake Formation autorizzazioni per le tabelle di Security Lake.
- `events`— Consente ai responsabili di gestire le regole utilizzate per notificare agli abbonati nuovi dati nelle fonti Security Lake.
- `sqs`— Consente ai responsabili di creare e gestire le Amazon SQS code utilizzate per notificare agli abbonati nuovi dati nelle fonti Security Lake.
- `kms`— Consente ai responsabili di concedere l'accesso a Security Lake per scrivere dati utilizzando una chiave gestita dal cliente.
- `secretsmanager`— Consente ai responsabili di gestire i segreti utilizzati per notificare agli abbonati nuovi dati nelle fonti Security Lake tramite endpoint HTTPS.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowActionsWithAnyResource",
    "Effect": "Allow",
    "Action": [
      "securitylake:*",
      "organizations:DescribeOrganization",
      "organizations:ListDelegatedServicesForAccount",
      "organizations:ListAccounts",
      "iam:ListRoles",
      "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
    "Effect": "Allow",
    "Action": [
      "glue:CreateCrawler",
      "glue:StopCrawlerSchedule",
      "lambda:CreateEventSourceMapping",
      "lakeformation:GrantPermissions",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "lakeformation:GetDatalakeSettings",
      "events:ListConnections",
      "events:ListApiDestinations",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowManagingSecurityLakeS3Buckets",
```

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

```
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringEquals": {
        "lambda:Principal": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "glue:CreateTable",
      "glue:GetTable"
    ],
    "Resource": [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowEventBridgeActions",
    "Effect": "Allow",
    "Action": [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
```

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

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

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

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

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

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

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

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

AWS politica gestita: SecurityLakeServiceLinkedRole

Non puoi allegare la policy `SecurityLakeServiceLinkedRole` gestita alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a Security Lake di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Ruolo collegato ai servizi per Amazon Security Lake.

AWS politica gestita: AWS GlueServiceRole

La policy `AWSGlueServiceRole` gestita richiama il AWS Glue crawler e consente di eseguire la scansione dei dati di origine personalizzati e AWS Glue identificare i metadati delle partizioni. Questi metadati sono necessari per creare e aggiornare tabelle nel Data Catalog.

Per ulteriori informazioni, consulta Raccolta di dati da fonti personalizzate.

Security Lake aggiorna le policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Security Lake da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Security Lake.

Modifica	Descrizione	Data
AmazonSecurityLakeAdministrator: aggiornamento a una policy esistente	Security Lake ha aggiornato la policy per consentire `iam:PassRole` il nuovo `AmazonSecurityLakeMetastoreManagerV2` ruolo e consente a Security Lake di implementare o aggiornare i componenti del data lake.	23 febbraio 2024
AmazonSecurityLakeMetastoreManager: nuova policy	Security Lake ha aggiunto una nuova policy gestita che concede a Security Lake le	23 gennaio 2024

Modifica	Descrizione	Data
	autorizzazioni per gestire i metadati nel data lake.	
AmazonSecurityLakeAdministrator: nuova policy	Security Lake ha aggiunto una nuova politica gestita che garantisce un accesso principale completo a tutte le azioni di Security Lake.	30 maggio 2023
Security Lake ha iniziato a tracciare le modifiche	Security Lake ha iniziato a tenere traccia delle modifiche alle sue politiche AWS gestite.	29 novembre 2022

Ruolo collegato ai servizi per Amazon Security Lake

Security Lake utilizza un ruolo collegato al servizio AWS Identity and Access Management (IAM) denominato. `AWSServiceRoleForSecurityLake` Questo ruolo collegato ai servizi è un ruolo IAM collegato direttamente a Security Lake. È predefinito da Security Lake e include tutte le autorizzazioni richieste da Security Lake per chiamare altri Servizi AWS utenti per conto dell'utente e gestire il servizio Security Data Lake. Security Lake utilizza questo ruolo collegato ai servizi in tutti i Regioni AWS casi in cui Security Lake è disponibile.

Il ruolo collegato ai servizi elimina la necessità di aggiungere manualmente le autorizzazioni necessarie durante la configurazione di Security Lake. Security Lake definisce le autorizzazioni di questo ruolo collegato al servizio e, se non diversamente definito, solo Security Lake può assumere il ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM. È possibile eliminare un ruolo collegato al servizio solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di perché impedisce la rimozione involontaria delle autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Sì con un link per esaminare la documentazione del ruolo collegata al servizio per quel servizio.

Argomenti

Autorizzazioni di ruolo collegate al servizio per Security Lake

Security Lake utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForSecurityLake` Questo ruolo collegato al servizio prevede che il `securitylake.amazonaws.com` servizio assuma il ruolo.

La politica di autorizzazione per il ruolo, denominata policy AWS gestita`SecurityLakeServiceLinkedRole`, consente a Security Lake di creare e gestire il data lake di sicurezza. Consente inoltre a Security Lake di eseguire attività come le seguenti sulle risorse specificate:

- Usa AWS Organizations le azioni per recuperare informazioni sugli account associati
- Usa Amazon Elastic Compute Cloud (Amazon EC2) per recuperare informazioni sui log di flusso di Amazon VPC
- Utilizza AWS CloudTrail le azioni per recuperare informazioni sul ruolo collegato al servizio

Il ruolo è configurato con la seguente politica di autorizzazioni:

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

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

```
        },
        {
            "Sid": "ListDelegatedAdmins",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securitylake.amazonaws.com"
                }
            }
        }
    ]
}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione del ruolo collegato al servizio di Security Lake

Non è necessario creare manualmente il ruolo `AWSServiceRoleForSecurityLake` collegato ai servizi per Security Lake. Quando abiliti Security Lake per il tuoAccount AWS, Security Lake crea automaticamente il ruolo collegato al servizio per te.

Modifica del ruolo collegato al servizio di Security Lake

Security Lake non consente di modificare il ruolo `AWSServiceRoleForSecurityLake` collegato al servizio. Dopo la creazione di un ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché diverse entità potrebbero fare riferimento al ruolo. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione del ruolo collegato al servizio di Security Lake

Non è possibile eliminare il ruolo collegato al servizio da Security Lake. Puoi invece eliminare il ruolo collegato al servizio dalla console IAM, dall'API o. AWS CLI Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Prima di poter eliminare il ruolo collegato al servizio, è necessario verificare che il ruolo non abbia sessioni attive e rimuovere le risorse utilizzate`AWSServiceRoleForSecurityLake`.

> **Note**
>
> Se Security Lake utilizza il `AWSServiceRoleForSecurityLake` ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In tal caso, attendi qualche minuto e riprova l'operazione.

Se elimini il ruolo `AWSServiceRoleForSecurityLake` collegato al servizio e devi crearlo di nuovo, puoi crearlo nuovamente abilitando Security Lake per il tuo account. Quando abiliti nuovamente Security Lake, Security Lake crea automaticamente nuovamente il ruolo collegato al servizio per te.

Supportato Regioni AWS per il ruolo collegato ai servizi di Security Lake

Security Lake supporta l'utilizzo del ruolo `AWSServiceRoleForSecurityLake` collegato ai servizi in tutti i Regioni AWS casi in cui Security Lake è disponibile. Per un elenco delle regioni in cui Security Lake è attualmente disponibile, consultaRegioni ed endpoint Amazon Security Lake Lake Lake.

Protezione dei dati in Amazon Security Lake

Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in Amazon Security Lake. Come descritto in questo modello, AWSè responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.

- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Security Lake o altri utenti Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

Amazon Security Lake archivia in modo sicuro i dati archiviati utilizzando soluzioni di AWS crittografia. I log di sicurezza non elaborati e i dati degli eventi vengono archiviati in un bucket Amazon Simple Storage Service (Amazon S3) multi-tenant in un account gestito da Security Lake. Security Lake crittografa questi dati non elaborati utilizzando una chiave di AWSproprietà di (). AWS Key Management Service AWS KMS AWSle chiavi di proprietà sono una raccolta di AWS KMS chiavi che un AWS servizio, in questo caso Security Lake, possiede e gestisce per l'uso in più account. AWS

Security Lake esegue processi di estrazione, trasformazione e caricamento (ETL) su dati di log ed eventi non elaborati. I dati elaborati rimangono crittografati nell'account del servizio Security Lake.

Una volta completati i processi ETL, Security Lake crea bucket S3 single-tenant nel tuo account (un bucket per ogni bucket in Regione AWS cui hai abilitato Security Lake). I dati vengono archiviati nel bucket S3 multi-tenant solo temporaneamente fino a quando Security Lake non è in grado di consegnarli in modo affidabile ai bucket S3 single-tenant. I bucket single-tenant includono una policy basata sulle risorse che autorizza Security Lake a scrivere dati di log ed eventi nei bucket. Per

crittografare i dati nel bucket S3, puoi scegliere una chiave di crittografia gestita da S3 o una chiave gestita dal cliente (da). AWS KMS Entrambe le opzioni utilizzano la crittografia simmetrica.

Utilizzo di una chiave KMS per la crittografia dei dati

Per impostazione predefinita, i dati forniti da Security Lake al tuo bucket S3 sono crittografati mediante crittografia lato server di Amazon con chiavi di crittografia gestite da Amazon S3 (SSE-S3). Per fornire un livello di sicurezza da gestire direttamente, puoi invece utilizzare la crittografia lato server con chiavi (SSE-KMS) per i dati di Security Lake. AWS KMS

SSE-KMS non è supportato nella console di Security Lake. Per utilizzare SSE-KMS con l'API o la CLI di Security Lake, devi prima creare una chiave KMS o utilizzare una chiave esistente. Alla chiave si allega una policy che determina quali utenti possono utilizzare la chiave per crittografare e decrittografare i dati di Security Lake.

Se utilizzi una chiave gestita dal cliente per crittografare i dati scritti nel tuo bucket S3, non puoi scegliere una chiave multiregionale. Per le chiavi gestite dal cliente, Security Lake crea una concessione per tuo conto inviando una richiesta a. `CreateGrant` AWS KMS Le concessioni AWS KMS vengono utilizzate per consentire a Security Lake di accedere a una chiave KMS in un account cliente.

Security Lake richiede la concessione per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia `GenerateDataKey` richieste per AWS KMS generare chiavi dati crittografate dalla chiave gestita dal cliente.
- Invia `RetireGrant` richieste aAWS KMS. Quando effettui aggiornamenti al tuo data lake, questa operazione consente il ritiro della sovvenzione aggiunta alla chiave AWS KMS per l'elaborazione ETL.

Security Lake non necessita di autorizzazioni. `Decrypt` Quando gli utenti autorizzati della chiave leggono i dati di Security Lake, S3 gestisce la decrittografia e gli utenti autorizzati sono in grado di leggere i dati in forma non crittografata. Tuttavia, un abbonato necessita delle `Decrypt` autorizzazioni per utilizzare i dati di origine. Per ulteriori informazioni sulle autorizzazioni degli abbonati, consulta. Gestione dell'accesso ai dati per gli abbonati a Security Lake

La tua chiave KMS può accettare richieste di concessione, consentendo a Security Lake di accedere alla chiave, quando crei una politica chiave o utilizzi una politica chiave esistente con le autorizzazioni appropriate. Per istruzioni sulla creazione di una politica chiave, consulta Creazione di una politica

chiave nella Guida per gli AWS Key Management Servicesviluppatori. Allega la seguente politica chiave alla tua chiave 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": "*"
}
```

Autorizzazioni IAM richieste quando si utilizza una chiave gestita dal cliente

Consulta la sezione Guida introduttiva: prerequisiti per una panoramica dei ruoli IAM che devi creare per utilizzare Security Lake.

Quando aggiungi una fonte personalizzata o un abbonato, Security Lake crea ruoli IAM nel tuo account. Questi ruoli sono destinati a essere condivisi con altre identità IAM. Consentono a una fonte personalizzata di scrivere dati nel data lake e a un abbonato di utilizzare i dati dal data lake. Una policy AWS gestita denominata `AmazonSecurityLakePermissionsBoundary` definisce i limiti di autorizzazione per questi ruoli.

Crittografia delle code Amazon SQS

Quando crei il tuo data lake, Security Lake crea due code Amazon Simple Queue Service (Amazon SQS) non crittografate nell'account amministratore delegato di Security Lake. È necessario crittografare queste code per proteggere i dati. La crittografia lato server (SSE) predefinita fornita da Amazon Simple Queue Service non è sufficiente. È necessario creare una chiave gestita dal cliente in AWS Key Management Service (AWS KMS) per crittografare le code e concedere al servizio Amazon S3 le autorizzazioni principali per lavorare con le code crittografate. Per istruzioni su come concedere queste autorizzazioni, consulta Perché le notifiche degli eventi di Amazon S3 non vengono recapitate a una coda Amazon SQS che utilizza la crittografia lato server? nel AWS Knowledge Center.

Poiché Security Lake supporta AWS Lambda i processi di estrazione, trasferimento e caricamento (ETL) sui tuoi dati, devi anche concedere le autorizzazioni Lambda per gestire i messaggi nelle code

di Amazon SQS. Per informazioni, consulta Autorizzazioni per i ruoli di esecuzione nella Guida per gli sviluppatori. AWS Lambda

Crittografia in transito

Security Lake crittografa tutti i dati in transito tra AWS i servizi. Security Lake protegge i dati in transito, mentre viaggiano da e verso il servizio, crittografando automaticamente tutti i dati tra reti utilizzando il protocollo di crittografia Transport Layer Security (TLS) 1.2. Le richieste HTTPS dirette inviate alle API di Security Lake vengono firmate utilizzando l'algoritmo AWS Signature Version 4 per stabilire una connessione sicura.

Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio

Puoi scegliere di rinunciare all'utilizzo dei tuoi dati per sviluppare e migliorare Security Lake e altri servizi di AWS sicurezza utilizzando la politica di AWS Organizations opt-out. Puoi scegliere di rinunciare anche se Security Lake al momento non raccoglie tali dati. Per ulteriori informazioni in merito, consulta le Policy di rifiuto dei servizi di IA nella Guida per l'utente di AWS Organizations.

Attualmente, Security Lake non raccoglie i dati di sicurezza che elabora per conto dell'utente, né i dati di sicurezza caricati sul data lake di sicurezza creato da questo servizio. Per sviluppare e migliorare il servizio Security Lake e le funzionalità di altri servizi di AWS sicurezza, Security Lake potrebbe raccogliere tali dati in futuro, compresi i dati caricati da fonti di dati di terze parti. Aggiorneremo questa pagina quando Security Lake intende raccogliere tali dati e ne descriveremo il funzionamento. Avrai comunque la possibilità di annullare l'iscrizione in qualsiasi momento.

> **Note**
>
> I tuoi account AWS devono essere gestiti centralmente da AWS Organizations affinché tu possa utilizzare la policy di rifiuto esplicito. Se non hai ancora creato un'organizzazione per i tuoi account AWS, consulta Creazione e gestione di un'organizzazione nella Guida per l'utente di AWS Organizations.

Il rifiuto esplicito ha gli effetti seguenti:

- Security Lake eliminerà i dati raccolti e archiviati prima della revoca del consenso (se presente).
- Dopo l'annullamento, Security Lake non raccoglierà o memorizzerà più questi dati.

Convalida della conformità per Amazon Security Lake

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWSincentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWSper creare applicazioni conformi alla normativa HIPAA.

  > **Note**
  >
  > Non tutti i Servizi AWSsono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- AWSGuide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Configvaluta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse

AWSe verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- AWS Audit Manager: questo Servizio AWSaiuta a verificare continuamente l'utilizzo di AWSper semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Procedure consigliate per la sicurezza per Security Lake

Consulta le seguenti best practice per lavorare con Amazon Security Lake.

Concedi agli utenti di Security Lake le autorizzazioni minime possibili

Segui il principio del privilegio minimo concedendo il set minimo di autorizzazioni ai criteri di accesso per i tuoi utenti, gruppi di utenti e ruoli AWS Identity and Access Management (IAM). Ad esempio, potresti consentire a un utente IAM di visualizzare un elenco di fonti di log in Security Lake ma non di creare fonti o abbonati. Per ulteriori informazioni, consulta Esempi di policy basate sull'identità per Amazon Security Lake.

Puoi anche usarlo AWS CloudTrail per tenere traccia dell'utilizzo delle API in Security Lake. CloudTrailfornisce un registro delle azioni API intraprese da un utente, un gruppo o un ruolo in Security Lake. Per ulteriori informazioni, consulta Registrazione delle chiamate API di Amazon Security Lake utilizzando AWS CloudTrail.

Visualizza la pagina di riepilogo

La pagina di riepilogo della console Security Lake fornisce una panoramica dei problemi degli ultimi 14 giorni che hanno avuto un impatto sul servizio Security Lake e sui bucket Amazon S3 in cui sono archiviati i dati. Puoi approfondire questi problemi per aiutarti a mitigare il possibile impatto relativo alla sicurezza.

Integrazione con Security Hub

Integra Security Lake e AWS Security Hub ricevi i risultati di Security Hub in Security Lake. Security Hub genera risultati da molte integrazioni diverse Servizi AWS e di terze parti. Ricevere i risultati di Security Hub ti aiuta a ottenere una panoramica del tuo livello di conformità e verificare se stai rispettando le best practice AWS di sicurezza.

Per ulteriori informazioni, consulta Integrazione con AWS Security Hub.

Monitor per gli eventi di Security Lake

Puoi monitorare Security Lake utilizzando le CloudWatch metriche di Amazon. CloudWatchraccoglie dati grezzi da Security Lake ogni minuto e li elabora in metriche. Puoi impostare allarmi che attivano notifiche quando le metriche corrispondono a soglie specificate.

Per ulteriori informazioni, consulta CloudWatchParametri per Amazon Security Lake.

Resilienza in Amazon Security Lake

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità effettiva elevata. Queste zone di disponibilità offrono un modo efficace per progettare e gestire le applicazioni e i database. Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

La disponibilità di Security Lake è legata alla disponibilità regionale. La distribuzione su più zone di disponibilità aiuta il servizio a tollerare i guasti in ogni singola zona di disponibilità.

La disponibilità del piano dati di Security Lake non è legata alla disponibilità di alcuna regione. Tuttavia, la disponibilità del piano di controllo di Security Lake è strettamente legata alla disponibilità della regione Stati Uniti orientali (Virginia settentrionale).

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura AWS globale, Security Lake, in cui i dati sono supportati da Amazon Simple Storage Service (Amazon S3), offre diverse funzionalità per supportare le tue esigenze di resilienza e backup dei dati.

Configurazione del ciclo di vita

> Una configurazione del ciclo di vita è un insieme di regole che definiscono le operazioni applicate da Amazon S3 a un gruppo di oggetti. Tramite le regole di configurazione del ciclo di vita, è possibile indicare ad Amazon S3 di trasferire gli oggetti in classi di storage meno costose, archiviarli o eliminarli. Per ulteriori informazioni, consulta Gestione del ciclo di vita dello storage nella Guida per l'utente di Amazon S3.

Funzione Versioni multiple

La funzione Controllo delle versioni è un modo per conservare più versioni di un oggetto nello stesso bucket. La funzione Controllo delle versioni può essere impiegata per conservare, recuperare e ripristinare qualsiasi versione di ogni oggetto archiviato nel bucket Amazon S3. Il controllo delle versioni consente di ripristinare sia le azioni involontarie degli utenti che i guasti delle applicazioni. Per ulteriori informazioni, consulta Using versioning in bucket S3 nella Amazon S3 User Guide.

Classi di archiviazione

Amazon S3 offre una gamma di classi di archiviazione tra cui scegliere in base ai requisiti del carico di lavoro. Le classi di archiviazione S3 Standard-IA e S3 One Zone-IA sono progettate per i dati a cui si accede almeno una volta al mese e richiedono l'accesso in millisecondi. La classe di archiviazione S3 Glacier Instant Retrieval è progettata per i dati di archiviazione di lunga durata a cui si accede in millisecondi circa una volta al trimestre. Per i dati di archiviazione che non richiedono accesso immediato, come i backup, è possibile utilizzare le classi di archiviazione S3 Glacier Flexier Retrieval o S3 Glacier Deep Archive. Per ulteriori informazioni, consulta Using Amazon S3 Storage Classes nella Amazon S3 User Guide.

Sicurezza dell'infrastruttura in Amazon Security Lake

In quanto servizio gestito, Amazon Security Lake è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Le chiamate API AWS pubblicate vengono utilizzate per accedere a Security Lake tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security

Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Analisi della configurazione e delle vulnerabilità in Security Lake

Configurazione e controllo IT sono una responsabilità condivisa tra AWS e te, il nostro cliente. Per ulteriori informazioni, consulta il modello di responsabilità condivisa di AWS.

Mondi Amazon SecLake di Amazon SecLake

SecLake di SecLake AWS CloudTrail Servizio AWS Ciò include le azioni dalla console di Security Lake e le chiamate programmatiche alle operazioni dell'API di Security Lake. Utilizzando le informazioni raccolte daCloudTrail, è possibile determinare quali richieste sono state effettuate a Security Lake. Per ogni richiesta, è possibile identificare quando è stata effettuata, l'indirizzo IP da cui è stata effettuata, chi l'ha effettuata e ulteriori dettagli. Per ulteriori informazioni, consulta Registrazione delle chiamate API di Amazon Security Lake utilizzando AWS CloudTrail.

Secdi di di di di di di di CloudWatch di di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake di SecLake CloudWatchle metriche per il data lake di Security Lake vengono raccolte automaticamente e inviate a CloudWatch intervalli di un minuto. Puoi anche impostare un allarme per ricevere una notifica se una notifica se una soglia specificata viene raggiunta per un parametro per ricevere una notifica se una soglia specificata viene raggiunta per un parametro per ricevere una notifica se una soglia specificata viene raggiunta per un parametro per Per un elenco di tutte le metriche inviate da Security LakeCloudWatch, consulta. Parametri e dimensioni di Security Lake

CloudWatchParametri per Amazon Security Lake

Puoi monitorare Security Lake utilizzando AmazonCloudWatch, che raccoglie i dati non elaborati ogni minuto e li elabora trasformandoli in parametri leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e per offrire una prospettiva migliore sui dati del parametro. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte.

Argomenti

Parametri e dimensioni di Security Lake

Il namespace `AWS/SecurityLake` include i parametri descritti di seguito.

Parametro	Descrizione
`ProcessedSize`	Il volume di dati con supporto nativo Servizi AWS attualmente archiviato nel tuo data lake. Unità: byte

Le seguenti dimensioni sono disponibili per le metriche di Security Lake.

Dimensione	Descrizione
`Account`	`ProcessedSize` metrica per uno specifico Account AWS. Questa dimensione è disponibi le solo quando si visualizza `Per-Account Source Version Metrics` onCloudWatch.
`Region`	`ProcessedSize` metrica per uno specifico Regione AWS.
`Source`	`ProcessedSize` metrica per una fonte di AWS registro specifica.
`SourceVersion`	`ProcessedSize` metrica per una versione specifica di un'origine di AWS registro.

Puoi visualizzare le metriche per account specifici Account AWS (`Per-Account Source Version Metrics`) o per tutti gli account di un'organizzazione (`Per-Source Version Metrics`).

Visualizzazione delle CloudWatch metriche per Security Lake

Puoi monitorare i parametri per Security Lake utilizzando la CloudWatch console, l'interfaccia a riga CloudWatch di comando (CLI) oppure a livello di codice utilizzando l'API a livello di codice utilizzando l'API. CloudWatch Scegli il tuo metodo preferito e segui i passaggi per accedere alle metriche di Security Lake.

CloudWatch console

1. Aprire la console CloudWatch all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, nel pannello di navigazione, scegli Parametri.
3. Nella scheda Sfoglia, scegli Security Lake.
4. Scegli Metriche della versione di origine per account o Metriche della versione sorgente per account.
5. Seleziona una metrica per visualizzarla in dettaglio. Puoi anche scegliere di effettuare le seguenti operazioni:
   - Per ordinare i parametri, utilizza l'intestazione della colonna.
   - Per il il il il grafico di un parametro di un parametro il il grafico di un parametro il il grafico di un parametro il grafico di un parametro il grafico di un parametro il grafico di un parametro
   - Per filtrare per metrica, seleziona il nome della metrica, quindi scegli Aggiungi alla ricerca.

CloudWatch API

Per accedere alle metriche di Security Lake utilizzando l'CloudWatchAPI, utilizza l'`GetMetricStatistics`azione.

AWS CLI

Per accedere alle metriche di Security Lake utilizzando il comandoAWS CLI, esegui il `get-metric-statistics`comando.

Per ulteriori informazioni sul monitoraggio tramite metriche, consulta Usa le CloudWatch metriche Amazon nella Amazon CloudWatch User Guide.

Impostazione degli CloudWatch allarmi per le metriche di Security Lake

CloudWatch consente inoltre di impostare allarmi quando viene raggiunta la soglia definita per un parametro. Ad esempio, puoi impostare un allarme per la ProcessedSizemetrica, in modo da ricevere una notifica quando il volume di dati da una fonte specifica supera una soglia specifica.

Per istruzioni sull'impostazione degli allarmi, consulta Utilizzo degli CloudWatch allarmi Amazon nella Guida per l'CloudWatchutente di Amazon.

Registrazione delle chiamate API di Amazon Security Lake utilizzando AWS CloudTrail

Amazon Security Lake si integra con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un AWS servizio in Security Lake. CloudTrailacquisisce le chiamate API per Security Lake come eventi. Le chiamate acquisite includono chiamate dalla console Security Lake e chiamate in codice alle operazioni API di Security Lake. Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi su un bucket Amazon S3, inclusi gli eventi per Security Lake. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Utilizzando le informazioni raccolte daCloudTrail, è possibile determinare la richiesta effettuata a Security Lake, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni su CloudTrail, consulta la Guida per l'utente di AWS CloudTrail.

Informazioni su Security Lake in CloudTrail

CloudTrail è abilitato sull'Account AWS al momento della sua creazione. Quando si verifica un'attività in Security Lake, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continua degli eventi in programmaAccount AWS, inclusi quelli per Security Lake, crea un percorso. Un percorso consente di CloudTrail inviare eventi come file di registro a un bucket Amazon S3 specificato. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei log CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni e Ricezione di file di log CloudTrail da più account

Le azioni di Security Lake vengono registrate CloudTrail e documentate nel Security Lake API Reference. Ad esempio, le chiamate alle operazioni `UpdateDataLake`, `ListLogSources` e `CreateSubscriber` generano voci nei file di log CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente AWS Identity and Access Management o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail.

Comprendere le voci dei file di registro di Security Lake

I file di log di CloudTrail contengono una o più voci di log. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sul operazione richiesta, data e ora dell'operazione, parametri richiesti e così via. I file di log di CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro per l'`GetSubscriber`azione 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"
}
```

Etichettatura delle risorse di Amazon Security Lake

Un tag è un'etichetta opzionale che puoi definire e assegnare alle AWS risorse, inclusi determinati tipi di risorse Amazon Security Lake. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Ad esempio, puoi utilizzare i tag per applicare politiche, allocare costi, distinguere tra risorse o identificare risorse che supportano determinati requisiti o flussi di lavoro di conformità.

È possibile assegnare tag ai seguenti tipi di risorse Security Lake: abbonati e configurazione del data lake individualmente. Account AWS Regioni AWS

Argomenti

Nozioni fondamentali sull'etichettatura

Una risorsa può avere fino a 50 tag. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale, entrambi definibili dall'utente. Una chiave di tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

Ad esempio, se aggiungi abbonati per analizzare i dati di sicurezza provenienti da ambienti diversi (un set di abbonati per i dati cloud e un altro set per i dati locali), puoi assegnare una chiave di `Environment` tag a tali abbonati. Il valore del tag associato potrebbe essere `Cloud` destinato agli abbonati che analizzano i dati provenienti da Servizi AWS e per gli altri. `On-Premises`

Quando definisci e assegni tag alle risorse di Amazon Security Lake, tieni presente quanto segue:

- Ogni risorsa può avere un massimo di 50 tag.
- Per ogni risorsa, ogni chiave di tag deve essere unica e può avere un solo valore di tag.

- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Come best practice, ti consigliamo di definire una strategia per utilizzare i tag in maiuscolo e di implementarla in modo coerente tra le tue risorse.
- Una chiave tag può contenere un massimo di 128 caratteri UTF-8. Il valore di un tag può contenere un massimo di 256 caratteri UTF-8. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: _.:/= + - @
- Il `aws:` prefisso è riservato all'uso di AWS. Non puoi usarlo in nessuna chiave o valore di tag che definisci. Inoltre, non è possibile modificare o rimuovere le chiavi o i valori dei tag che utilizzano questo prefisso. I tag che utilizzano questo prefisso non vengono conteggiati per la quota di 50 tag per ogni risorsa.
- Tutti i tag che assegni sono disponibili solo per te Account AWS e solo nel gruppo Regione AWS in cui li assegni.
- Se si assegnano tag a una risorsa utilizzando Security Lake, i tag vengono applicati solo alla risorsa archiviata direttamente in Security Lake nel paese applicabile. Regione AWS Non vengono applicati a nessuna risorsa di supporto associata che Security Lake crea, utilizza o gestisce per te in altri Servizi AWS. Ad esempio, se si assegnano tag al data lake, i tag vengono applicati solo alla configurazione del data lake in Security Lake per la regione specificata. Non vengono applicati al bucket Amazon Simple Storage Service (Amazon S3) che archivia i dati di log ed eventi. Per assegnare tag anche a una risorsa associata, puoi utilizzare AWS Resource Groups o Servizio AWS quello che memorizza la risorsa, ad esempio Amazon S3 per un bucket S3. L'assegnazione di tag alle risorse associate può aiutarti a identificare le risorse di supporto per il tuo data lake.
- Se si elimina una risorsa, vengono eliminati anche tutti i tag assegnati alla risorsa.

Per ulteriori restrizioni, suggerimenti e best practice, consulta Tagging your AWS resources nella Tagging AWS Resources User Guide.

> **Important**
>
> Non archiviate dati riservati o di altro tipo nei tag. I tag sono accessibili da molti Servizi AWS, tra cui AWS Billing and Cost Management. Non sono destinati a essere utilizzati per dati sensibili.

Per aggiungere e gestire i tag per le risorse di Security Lake, puoi utilizzare la console di Security Lake o l'API di Security Lake.

Utilizzo di tag nelle policy IAM

Dopo aver iniziato ad assegnare tag alle risorse, puoi definire autorizzazioni a livello di risorsa basate su tag nelle policy (IAM). AWS Identity and Access Management Utilizzando i tag in questo modo, puoi implementare un controllo granulare su quali utenti e ruoli all'interno dell'azienda Account AWS sono autorizzati a creare e contrassegnare risorse e quali utenti e ruoli sono autorizzati ad aggiungere, modificare e rimuovere tag più in generale. Per controllare l'accesso in base ai tag, puoi utilizzare le chiavi di condizione relative ai tag nell'elemento Condition delle politiche IAM.

Ad esempio, puoi creare una policy che consenta a un utente di avere accesso completo a tutte le risorse di Amazon Security Lake, se il `Owner` tag della risorsa specifica il suo nome utente:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Se vengono definite autorizzazioni a livello di risorsa basate su tag, le autorizzazioni diventano subito effettive. Ciò significa che le risorse sono più sicure non appena vengono create e che è possibile avviare rapidamente l'applicazione di tag alle nuove risorse. È inoltre possibile utilizzare le autorizzazioni a livello di risorsa per controllare quali chiavi e valori di tag possono essere associati a risorse nuove ed esistenti. Per ulteriori informazioni, consulta Controlling access to AWS resources using tags nella IAM User Guide.

Aggiungere tag alle risorse di Amazon Security Lake

Per aggiungere tag a una risorsa Amazon Security Lake, puoi utilizzare la console Security Lake o l'API Security Lake.

> **Important**
>
> L'aggiunta di tag a una risorsa può influire sull'accesso alla risorsa. Prima di aggiungere un tag a una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare i tag per controllare l'accesso alle risorse.

Console

Quando abiliti Security Lake per un abbonato Regione AWS o crei un abbonato, la console Security Lake offre opzioni per aggiungere tag alla risorsa, ovvero la configurazione del data lake per la regione o il sottoscrittore. Segui le istruzioni sulla console per aggiungere tag alla risorsa quando la crei.

Per aggiungere uno o più tag a una risorsa esistente utilizzando la console Security Lake, segui questi passaggi.

Per aggiungere un tag a una risorsa

1. Apri la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. A seconda del tipo di risorsa a cui vuoi aggiungere un tag, esegui una delle seguenti operazioni:
   - Per una configurazione di data lake, scegli Regioni nel riquadro di navigazione. Quindi, nella tabella Regioni, seleziona la Regione.
   - Per un abbonato, scegli Sottoscrittori nel riquadro di navigazione. Quindi, nella tabella I miei abbonati, seleziona l'abbonato.

     Se l'abbonato non compare nella tabella, usa il Regione AWS selettore nell'angolo superiore destro della pagina per selezionare la regione in cui hai creato l'abbonato. La tabella elenca gli abbonati esistenti solo per la regione corrente.
3. Scegli Modifica.
4. Espandere la sezione Tag. Questa sezione elenca tutti i tag attualmente assegnati alla risorsa.
5. Nella sezione Tag, seleziona Aggiungi nuovo tag.
6. Nella casella Chiave, inserisci la chiave del tag da aggiungere alla risorsa. Quindi, nella casella Valore, inserite facoltativamente un valore di tag per la chiave.

Una chiave di tag può contenere fino a un massimo di 128 caratteri. Un valore di tag può contenere fino a un massimo di 256 caratteri. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: _.:/= + - @

7. Per aggiungere un altro tag alla risorsa, scegli Aggiungi nuovo tag, quindi ripeti il passaggio precedente. Puoi assegnare fino a 50 tag a una risorsa.
8. Quando hai finito di aggiungere i tag, scegli Salva.

API

Per creare una risorsa e aggiungervi uno o più tag a livello di codice, utilizzate l'`Create`operazione appropriata per il tipo di risorsa che desiderate creare:

- Configurazione del data lake: usa l'CreateDataLakeoperazione o, se stai usando il AWS Command Line Interface (AWS CLI), esegui il create-data-lakecomando.
- Sottoscrittore: utilizza l'CreateSubscriberoperazione o, se utilizzi il AWS CLI, esegui il comando create-subscriber.

Nella richiesta, utilizzate il `tags` parametro per specificare il tag key (`key`) e il tag value opzionale (`value`) per ogni tag da aggiungere alla risorsa. Il `tags` parametro specifica una matrice di oggetti. Ogni oggetto specifica una chiave di tag e il relativo valore di tag associato.

Per aggiungere uno o più tag a una risorsa esistente, utilizza l'TagResourceoperazione dell'API Security Lake o, se utilizzi il AWS CLI, esegui il comando tag-resource. Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa a cui desideri aggiungere un tag. Utilizza il `tags` parametro per specificare la chiave del tag (`key`) e il valore del tag opzionale (`value`) per ogni tag da aggiungere. Come nel caso delle `Create` operazioni e dei comandi, il `tags` parametro specifica una matrice di oggetti, un oggetto per ogni chiave di tag e il valore del tag associato.

Ad esempio, il AWS CLI comando seguente aggiunge una chiave di `Environment` tag con un valore di `Cloud` tag al sottoscrittore specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

Dove:

- `resource-arn`specifica l'ARN del sottoscrittore a cui aggiungere un tag.
- *`Environment`*è la chiave del tag da aggiungere al sottoscrittore.
- *`Cloud`*è il valore del tag per la chiave del tag specificata (*`Environment`*).

Nell'esempio seguente, il comando aggiunge diversi tag al sottoscrittore.

```
$ 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
```

Per ogni oggetto di una `tags` matrice, sono obbligatori `key` sia gli `value` argomenti che. Tuttavia, il valore dell'`value`argomento può essere una stringa vuota. Se non desiderate associare un valore di tag a una chiave di tag, non specificate un valore per l'`value`argomento. Ad esempio, il comando seguente aggiunge una chiave di `Owner` tag senza alcun valore di tag associato:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Se un'operazione di tagging ha esito positivo, Security Lake restituisce una risposta HTTP 200 vuota. Altrimenti, Security Lake restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Revisione dei tag per le risorse di Amazon Security Lake

Puoi esaminare i tag (sia chiavi che valori dei tag) per una risorsa Amazon Security Lake utilizzando la console Security Lake o l'API Security Lake.

Console

Segui questi passaggi per esaminare i tag di una risorsa utilizzando la console Security Lake.

Per esaminare i tag di una risorsa

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. A seconda del tipo di risorsa di cui desideri esaminare i tag, esegui una delle seguenti operazioni:

   - Per una configurazione di data lake, scegli Regioni nel riquadro di navigazione. Nella tabella Regioni, seleziona la Regione, quindi scegli Modifica. Quindi espandi la sezione Tag.
   - Per un abbonato, scegli Abbonati nel riquadro di navigazione. Quindi, nella tabella I miei abbonati, scegli il nome dell'abbonato.

     Se l'abbonato non compare nella tabella, usa il Regione AWS selettore nell'angolo in alto a destra della pagina per selezionare la regione in cui hai creato l'abbonato. La tabella elenca gli abbonati esistenti solo per la regione corrente.

La sezione Tag elenca tutti i tag attualmente assegnati alla risorsa.

API

Per recuperare e rivedere i tag di una risorsa esistente a livello di codice, utilizza il ListTagsForResourcefunzionamento dell'API Security Lake. Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa.

Se stai usando il AWS Command Line Interface (AWS CLI), esegui il list-tags-for-resourcecomando e usa il `resource-arn` parametro per specificare l'ARN della risorsa. Per esempio:

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

Nell'esempio precedente, *arn:aws:securitylake:us-east-*1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab è l'ARN di un abbonato esistente.

Se l'operazione ha esito positivo, Security Lake restituisce un array. `tags` Ogni oggetto dell'array specifica un tag (sia la chiave del tag che il valore del tag) attualmente assegnato alla risorsa. Per esempio:

```
{
```

```
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Dove `Environment` e `CostCenter` `Owner` sono le chiavi dei tag assegnate alla risorsa. `Cloud`è il valore del tag associato alla chiave del `Environment` tag. `12345`è il valore del tag associato alla chiave del `CostCenter` tag. La chiave `Owner` tag non ha un valore di tag associato.

Modifica dei tag per le risorse di Amazon Security Lake

Per modificare i tag (chiavi o valori dei tag) per una risorsa Amazon Security Lake, puoi utilizzare la console Security Lake o l'API Security Lake.

> **Important**
>
> La modifica dei tag di una risorsa può influire sull'accesso alla risorsa. Prima di modificare la chiave o il valore di un tag per una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse.

Console

Segui questi passaggi per modificare i tag di una risorsa utilizzando la console Security Lake.

Per modificare i tag di una risorsa

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.

2. A seconda del tipo di risorsa di cui desiderate modificare i tag, effettuate una delle seguenti operazioni:

   - Per una configurazione di data lake, scegli Regioni nel riquadro di navigazione. Quindi, nella tabella Regioni, seleziona la Regione.
   - Per un abbonato, scegli Sottoscrittori nel riquadro di navigazione. Quindi, nella tabella I miei abbonati, seleziona l'abbonato.

     Se l'abbonato non compare nella tabella, usa il Regione AWS selettore nell'angolo superiore destro della pagina per selezionare la regione in cui hai creato l'abbonato. La tabella elenca gli abbonati esistenti solo per la regione corrente.
3. Scegli Modifica.
4. Espandere la sezione Tag. La sezione Tag elenca tutti i tag attualmente assegnati alla risorsa.
5. Effettua una delle seguenti operazioni:

   - Per aggiungere un valore di tag a una chiave di tag esistente, inserite il valore nella casella Valore accanto alla chiave del tag.
   - Per modificare una chiave di tag esistente, scegliete Rimuovi accanto al tag. Quindi scegli Aggiungi nuovo tag. Nella casella Chiave che appare, inserisci la nuova chiave del tag. Facoltativamente, inserite un valore di tag associato nella casella Valore.
   - Per modificare il valore di un tag esistente, scegliete X nella casella Valore che contiene il valore. Quindi inserite il nuovo valore del tag nella casella Valore.
   - Per rimuovere un valore di tag esistente, scegliete X nella casella Valore che contiene il valore.
   - Per rimuovere un tag esistente (sia la chiave che il valore del tag), scegliete Rimuovi accanto al tag.

   Una risorsa può avere fino a 50 tag. Una chiave di tag può contenere fino a un massimo di 128 caratteri. Un valore di tag può contenere fino a un massimo di 256 caratteri. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: _.:/= + - @
6. Quando hai finito di modificare i tag, scegli Salva.

API

Quando modificate un tag per una risorsa a livello di codice, sovrascrivete il tag esistente con nuovi valori. Pertanto, il modo migliore per modificare un tag dipende dal fatto che si desideri modificare una chiave di tag, un valore di tag o entrambi. Per modificare una chiave di tag, rimuovi il tag corrente e aggiungi un nuovo tag.

Per modificare o rimuovere solo il valore del tag associato a una chiave di tag, sovrascrivi il valore esistente utilizzando il TagResourcefunzionamento dell'API Security Lake. Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando tag-resource. Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa di cui desideri modificare o rimuovere il valore del tag.

Per modificare il valore di un tag, utilizza il `tags` parametro per specificare la chiave del tag di cui desideri modificare il valore del tag. Specificate anche il nuovo valore del tag per la chiave. Ad esempio, il AWS CLI comando seguente modifica il valore del tag da `Cloud` a `On-Premises` per la chiave di `Environment` tag assegnata al sottoscrittore specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ 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
```

Dove:

- `resource-arn`specifica l'ARN del sottoscrittore.
- *`Environment`*è la chiave del tag associata al valore del tag da modificare.
- *`On-Premises`*è il nuovo valore del tag per la chiave di tag specificata (*`Environment`*).

Per rimuovere un valore di tag da una chiave di tag, non specificate un valore per l'`value`argomento della chiave nel `tags` parametro. Per esempio:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Se l'operazione ha esito positivo, Security Lake restituisce una risposta HTTP 200 vuota. Altrimenti, Security Lake restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Rimozione di tag dalle risorse di Amazon Security Lake

Per rimuovere i tag da una risorsa Amazon Security Lake, puoi utilizzare la console Security Lake o l'API Security Lake.

> **Important**
>
> La rimozione dei tag da una risorsa può influire sull'accesso alla risorsa. Prima di rimuovere un tag, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse.

Console

Segui questi passaggi per rimuovere uno o più tag da una risorsa utilizzando la console Security Lake.

Per rimuovere un tag da una risorsa

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. A seconda del tipo di risorsa da cui si desidera rimuovere un tag, effettuate una delle seguenti operazioni:
   - Per una configurazione di data lake, scegli Regioni nel riquadro di navigazione. Quindi, nella tabella Regioni, seleziona la Regione.
   - Per un abbonato, scegli Sottoscrittori nel riquadro di navigazione. Quindi, nella tabella I miei abbonati, seleziona l'abbonato.

     Se l'abbonato non compare nella tabella, usa il Regione AWS selettore nell'angolo superiore destro della pagina per selezionare la regione in cui hai creato l'abbonato. La tabella elenca gli abbonati esistenti solo per la regione corrente.
3. Scegli Modifica.
4. Espandere la sezione Tag. La sezione Tag elenca tutti i tag attualmente assegnati alla risorsa.

5. Effettua una delle seguenti operazioni:
   - Per rimuovere solo il valore del tag, scegliete X nella casella Valore che contiene il valore da rimuovere.
   - Per rimuovere sia la chiave che il valore del tag (in coppia) per un tag, scegliete Rimuovi accanto al tag da rimuovere.
6. Per rimuovere tag aggiuntivi dalla risorsa, ripeti il passaggio precedente per ogni tag aggiuntivo da rimuovere.
7. Quando hai finito di rimuovere i tag, scegli Salva.

API

Per rimuovere uno o più tag da una risorsa a livello di codice, utilizza il UntagResourcefunzionamento dell'API Security Lake. Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa da cui rimuovere un tag. Usa il `tagKeys` parametro per specificare la chiave del tag da rimuovere. Per rimuovere più tag, aggiungete il `tagKeys` parametro e l'argomento per ogni tag da rimuovere, separati da una e commerciale (&), ad esempio. `tagKeys=key1&tagKeys=key2` Per rimuovere solo un valore di tag specifico (non una chiave di tag) da una risorsa, modifica il tag anziché rimuovere il tag.

Se stai usando il AWS Command Line Interface (AWS CLI), esegui il comando untag-resource per rimuovere uno o più tag da una risorsa. Per il `resource-arn` parametro, specificate l'ARN della risorsa da cui rimuovere un tag. Utilizzate il `tag-keys` parametro per specificare la chiave del tag da rimuovere. Ad esempio, il comando seguente rimuove il `Environment` tag (sia la chiave del tag che il valore del tag) dal sottoscrittore specificato:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

Dove `resource-arn` specifica l'ARN del sottoscrittore da cui rimuovere un tag *`Environment`* ed è la chiave del tag da rimuovere.

Per rimuovere più tag da una risorsa, aggiungi ogni chiave di tag aggiuntiva come argomento per il parametro. `tag-keys` Per esempio:

```
$ aws securitylake untag-resource \
```

```
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

Se l'operazione ha esito positivo, Security Lake restituisce una risposta HTTP 200 vuota. Altrimenti, Security Lake restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Risoluzione dei problemi di Amazon Security Lake

Consulta i seguenti argomenti se riscontri problemi durante l'utilizzo di Security Lake.

Risoluzione dei problemi relativi allo stato del data lake

La pagina Problemi della console Security Lake mostra un riepilogo dei problemi che riguardano il data lake. Ad esempio, Security Lake non può abilitare la raccolta dei log per gli eventi di AWS CloudTrail gestione se non hai creato un CloudTrail trail per la tua organizzazione. La pagina Problemi riporta i problemi che si sono verificati negli ultimi 14 giorni. È possibile visualizzare una descrizione di ogni problema e le procedure di risoluzione suggerite.

Per accedere a livello di codice a un riepilogo dei problemi, puoi utilizzare il ListDataLakeExceptionsfunzionamento dell'API Security Lake. Se stai usando AWS CLI, esegui il comando. list-data-lake-exceptions Per il `regions` parametro, puoi specificare uno o più codici regionali, ad esempio per la regione Stati Uniti orientali (Virginia settentrionale), `us-east-1` per visualizzare i problemi che riguardano tali regioni. Se non si include il `regions` parametro, vengono restituiti problemi che riguardano tutte le regioni. Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.

Ad esempio, il AWS CLI comando seguente elenca i problemi che riguardano le `eu-west-3` regioni `us-east-1` and. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securitylake list-data-lake-exceptions \
--regions "us-east-1" "eu-west-3"
```

Per notificare a un utente di Security Lake un problema o un errore, utilizzate il CreateDataLakeExceptionSubscriptionfunzionamento dell'API Security Lake. L'utente può ricevere notifiche tramite e-mail, consegna a una coda Amazon Simple Queue Service (Amazon SQS), consegna a AWS Lambda una funzione o un altro protocollo supportato.

Ad esempio, il AWS CLI comando seguente invia notifiche relative alle eccezioni di Security Lake all'account specificato tramite invio di SMS. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securitylake create-data-lake-exception-subscription \
```

```
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

Per visualizzare i dettagli sulla sottoscrizione di un'eccezione, è possibile utilizzare l'GetDataLakeExceptionSubscriptionoperazione. Per aggiornare una sottoscrizione ad eccezione, è possibile utilizzare l'UpdateDataLakeExceptionSubscriptionoperazione. Per eliminare una sottoscrizione di eccezione e interrompere le notifiche, è possibile utilizzare l'DeleteDataLakeExceptionSubscriptionoperazione.

Risoluzione dei problemi relativi a Lake Formation

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Security Lake e AWS Lake Formation database o tabelle. Per ulteriori argomenti sulla risoluzione dei problemi di Lake Formation, consulta la sezione Risoluzione dei problemi della Guida per gli AWS Lake Formation sviluppatori.

Tabella non trovata

Potresti ricevere questo errore quando tenti di creare un abbonato.

Per risolvere questo errore, assicurati di aver già aggiunto fonti nella regione. Se hai aggiunto fonti quando il servizio Security Lake era in versione di anteprima, devi aggiungerle nuovamente prima di creare un abbonato. Per ulteriori informazioni sull'aggiunta di fonti, consultaGestione del codice in Amazon Security Lake.

400 AccessDenied

Potresti ricevere questo errore quando aggiungi una fonte personalizzata e chiami l'`CreateCustomLogSource`API.

Per risolvere l'errore, controlla le tue autorizzazioni di Lake Formation. Il ruolo IAM che chiama l'API deve disporre delle autorizzazioni Create table per il database Security Lake. Per ulteriori informazioni, consulta Concessione delle autorizzazioni del database utilizzando la console Lake Formation e il metodo named resource nella AWS Lake Formation Developer Guide.

SYNTAX_ERROR: riga 1:8: SELECT * non consentita dalla relazione che non ha colonne

Potresti ricevere questo errore quando esegui una query su una tabella di origine per la prima volta in Lake Formation.

Per risolvere l'errore, concedi l'`SELECT`autorizzazione al ruolo IAM che stai utilizzando quando hai effettuato l'accesso al tuo Account AWS. Per istruzioni su come concedere l'`SELECT`autorizzazione, consulta Concessione delle autorizzazioni alla tabella utilizzando la console Lake Formation e il metodo della risorsa denominata nella AWS Lake Formation Developer Guide.

Security Lake non è riuscito ad aggiungere l'ARN principale del chiamante all'amministratore del data lake di Lake Formation. Gli attuali amministratori di data lake possono includere principi non validi che non esistono più.

Potresti ricevere questo errore quando abiliti Security Lake o ne aggiungi una Servizio AWS come fonte di registro.

Per risolvere l'errore, procedi nel seguente modo:

1. Aprire la console Lake Formation all'indirizzo https://console.aws.amazon.com/lakeformation/.
2. Accedi come utente amministrativo.
3. Nel riquadro di navigazione, in Autorizzazioni, scegli Ruoli e attività amministrative.
4. Nella sezione Amministratori di Data lake, scegli Scegli amministratori.
5. Cancella i principali etichettati come Non trovati in IAM, quindi scegli Salva.
6. Prova di nuovo a eseguire l'operazione Security Lake.

Security Lake CreateSubscriber with Lake Formation non ha creato un nuovo invito alla condivisione di risorse RAM da accettare

Potresti visualizzare questo errore se hai condiviso risorse con la condivisione di dati tra account Lake Formation versione 2 o versione 3 prima di creare un abbonato Lake Formation in Security Lake. Questo perché la condivisione tra account di Lake Formation versione 2 e versione 3 ottimizza il numero di condivisioni di risorse AWS RAM mappando più concessioni di autorizzazioni tra account con una condivisione di risorse RAM. AWS

Assicurati di verificare che il nome della condivisione di risorse abbia l'ID esterno specificato durante la creazione del sottoscrittore e che l'ARN della condivisione di risorse corrisponda all'ARN nella risposta. `CreateSubscriber`

Risoluzione dei problemi relativi alle interrogazioni in Amazon Athena

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando usi Athena per interrogare gli oggetti archiviati nel tuo bucket Security Lake S3. Per ulteriori argomenti sulla risoluzione dei problemi di Athena, consulta la sezione Risoluzione dei problemi in Athena della Guida per l'utente di Amazon Athena.

L'interrogazione non restituisce nuovi oggetti nel data lake

La tua query Athena potrebbe non restituire nuovi oggetti nel tuo data lake anche se il bucket S3 per Security Lake contiene tali oggetti. Ciò può verificarsi se hai disabilitato Security Lake e poi lo hai riabilitato. Di conseguenza, le AWS Glue partizioni potrebbero non registrare correttamente i nuovi oggetti.

Per risolvere l'errore, procedi nel seguente modo:

1. Apri la AWS Lambda console all'indirizzo https://console.aws.amazon.com/lambda/.
2. Dalla barra di navigazione, nel selettore Regioni, scegli la regione in cui Security Lake è abilitato ma la query Athena non restituisce risultati.
3. *Dal riquadro di navigazione, scegliete* ***Funzioni*** *e selezionate la funzione* ***SecurityLake_Glue_Partition_Updater_Lambda_*** *region>.*
4. Nella scheda Configurazioni, scegli Trigger.
5. Seleziona l'opzione accanto alla funzione e scegli Modifica.
6. Seleziona Attiva trigger e scegli Salva. Questo trasformerà lo stato della funzione in Attivato.

Impossibile accedere alle AWS Glue tabelle

Un abbonato all'accesso alle query potrebbe non essere in grado di accedere alle AWS Glue tabelle che contengono dati di Security Lake.

Innanzitutto, assicurati di aver seguito i passaggi descritti in. Configurazione della condivisione delle tabelle tra account (fase di sottoscrizione)

Se l'abbonato non ha ancora accesso, segui questi passaggi:

1. Apri la AWS Glue console all'indirizzo https://console.aws.amazon.com/glue/.
2. Dal pannello di navigazione, scegli Impostazioni Data Catalog e Catalog.
3. Autorizza l'abbonato ad accedere alle AWS Glue tabelle con una politica basata sulle risorse. Per informazioni sulla creazione di politiche basate sulle risorse, consulta Esempi di policy basate sulle risorse nella Guida per gli sviluppatori. AWS Glue AWS Glue

Risoluzione dei problemi di Organizations

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Security Lake e AWS Organizations. Per ulteriori argomenti sulla risoluzione dei problemi di Organizations, consulta la sezione Risoluzione dei problemi della Guida per AWS Organizations l'utente.

Si è verificato un errore di accesso negato durante la chiamata dell' CreateDataLake operazione: l'account deve essere l'account amministratore delegato di un'organizzazione o un account autonomo.

Potresti ricevere questo errore se elimini l'organizzazione a cui apparteneva un account amministratore delegato e poi provi a utilizzare quell'account per configurare Security Lake utilizzando la console di Security Lake o l'API. CreateDataLake

Per risolvere l'errore, utilizza un account amministratore delegato di un'organizzazione diversa o un account autonomo.

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Security Lake

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Security Lake e IAM.

Non sono autorizzato a eseguire un'azione in Security Lake

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona che ti ha fornito le credenziali.

Il seguente errore di esempio si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli di un file fittizio *`subscriber`* ma non dispone delle autorizzazioni fittizie. `SecurityLake:`*`GetSubscriber`*

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le sue politiche per consentirgli di accedere alle informazioni utilizzando l'azione. *`subscriber`* `SecurityLake:`*`GetSubscriber`*

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Security Lake.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Security Lake. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse di Security Lake

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Security Lake supporta queste funzionalità, consultaCome funziona Amazon Security Lake con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Come vengono determinati i prezzi di Security Lake

I prezzi di Amazon Security Lake si basano su due dimensioni: l'ingestione e la conversione dei dati. Security Lake funziona anche con altriServizi AWSper archiviare e condividere i tuoi dati e potresti incorrere in costi separati per queste attività.

Quando si attiva la raccolta dei registri per la prima volta in unAccount AWSin qualsiasiRegione AWSsupportato da Security Lake, quell'account viene automaticamente registrato a una prova gratuita di 15 giorni di Security Lake. Durante la prova gratuita potresti comunque incorrere in addebiti derivanti da altri servizi.

Inserimento dei dati

Questi costi derivano dal volume di dati ingeritiAWS CloudTrailregistri e altroServizio AWSlog ed eventi (log di query su Amazon Route 53),AWS Security Hubrisultati e Amazon VPC Flow Logs).

Conversione dei dati

Questi costi derivano dal volume diServizio AWSregistri ed eventi a cui Security Lake si normalizzaOpen Cybersecurity Schema Framework (OCSF)schema e converte in formato Apache Parquet.

Costi dei servizi correlati

Ecco alcuni costi che potresti dover sostenere rispetto ad altriServizi AWSper archiviare e condividere i dati nel tuo data lake di sicurezza:

- Amazon S3: questi costi derivano dalla manutenzione dei bucket Amazon S3 nel tuo account Security Lake, dall'archiviazione dei dati lì e dalla valutazione e dal monitoraggio del bucket per la sicurezza e il controllo degli accessi. Per ulteriori informazioni, consulta i Prezzi di Amazon S3.
- Amazon SQS: questi costi derivano dalla creazione di una coda Amazon SQS per la consegna dei messaggi. Per ulteriori informazioni, consulta la paginaPrezzi Amazon SQS.
- Amazon EventBridge — Questi costi provengono da Amazon EventBridge invio di notifiche relative agli oggetti agli endpoint dell'abbonamento. Per ulteriori informazioni, consulta la paginaAmazon EventBridgeprezzi.

I costi sostenuti da un abbonato per l'interrogazione dei dati da Security Lake e l'archiviazione dei risultati delle query sono a carico dell'abbonato.

Per ulteriori informazioni, consulta la paginaPrezzi di Security Lake.

Analisi dell'utilizzo di Security Lake e dei costi stimati

IlUtilizzola pagina della console Amazon Security Lake consente di esaminare l'utilizzo corrente di Security Lake, nonché l'utilizzo futuro e le stime dei costi. Se stai attualmente partecipando a una prova gratuita di 15 giorni, l'utilizzo durante il periodo di prova può aiutarti a stimare i costi per l'utilizzo di Security Lake al termine del periodo di prova gratuito. Per una panoramica dei prezzi di Security Lake, vediCome vengono determinati i prezzi di Security Lake. Per informazioni dettagliate ed esempi di costi, vederePrezzi di Amazon Security Lake.

In Security Lake, i costi di utilizzo stimati sono riportati in dollari USA e si applicano solo agli attualiRegione AWS. I costi coprono l'utilizzo di Security Lake da parte di tutti gli account dell'organizzazione e includono la conversione al formato Open Cybersecurity Schema Framework (OCSF) e Apache Parquet. Tuttavia, i costi previsti non includono i costi per altri servizi con cui collabora Security Lake, come Amazon Simple Storage Service (Amazon S3) eAWS Glue.

SulUtilizzopagina, scegli un periodo di tempo per il quale visualizzare i dati sull'utilizzo e sui costi. Il periodo di tempo predefinito è l'ultimo giorno di calendario. È necessario disporre di almeno 1 giorno di utilizzo di Security Lake per visualizzare le proiezioni dei costi.

La parte superiore della pagina mostra ilCosto previsto per tutti gli account. Questo è il costo di Security Lake previsto al momentoRegione AWSper i prossimi 30 giorni di calendario in base all'utilizzo effettivo durante il periodo di tempo selezionato. L'utilizzo effettivo e il costo previsto si riferiscono a tutti gli account dell'organizzazione.

Nel resto della pagina, i dati sull'utilizzo e sui costi sono suddivisi nelle due tabelle seguenti:

- Utilizzo e costo per fonte— Questo è l'utilizzo corrente di Security Lake suddiviso per origine dati, nonché l'utilizzo e i costi stimati per i prossimi 30 giorni di calendario in base all'utilizzo effettivo durante il periodo di tempo selezionato. L'utilizzo effettivo, l'utilizzo previsto e il costo previsto riflettono tutti gli account dell'organizzazione. Se si seleziona una fonte, si apre un pannello diviso che mostra quali account hanno generato log ed eventi da quella fonte. Per ogni account, il pannello diviso include sia l'utilizzo effettivo da quella fonte sia l'utilizzo e i costi previsti.
- Utilizzo e costo per account— Questo è l'utilizzo corrente di Security Lake suddiviso per account, nonché l'utilizzo e i costi stimati per i prossimi 30 giorni di calendario in base all'utilizzo effettivo durante il periodo di tempo selezionato. Se si seleziona un account, si apre un pannello diviso che mostra le fonti che hanno contribuito all'utilizzo di quell'account. Per ogni fonte che contribuisce, il pannello diviso include sia l'utilizzo effettivo che l'utilizzo e i costi previsti.

Tutto supportatoAWSle origini dati vengono visualizzate nelle tabelle precedenti, anche se non è stata aggiunta una fonte particolare in Security Lake. Ti consigliamo di aggiungere tuttoAWSfonti (se stai partecipando alla prova gratuita) per ottenere stime dei costi per il set completo di log ed eventi. Per istruzioni sull'aggiunta di unAWSfonte, vediRaccolta di dati dai AWS servizi. Le fonti personalizzate non sono incluse nei calcoli dell'utilizzo o dei costi.

Segui questi passaggi per esaminare i dati sull'utilizzo e sui costi nella console di Security Lake.

Per esaminare l'utilizzo di Security Lake e i costi previsti (console)

1. Apri la console Security Lake all'indirizzohttps://console.aws.amazon.com/securitylake/.
2. Usando ilRegione AWSselettore nell'angolo in alto a destra della pagina, seleziona la regione in cui desideri l'utilizzo e i costi.
3. Nel riquadro di navigazione, sceglilmpostazionie poiutilizzo.
4. Seleziona il periodo di tempo per il quale desideri visualizzare i dati su utilizzo e costi. L'impostazione predefinita è l'ultimo giorno.
5. SelezionaPer fonte di datioPer accountscheda per esaminare in dettaglio l'utilizzo e i costi.

Regioni ed endpoint Amazon Security Lake Lake Lake

Per un elenco delle regioni e degli endpoint di servizio supportati per Security Lake, consulta gli endpoint Amazon Security Lake nel Riferimenti generali di AWS.

Si consiglia di abilitare Security Lake LakeRegioni AWS. Ciò ti consente di utilizzare Security Lake per rilevare e indagare su attività non autorizzate o insolite anche nelle regioni che non stai utilizzando attivamente.

Disattivazione di Amazon Security Lake

Quando disabiliti Amazon Security Lake, Security Lake interrompe la raccolta di log ed eventi dalle tue AWS fonti. Le impostazioni esistenti di Security Lake e le risorse create nel tuo Account AWS vengono mantenute. Inoltre, i dati archiviati o pubblicati su altri Servizi AWS, come i dati sensibili nelle AWS Lake Formation tabelle e nei AWS CloudTrail registri, rimangono disponibili. I dati archiviati nel bucket Amazon Simple Storage Service (Amazon S3) rimangono disponibili in base al ciclo di vita dello storage Amazon S3.

La disabilitazione di Security Lake dalla pagina Impostazioni della console di Security Lake interrompe la raccolta di AWS log ed eventi in tutti Regioni AWS gli ambienti in cui Security Lake è attualmente abilitato. È possibile utilizzare la pagina Regioni sulla console per interrompere la raccolta dei registri in regioni specifiche. L'API Security Lake AWS CLI può anche interrompere la raccolta dei log nelle regioni specificate nella richiesta.

Se utilizzi l'integrazione con AWS Organizations e il tuo account fa parte di un'organizzazione che gestisce centralmente più account Security Lake, solo l'amministratore delegato di Security Lake può disabilitare Security Lake per sé e per gli account dei membri. Tuttavia, l'abbandono di un'organizzazione interrompe la raccolta dei log per un account membro.

Quando si disabilita Security Lake per un'organizzazione, la designazione di amministratore delegato viene mantenuta se si seguono le istruzioni di disabilitazione fornite in questa pagina. Non è necessario designare nuovamente l'amministratore delegato prima di poter riattivare Security Lake.

Per le sorgenti personalizzate, quando si disattiva Security Lake, è necessario disabilitare ogni fonte al di fuori della console di Security Lake. La mancata disabilitazione di un'integrazione comporterà che le integrazioni di origine continuino a inviare i log in Amazon S3. Inoltre, è necessario disabilitare l'integrazione dell'abbonato o l'abbonato sarà comunque in grado di utilizzare i dati di Security Lake. Per i dettagli su come rimuovere un'origine personalizzata o un'integrazione con un abbonato, consulta la documentazione del rispettivo provider.

Questo argomento spiega come disabilitare Security Lake utilizzando la console di Security Lake, l'API Security Lake o AWS CLI.

Console

1. Aprire la console Security Lake all'indirizzo https://console.aws.amazon.com/securitylake/.
2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere General (Generali).

3. Scegli Disabilita Security Lake.
4. Quando viene richiesta la conferma, immettete**`Disable`**, quindi scegliete Disabilita.

API

Per disabilitare Security Lake a livello di codice, utilizza il DeleteDataLakefunzionamento dell'API Security Lake. Se stai usando AWS CLI, esegui il comando. delete-date-lake Nella richiesta, utilizza l'`regions`elenco per specificare il codice regionale per ogni regione in cui desideri disabilitare Security Lake. Per un elenco dei codici regionali, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.

Per una distribuzione di Security Lake che utilizza AWS Organizations, solo l'amministratore delegato di Security Lake dell'organizzazione può disabilitare Security Lake per gli account dell'organizzazione.

Ad esempio, il AWS CLI comando seguente disabilita Security Lake nelle regioni and. `ap-northeast-1` `eu-central-1` Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

Cronologia dei documenti per la Guida per l'utente di Amazon Security Lake

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione di Amazon Security Lake. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Ultimo aggiornamento della documentazione: 29 febbraio 2024

Modifica	Descrizione	Data
Nuove versioni sorgenti	Aggiorna le autorizzazioni del ruolo per importare dati dalle nuove versioni delle fonti di dati.	29 febbraio 2024
Nuova fonte di registro AWS	Security Lake ha aggiunto EKS Audit Logs come fonte di AWS registro. I registri di controllo EKS ti aiutano a rilevare attività potenzialmente sospette nei tuoi cluster EKS all'interno di Amazon Elastic Kubernetes Service.	29 febbraio 2024
Aggiornamento alla politica gestita esistente	Security Lake ha aggiornato la policy per consentire `iam:PassRole` il nuovo `AmazonSecurityLakeMetastoreManagerV2` ruolo e consente a Security Lake di implementare o aggiornare i componenti del data lake.	23 febbraio 2024
Nuova politica gestita	Security Lake ha aggiunto una nuova policy AWS gestita,	23 gennaio 2024

	la `AmazonSecurityLake MetastoreManager` policy. Questa politica concede a Security Lake le autorizzazioni per gestire i metadati nel data lake.	
Disponibilità regionale	Security Lake è ora disponibile nei seguenti paesi Regioni AWS: Asia Pacifico (Osaka), Canada (Centrale), Europa (Parigi) ed Europa (Stoccolma). Per un elenco completo delle regioni in cui Security Lake è attualmente disponibile, consulta gli endpoint di Amazon Security Lake nel Riferimenti generali di AWS.	26 ottobre 2023
Nuove funzionalità	Ora puoi modificare determinate impostazioni per gli abbonati con accesso tramite query. Puoi anche assegnare tag alle risorse di Security Lake per te. Account AWS	20 luglio 2023
Nuova politica gestita	Security Lake ha aggiunto una nuova policy AWS gestita, la `AmazonSecurityLake Administrator` policy. Questa politica concede autorizzazioni amministrative che consentono l'accesso completo e principale a tutte le azioni di Security Lake.	30 maggio 2023

Disponibilità generale	Security Lake è ora disponibile a tutti.	30 maggio 2023
Nuova caratteristica	Security Lake ora invia i parametri ad Amazon CloudWatch.	4 maggio 2023
Disponibilità regionale	Security Lake è ora disponibile nei seguenti paesi Regioni AWS: Asia Pacifico (Singapore), Europa (Londra) e Sud America (San Paolo).	22 marzo 2023
Nuova caratteristica	Security Lake ora crea ruoli AWS Identity and Access Management (IAM) per conto dell'utente quando si utilizza la console Security Lake per abilitare e iniziare a utilizzare Security Lake.	15 febbraio 2023
Versione iniziale	Questa è la versione iniziale della Amazon Security Lake User Guide.	29 novembre 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.