aws

Guide de l’utilisateur

Amazon Security Lake

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Security Lake: Guide de l’utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'Amazon Security Lake ?

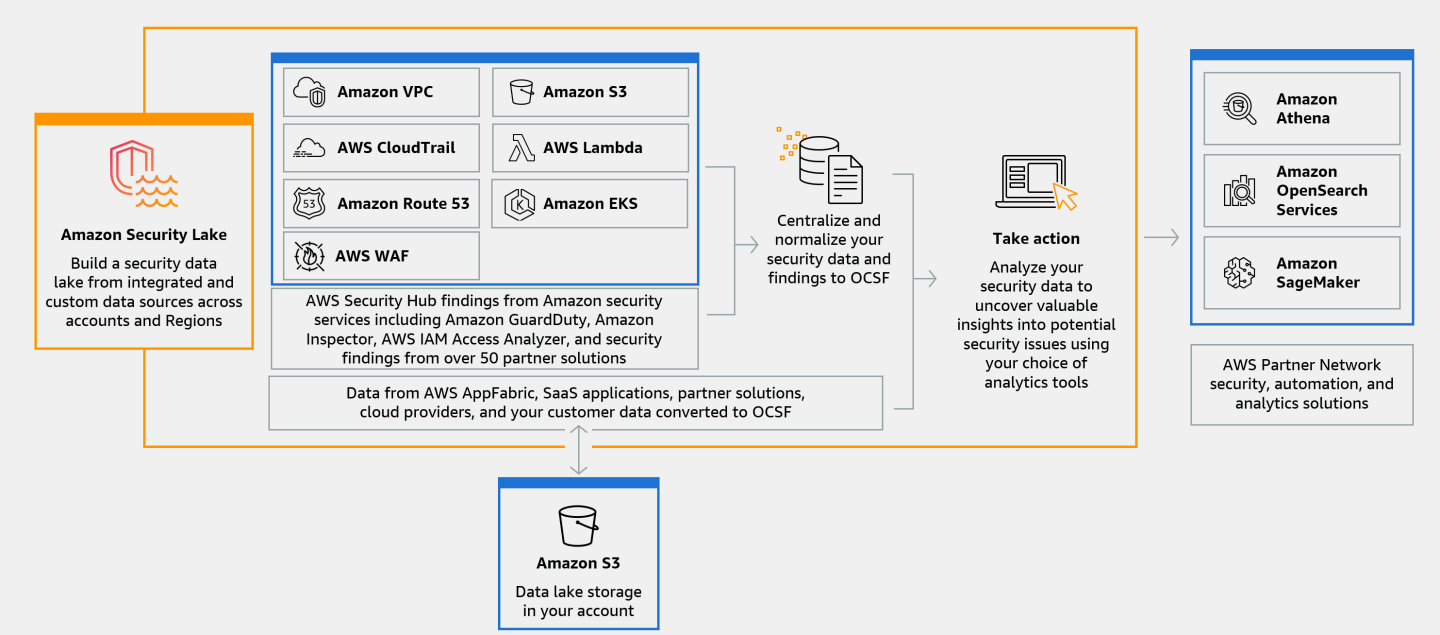
Amazon Security Lake est un service de lac de données de sécurité entièrement géré. Vous pouvez utiliser Security Lake pour centraliser automatiquement les données de sécurité provenant d' AWS environnements, de fournisseurs de SaaS, de sources sur site, de sources cloud et de sources tierces dans un lac de données spécialement conçu et stocké dans votre. Compte AWS Security Lake vous aide à analyser les données de sécurité, afin que vous puissiez mieux comprendre votre posture de sécurité dans l'ensemble de l'entreprise. Avec Security Lake, vous pouvez également améliorer la protection des charges de travail, des applications et des données.

Le lac de données est soutenu par des compartiments Amazon Simple Storage Service (Amazon S3), et vous restez propriétaire de vos données.

Security Lake automatise la collecte des données relatives aux journaux et aux événements liés à la sécurité à partir de services intégrés AWS services et tiers. Il vous aide également à gérer le cycle de vie des données grâce à des paramètres de rétention et de réplication personnalisables. Security Lake convertit les données ingérées au format Apache Parquet et en un schéma open source standard appelé Open Cybersecurity Schema Framework (OCSF). Grâce au support OCSF, Security Lake normalise et combine les données de sécurité issues d' AWS un large éventail de sources de données de sécurité d'entreprise.

AWS services D'autres services tiers peuvent s'abonner aux données stockées dans Security Lake à des fins de réponse aux incidents et d'analyse des données de sécurité.

Présentation de Security Lake



Caractéristiques de Security Lake

Voici quelques-unes des principales méthodes utilisées par Security Lake pour vous aider à centraliser, à gérer et à vous abonner aux données des journaux et des événements liés à la sécurité.

Agrégation des données dans votre compte

Security Lake crée un lac de données de sécurité spécialement conçu dans votre compte. Security Lake collecte les données des journaux et des événements à partir du cloud, sur site et de sources de données personnalisées pour tous les comptes et régions. Le lac de données est soutenu par des compartiments Amazon Simple Storage Service (Amazon S3), et vous restez propriétaire de vos données.

Diverses sources de journaux et d'événements prises en charge

Security Lake collecte les journaux et les événements de sécurité provenant de sources multiples, y compris des services locaux et tiers. AWS services Après avoir ingéré les journaux, quelle que soit leur source, vous pouvez y accéder de manière centralisée et gérer leur cycle de vie. Pour plus de détails sur les sources à partir desquelles les journaux et les événements sont collectés

par Security Lake, voir gestion des sources dans Amazon Security Security Security Security Security Security Security Security Security

Transformation et normalisation des données

Security Lake partitionne automatiquement les données entrantes prises en charge de manière native AWS services et les convertit en un format Parquet efficace en termes de stockage et de requêtes. Il transforme également les données prises en charge de manière native AWS services vers le schéma open source Open Cybersecurity Schema Framework (OCSF). Cela rend les données compatibles avec celles d'autres AWS services fournisseurs tiers sans qu'il soit nécessaire de les traiter ultérieurement. Dans la mesure où Security Lake normalise les données, de nombreuses solutions de sécurité peuvent utiliser ces données en parallèle.

Plusieurs niveaux d'accès pour les abonnés

Les abonnés consomment les données stockées dans Security Lake. Vous pouvez choisir le niveau d'accès de l'abonné à vos données. Les abonnés ne peuvent consommer des données qu'à partir des sources et dans le Régions AWS, que vous spécifiez. Les abonnés peuvent être automatiquement avertis des nouveaux objets lorsqu'ils sont écrits dans le lac de données. Les abonnés peuvent également interroger les données du lac de données. Security Lake crée et échange automatiquement les informations d'identification nécessaires entre Security Lake et l'abonné.

Gestion des données multicomptes et multirégions

Vous pouvez activer Security Lake de manière centralisée dans toutes les régions où il est disponible, et dans plusieurs d'entre elles Comptes AWS. Dans Security Lake, vous pouvez également désigner des régions cumulatives pour consolider les données des journaux de sécurité et des événements provenant de plusieurs régions. Cela peut vous aider à respecter les exigences de conformité en matière de résidence des données.

Configurable et personnalisable

Security Lake est un service configurable et personnalisable. Vous pouvez spécifier les sources, les comptes et les régions pour lesquels vous souhaitez configurer la collecte de journaux. Vous pouvez également spécifier le niveau d'accès d'un abonné au lac de données.

Gestion et optimisation du cycle de vie des données

Security Lake gère le cycle de vie de vos données à l'aide de paramètres de conservation et de coûts de stockage personnalisables grâce à une hiérarchisation automatique du stockage. Security Lake partitionne et convertit automatiquement les données de sécurité entrantes en un format Apache Parquet efficace pour le stockage et les requêtes.

Accès à Security Lake

Pour obtenir la liste des régions dans lesquelles Security Lake est actuellement disponible, consultezAmazon Security Security Security Security Security Security Security Security Security Security Security Security Security Security. Pour en savoir plus sur les régions, consultez la section Points AWS de terminaison de service dans le Références générales AWS.

Dans chaque région, vous pouvez accéder à Security Lake de l'une des manières suivantes :

AWS Management Console

AWS Management Console Il s'agit d'une interface basée sur un navigateur que vous pouvez utiliser pour créer et gérer AWS des ressources. La console Security Lake permet d'accéder à votre compte et à vos ressources Security Lake. Vous pouvez effectuer la plupart des tâches de Security Lake à l'aide de la console Security Lake.

API Security Lake

Pour accéder à Security Lake par programmation, utilisez l'API Security Lake et envoyez des requêtes HTTPS directement au service. Pour plus d'informations, consultez le document de référence de l'API Security Lake.

AWS Command Line Interface (AWS CLI)

Avec le AWS CLI, vous pouvez émettre des commandes sur la ligne de commande de votre système pour effectuer des tâches et AWS des tâches de Security Lake. L'utilisation de la ligne de commande peut être plus rapide et plus pratique que celle de la console. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts exécutant des tâches . Pour plus d'informations sur l'installation et l'utilisation du AWS CLI, consultez le AWS Command Line Interface.

AWS SDK

AWS fournit des SDK composés de bibliothèques et d'exemples de code pour divers langages de programmation et plateformes, tels que Java, Go, Python, C++ et .NET. Les SDK fournissent un accès pratique et programmatique à Security Lake et à d'autres. AWS services Ils gèrent également des tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur l'installation et l'utilisation des AWS SDK, consultez la section Outils sur AWS lesquels vous pouvez vous appuyer.

Services connexes

Security Lake utilise également AWS services les autres éléments suivants :

- Amazon EventBridge — Security Lake est utilisé EventBridge pour avertir les abonnés lorsque des objets sont écrits dans le lac de données.
- AWS Glue— Security Lake utilise des AWS Glue robots d'exploration pour créer les AWS Glue Data Catalog tables et envoyer les données nouvellement écrites au catalogue de données. Security Lake stocke également les métadonnées de partition pour AWS Lake Formation les tables du catalogue de données.
- AWS Lake Formation— Security Lake crée une table Lake Formation distincte pour chaque source qui fournit des données à Security Lake. Les tables Lake Formation contiennent des informations sur les données de chaque source, notamment des informations sur le schéma, la partition et l'emplacement des données. Les abonnés ont la possibilité de consommer des données en interrogeant les tables de Lake Formation.
- AWS Lambda— Security Lake utilise les fonctions Lambda pour prendre en charge les tâches d'extraction, de transformation et de chargement (ETL) sur des données brutes et pour enregistrer des partitions pour les données sources. AWS Glue
- Amazon S3 — Security Lake stocke vos données sous forme d'objets Amazon S3. Les classes de stockage et les paramètres de rétention sont basés sur les offres Amazon S3. Security Lake ne prend pas en charge Amazon S3 Select.

Security Lake collecte des données à partir de sources personnalisées en plus des éléments suivants AWS services :

- AWS CloudTrail événements de gestion et de données (S3, Lambda)
- Journaux d'audit Amazon Elastic Kubernetes Service (Amazon EKS)
- Journaux de requête Amazon Route 53 Resolver
- AWS Security Hub résultats
- Journaux de flux Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF Journaux v2

Pour plus d'informations sur ces sources, consultezCollecte de données auprès de AWS services. Vous pouvez consommer les objets Amazon S3 de votre lac de données de sécurité en créant un abonné capable de lire les données du schéma OCSF. Vous pouvez également interroger des

données à l'aide d'Amazon Athena, d'Amazon Redshift et de services d'abonnement tiers intégrés à. AWS Glue

Concepts et terminologie

Cette section décrit les principaux concepts et termes qui vous aideront à utiliser Amazon Security Lake.

Région contributrice

Un ou plusieursRégions AWS qui fournissent des données à une région cumulée.

Data lake

Vos données qui sont stockés dans Amazon Simple Storage Service (Amazon S3) et gérées par Security Security LakeAWS Glue l'utilise pour envoyer les données nouvellement écrites au catalogue de données. Security Lake crée également uneAWS Lake Formation table pour chaque source qui fournit des données au lac de données. Un lac de données stocke généralement les éléments suivants :

- Données structurées et non structurées
- Données brutes et transformées

Security Lake est un service de lac de données conçu pour collecter des journaux et des événements liés à la sécurité.

Cadre de schéma de cybersécurité ouvert (OCSF)

Schéma open source standardisé pour les journaux et les événements de sécurité. Il a été développé parAWS et d'autres leaders du secteur de la sécurité dans divers domaines de sécurité. Security Lake convertit automatiquement les journaux et les événements qu'il collecteAWS services dans le schéma OCSF. Les sources personnalisées convertissent leurs journaux et événements en OCSF avant de les envoyer à Security Lake.

Région cumulée

EtRégion AWS qui consolide les journaux de sécurité et les événements d'une ou de plusieurs régions contributrices. La spécification d'une ou de plusieurs régions cumulatives peut vous aider à vous conformer aux exigences de conformité régionales.

Source

Ensemble de journaux et d'événements générés à partir d'un système unique qui correspond à une classe d'événements spécifique dans OCSF. Security Une source peut être un autre

serviceAWS service ou un service tiers. Pour les sources tierces, vous devez convertir les données vers le schéma OCSF avant de les envoyer à Security Lake.

Subscriber

Service qui utilise les journaux et les événements de Security Lake. Un abonné peut être un autre serviceAWS service ou un service tiers.

Commencer à utiliser Amazon Security Lake

Cette section explique comment activer et commencer à utiliser Security Lake. Vous allez apprendre à configurer les paramètres de votre lac de données et à configurer la collecte de journaux. Vous pouvez activer et utiliser Security Lake via AWS Management Console ou par programmation. Quelle que soit la méthode utilisée, vous devez d'abord configurer un Compte AWS et un utilisateur administratif. Les étapes suivantes varient en fonction de la méthode d'accès. La console Security Lake propose un processus de démarrage rationalisé et crée tous les rôles nécessaires AWS Identity and Access Management (IAM) dont vous avez besoin pour créer votre lac de données.

> **Important**
>
> Security Lake ne prend pas en charge le remblayage des événements de source de log AWS bruts existants qui ont été générés avant l'activation de Security Lake.

Compte AWS Configuration initiale

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des AWS services et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

   Pour obtenir des instructions, voir Activer un MFA périphérique virtuel pour votre utilisateur Compte AWS root (console) dans le guide de IAM l'utilisateur.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URLidentifiant envoyé à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAMIdentity Center, consultez la section Connexion au portail AWS d'accès dans le guide de Connexion à AWS l'utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme à la meilleure pratique consistant à appliquer les autorisations du moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Identifiez le compte que vous utiliserez pour activer Security Lake

Security Lake s'intègre AWS Organizations pour gérer la collecte de journaux sur plusieurs comptes d'une organisation. Si vous souhaitez utiliser Security Lake pour une organisation, vous devez utiliser votre compte de gestion Organizations pour désigner un administrateur délégué de Security Lake. Vous devez ensuite utiliser les informations d'identification de l'administrateur délégué pour activer Security Lake, ajouter des comptes membres et activer Security Lake pour eux. Pour de plus amples informations, veuillez consulter Gérer plusieurs comptes avec AWS Organizations.

Vous pouvez également utiliser Security Lake sans l'intégration Organizations pour un compte autonome ne faisant pas partie d'une organisation.

Considérations relatives à l'activation d'Amazon Security Lake

Avant d'activer Security Lake, tenez compte des points suivants :

- Security Lake fournit des fonctionnalités de gestion interrégionales, ce qui signifie que vous pouvez créer votre lac de données et configurer la collecte de journaux dans Régions AWS celui-ci. Pour activer Security Lake dans toutes les régions prises en charge, vous pouvez choisir n'importe

quel point de terminaison régional pris en charge. Vous pouvez également ajouter des régions cumulatives pour agréger les données de plusieurs régions dans une seule région.

- Nous vous recommandons d'activer Security Lake dans tous les modèles pris en charge Régions AWS. Dans ce cas, Security Lake peut collecter des données liées à des activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement. Si Security Lake n'est pas activé dans toutes les régions prises en charge, sa capacité à collecter des données auprès d'autres services que vous utilisez dans plusieurs régions est réduite.
- Lorsque vous activez Security Lake pour la première fois dans une région, un rôle lié à un service est créé pour le compte que vous avez appelé. `AWSServiceRoleForSecurityLake` Ce rôle inclut les autorisations d'appeler d'autres personnes AWS services en votre nom et d'exploiter le lac de données de sécurité. Pour plus d'informations sur le fonctionnement des rôles liés à un service, consultez la section Utilisation des rôles liés à un service dans le Guide de l'utilisateur. IAM Si vous activez Security Lake en tant qu'administrateur délégué de Security Lake, Security Lake crée le rôle lié au service dans chaque compte membre de l'organisation.
- Security Lake ne prend pas en charge Amazon S3 Object Lock. Lorsque les compartiments du lac de données sont créés, S3 Object Lock est désactivé par défaut. L'activation du verrouillage d'objets sur un bucket interrompt la transmission des données de journal normalisées au lac de données.

Commencer à utiliser la console

Ce didacticiel explique comment activer et configurer Security Lake via le AWS Management Console. Dans le cadre de AWS Management Console, la console Security Lake propose un processus de démarrage rationalisé et crée tous les rôles nécessaires AWS Identity and Access Management (IAM) dont vous avez besoin pour créer votre lac de données.

Étape 1 : Configuration des sources

Security Lake collecte les données des journaux et des événements à partir de diverses sources et sur votre Comptes AWS territoire Régions AWS. Suivez ces instructions pour identifier les données que vous souhaitez que Security Lake collecte. Vous ne pouvez utiliser ces instructions que pour ajouter une source prise en charge nativement AWS service . Pour plus d'informations sur l'ajout d'une source personnalisée, consultezCollecte de données à partir de sources personnalisées.

Pour configurer la collecte des sources de log

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez une région. Vous pouvez activer Security Lake dans la région actuelle et dans d'autres régions lors de l'intégration.
3. Choisissez Démarrer.
4. Pour Sélectionner les sources de journaux et d'événements, choisissez l'une des options suivantes :

   a. Ingérer les AWS sources par défaut : lorsque vous choisissez l'option recommandée, CloudTrail les événements de données S3 ne sont pas inclus pour l'ingestion. En effet, l'ingestion d'un volume élevé d'événements de CloudTrail données S3 peut avoir un impact significatif sur le coût d'utilisation. Pour ingérer cette source, sélectionnez l'option Ingérer des AWS sources spécifiques.

   b. Ingérer des AWS sources spécifiques : avec cette option, vous pouvez sélectionner une ou plusieurs sources de journaux et d'événements que vous souhaitez ingérer.

> **Note**
>
> Lorsque vous activez Security Lake dans un compte pour la première fois, toutes les sources de journaux et d'événements sélectionnées feront l'objet d'une période d'essai gratuite de 15 jours. Pour plus d'informations sur les statistiques d'utilisation, consultezRévision de l'utilisation et des coûts estimés.

5. Pour Versions, choisissez la version de la source de données à partir de laquelle vous souhaitez ingérer les sources de journaux et d'événements.

> **Important**
>
> Si vous ne disposez pas des autorisations de rôle requises pour activer la nouvelle version de la source de AWS journal dans la région spécifiée, contactez votre administrateur Security Lake. Pour plus d'informations, consultez la section Mettre à jour les autorisations des rôles.

6. Pour Select Regions, choisissez d'ingérer les sources de journaux et d'événements provenant de toutes les régions prises en charge ou de régions spécifiques. Si vous choisissez Régions spécifiques, sélectionnez les régions à partir desquelles vous souhaitez ingérer les données.

7. Pour accéder au service, créez un nouveau IAM rôle ou utilisez un IAM rôle existant qui autorise Security Lake à collecter des données à partir de vos sources et à les ajouter à votre lac de données. Un rôle est utilisé dans toutes les régions dans lesquelles vous activez Security Lake.
8. Choisissez Suivant.

Étape 2 : définir les paramètres de stockage et les régions cumulatives (facultatif)

Vous pouvez spécifier la classe de stockage Amazon S3 dans laquelle vous souhaitez que Security Lake stocke vos données et pendant combien de temps. Vous pouvez également spécifier une région cumulative pour consolider les données de plusieurs régions. Il s'agit d'étapes facultatives. Pour de plus amples informations, veuillez consulter Gestion du cycle de vie dans Security Lake.

Pour configurer les paramètres de stockage et de cumul

1. Si vous souhaitez consolider les données de plusieurs régions contributrices dans une région cumulative, pour Sélectionner les régions cumulatives, choisissez Ajouter une région cumulative. Spécifiez la région cumulative et les régions qui y contribueront. Vous pouvez configurer une ou plusieurs régions cumulatives.
2. Pour Select storage classes, choisissez une classe de stockage Amazon S3. La classe de stockage par défaut est S3 Standard. Indiquez une période de conservation (en jours) si vous souhaitez que les données soient transférées vers une autre classe de stockage après cette période, puis choisissez Ajouter une transition. Une fois la période de rétention terminée, les objets expirent et Amazon S3 les supprime. Pour plus d'informations sur les classes de stockage et la rétention Amazon S3, consultezGestion de la rétention.
3. Si vous avez sélectionné une région cumulative lors de la première étape, pour accéder au service, créez un nouveau IAM rôle ou utilisez un IAM rôle existant qui autorise Security Lake à répliquer les données dans plusieurs régions.
4. Choisissez Suivant.

Étape 3 : révision et création d'un lac de données

Passez en revue les sources auprès desquelles Security Lake collectera les données, vos régions cumulatives et vos paramètres de conservation. Créez ensuite votre lac de données.

Pour consulter et créer le lac de données

1. Lors de l'activation de Security Lake, passez en revue les sources des journaux et des événements, les régions, les régions cumulatives et les classes de stockage.
2. Sélectionnez Create (Créer).

Après avoir créé votre lac de données, vous verrez la page de résumé sur la console Security Lake. Cette page fournit un aperçu du nombre de régions et de régions cumulatives, des informations sur les abonnés et les problèmes.

Le menu Problèmes affiche un résumé des problèmes survenus au cours des 14 derniers jours qui ont un impact sur le service Security Lake ou sur vos compartiments Amazon S3. Pour plus de détails sur chaque problème, vous pouvez accéder à la page Problèmes de la console Security Lake.

Étape 4 : Afficher et interroger vos propres données

Après avoir créé votre lac de données, vous pouvez utiliser Amazon Athena ou des services similaires pour afficher et interroger vos données à partir de AWS Lake Formation bases de données et de tables. Lorsque vous utilisez la console, Security Lake accorde automatiquement des autorisations d'affichage de base de données au rôle que vous utilisez pour activer Security Lake. Le rôle doit au minimum disposer des autorisations d'analyste de données. Pour plus d'informations sur les niveaux d'autorisation, voir la référence des personnages et des IAM autorisations de Lake Formation. Pour obtenir des instructions sur l'octroi d'`SELECT`autorisations, consultez la section Octroi d'autorisations au catalogue de données à l'aide de la méthode des ressources nommées dans le guide du AWS Lake Formation développeur.

Étape 5 : créer des abonnés

Après avoir créé votre lac de données, vous pouvez ajouter des abonnés pour consommer vos données. Les abonnés peuvent consommer des données en accédant directement aux objets de vos compartiments Amazon S3 ou en interrogeant le lac de données. Pour plus d'informations sur les abonnés, consultezGestion des abonnés dans Amazon Security Lake.

Commencer par programmation

Ce didacticiel explique comment activer et commencer à utiliser Security Lake par programmation. Amazon Security Lake vous API donne un accès complet et programmatique à votre compte, à vos

données et à vos ressources Security Lake. Vous pouvez également utiliser les outils de ligne de AWS commande (AWS Command Line Interfaceou les AWS outils pour PowerShell) ou pour accéder AWS SDKsà Security Lake.

Étape 1 : créer des IAM rôles

Si vous accédez à Security Lake par programmation, il est nécessaire de créer certains AWS Identity and Access Management (IAM) rôles afin de configurer votre lac de données.

> **Important**
>
> Il n'est pas nécessaire de créer ces IAM rôles si vous utilisez la console Security Lake pour activer et configurer Security Lake.

Vous devez créer des rôles IAM si vous souhaitez effectuer une ou plusieurs des actions suivantes (cliquez sur les liens pour obtenir plus d'informations sur IAM les rôles pour chaque action) :

- Création d'une source personnalisée : les sources personnalisées sont des sources autres que celles prises en charge de manière native AWS services qui envoient des données à Security Lake.
- Création d'un abonné avec accès aux données — Les abonnés autorisés peuvent accéder directement aux objets S3 depuis votre lac de données.
- Création d'un abonné avec accès aux requêtes : les abonnés autorisés peuvent interroger les données de Security Lake à l'aide de services tels qu'Amazon Athena.
- Configuration d'une région de cumul : une région de cumul consolide les données provenant de plusieurs. Régions AWS

Après avoir créé les rôles mentionnés précédemment, associez la politique AmazonSecurityLakeAdministrator AWS gérée au rôle que vous utilisez pour activer Security Lake. Cette politique accorde des autorisations administratives qui permettent à un mandant d'intégrer Security Lake et d'accéder à toutes les actions de Security Lake.

Joignez la politique AmazonSecurityLakeMetaStoreManager AWS gérée pour créer votre lac de données ou demander des données à partir de Security Lake. Cette politique est nécessaire pour que Security Lake puisse prendre en charge les tâches d'extraction, de transformation et de chargement (ETL) sur les données brutes des journaux et des événements qu'il reçoit des sources.

Étape 2 : activer Amazon Security Lake

Pour activer Security Lake par programmation, utilisez le CreateDataLakefonctionnement du Security Lake. API Si vous utilisez le AWS CLI, exécutez la create-data-lakecommande. Dans votre demande, utilisez le `region` champ de l'`configurations`objet pour spécifier le code de région dans lequel vous souhaitez activer Security Lake. Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.

Exemple 1

L'exemple de commande suivant active Security Lake dans les `us-east-2` régions `us-east-1` et. Dans les deux régions, ce lac de données est chiffré à l'aide de clés gérées par Amazon S3. Les objets expirent au bout de 365 jours et passent à la classe de stockage `ONEZONE_IA` S3 au bout de 60 jours. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ 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"
```

Exemple 2

L'exemple de commande suivant active Security Lake dans la `us-east-2` région. Ce lac de données est chiffré à l'aide d'une clé gérée par le client créée dans AWS Key Management Service (AWS KMS). Les objets expirent au bout de 500 jours et passent à la classe de stockage `GLACIER` S3 au bout de 30 jours. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}}]' \
```

```
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

> **Note**
>
> Si vous avez déjà activé Security Lake et que vous souhaitez mettre à jour les paramètres de configuration d'une région ou d'une source, utilisez l'UpdateDataLakeopération ou, si vous utilisez la AWS CLI, la update-data-lakecommande. N'utilisez pas l'`CreateDataLake`opération.

Étape 3 : Configuration des sources

Security Lake collecte les données des journaux et des événements à partir de diverses sources et sur votre Comptes AWS territoire Régions AWS. Suivez ces instructions pour identifier les données que vous souhaitez que Security Lake collecte. Vous ne pouvez utiliser ces instructions que pour ajouter une source prise en charge nativement AWS service . Pour plus d'informations sur l'ajout d'une source personnalisée, consultezCollecte de données à partir de sources personnalisées.

Pour définir une ou plusieurs sources de collecte par programmation, utilisez le CreateAwsLogSourcefonctionnement du Security Lake. API Pour chaque source, spécifiez une valeur unique régionale pour le `sourceName` paramètre. Utilisez éventuellement des paramètres supplémentaires pour limiter la portée de la source à des comptes spécifiques (`accounts`) ou à une version spécifique (`sourceVersion`).

> **Note**
>
> Si vous n'incluez aucun paramètre facultatif dans votre demande, Security Lake applique votre demande à tous les comptes ou à toutes les versions de la source spécifiée, en fonction du paramètre que vous excluez. Par exemple, si vous êtes l'administrateur délégué de Security Lake pour une organisation et que vous excluez le `accounts` paramètre, Security Lake applique votre demande à tous les comptes de votre organisation. De même, si vous excluez le `sourceVersion` paramètre, Security Lake applique votre demande à toutes les versions de la source spécifiée.

Si votre demande indique une région dans laquelle vous n'avez pas activé Security Lake, une erreur se produit. Pour corriger cette erreur, assurez-vous que le `regions` tableau indique uniquement les

régions dans lesquelles vous avez activé Security Lake. Vous pouvez également activer Security Lake dans la région, puis soumettre à nouveau votre demande.

Lorsque vous activez Security Lake dans un compte pour la première fois, toutes les sources de journaux et d'événements sélectionnées feront l'objet d'une période d'essai gratuite de 15 jours. Pour plus d'informations sur les statistiques d'utilisation, consultezRévision de l'utilisation et des coûts estimés.

Étape 4 : Configuration des paramètres de stockage et des régions cumulatives (facultatif)

Vous pouvez spécifier la classe de stockage Amazon S3 dans laquelle vous souhaitez que Security Lake stocke vos données et pendant combien de temps. Vous pouvez également spécifier une région cumulative pour consolider les données de plusieurs régions. Il s'agit d'étapes facultatives. Pour de plus amples informations, veuillez consulter Gestion du cycle de vie dans Security Lake.

Pour définir un objectif cible par programmation lorsque vous activez Security Lake, utilisez le CreateDataLakefonctionnement du Security Lake. API Si vous avez déjà activé Security Lake et que vous souhaitez définir un objectif cible, utilisez l'UpdateDataLakeopération, et non l'`CreateDataLake`opération.

Quelle que soit l'opération, utilisez les paramètres pris en charge pour spécifier les paramètres de configuration souhaités :

- Pour spécifier une région de cumul, utilisez le `region` champ pour spécifier la région dans laquelle vous souhaitez fournir des données aux régions de cumul. Dans le `regions` tableau de l'`replicationConfiguration`objet, spécifiez le code de région pour chaque région cumulative. Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.
- Pour définir les paramètres de conservation de vos données, utilisez les `lifecycleConfiguration` paramètres suivants :
  - Pour`transitions`, spécifiez le nombre total de jours (`days`) pendant lesquels vous souhaitez stocker des objets S3 dans une classe de stockage Amazon S3 spécifique (`storageClass`).
  - Pour`expiration`, spécifiez le nombre total de jours pendant lesquels vous souhaitez stocker des objets dans Amazon S3, en utilisant n'importe quelle classe de stockage, après la création des objets. À la fin de cette période de rétention, les objets expirent et Amazon S3 les supprime.

Security Lake applique les paramètres de rétention spécifiés à la région que vous spécifiez dans le `region` champ de l'`configurations`objet.

Par exemple, la commande suivante crée un lac de données `ap-northeast-2` sous forme de région cumulative. La `us-east-1` Région fournira des données à la `ap-northeast-2` Région. Cet exemple établit également une période d'expiration de 10 jours pour les objets ajoutés au lac de données.

```
$ 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"
```

Vous avez maintenant créé votre lac de données. Utilisez le ListDataLakesfonctionnement du Security Lake API pour vérifier l'activation de Security Lake et les paramètres de votre lac de données dans chaque région.

Si des problèmes ou des erreurs surviennent lors de la création de votre lac de données, vous pouvez afficher une liste d'exceptions à l'aide de l'ListDataLakeExceptionsopération et informer les utilisateurs des exceptions lors de l'CreateDataLakeExceptionSubscriptionopération. Pour de plus amples informations, veuillez consulter Résolution des problèmes liés à l'état des lacs.

Étape 5 : Afficher et interroger vos propres données

Après avoir créé votre lac de données, vous pouvez utiliser Amazon Athena ou des services similaires pour afficher et interroger vos données à partir de AWS Lake Formation bases de données et de tables. Lorsque vous activez Security Lake par programmation, les autorisations d'affichage de la base de données ne sont pas accordées automatiquement. Le compte administrateur du lac de données AWS Lake Formation doit accorder `SELECT` des autorisations au IAM rôle que vous souhaitez utiliser pour interroger les bases de données et les tables pertinentes. Le rôle doit au minimum disposer des autorisations d'analyste de données. Pour plus d'informations sur les niveaux d'autorisation, voir la référence des personnages et des IAM autorisations de Lake Formation. Pour obtenir des instructions sur l'octroi d'`SELECT`autorisations, consultez la section Octroi d'autorisations

au catalogue de données à l'aide de la méthode des ressources nommées dans le guide du AWS Lake Formation développeur.

Étape 6 : créer des abonnés

Après avoir créé votre lac de données, vous pouvez ajouter des abonnés pour consommer vos données. Les abonnés peuvent consommer des données en accédant directement aux objets de vos compartiments Amazon S3 ou en interrogeant le lac de données. Pour plus d'informations sur les abonnés, consultezGestion des abonnés dans Amazon Security Lake.

Gérer plusieurs comptes avec AWS Organizations

Vous pouvez utiliser Amazon Security Lake pour collecter des journaux et des événements de sécurité à partir de plusieurs sites Comptes AWS. Pour automatiser et rationaliser la gestion de plusieurs comptes, nous vous recommandons vivement d'intégrer Security Lake à AWS Organizations.

Dans Organizations, le compte que vous utilisez pour créer l'organisation est appelé compte de gestion. Pour intégrer Security Lake à Organizations, le compte de gestion doit désigner un compte administrateur Security Lake délégué pour l'organisation.

L'administrateur délégué de Security Lake peut activer Security Lake et configurer les paramètres de Security Lake pour les comptes des membres. L'administrateur délégué peut collecter des journaux et des événements au sein de l'organisation partout Régions AWS où Security Lake est activé (quel que soit le point de terminaison régional qu'il utilise actuellement). L'administrateur délégué peut également configurer Security Lake pour collecter automatiquement les données des journaux et des événements pour les nouveaux comptes de l'organisation.

L'administrateur délégué de Security Lake a accès aux données des journaux et des événements pour les comptes membres associés. En conséquence, ils peuvent configurer Security Lake pour collecter les données détenues par les comptes membres associés. Ils peuvent également autoriser les abonnés à utiliser les données détenues par les comptes membres associés.

Pour activer Security Lake pour plusieurs comptes au sein d'une organisation, le compte de gestion de l'organisation doit d'abord désigner un compte administrateur Security Lake délégué pour l'organisation. L'administrateur délégué peut ensuite activer et configurer Security Lake pour l'organisation.

> **Important**
>
> Utilisez l'RegisterDataLakeDelegatedAdministratorAPI de Security Lake pour autoriser Security Lake à accéder à votre organisation et enregistrer l'administrateur délégué de l'organisation.
> Si vous utilisez les API des organisations pour enregistrer un administrateur délégué, les rôles liés aux services pour les organisations risquent de ne pas être créés correctement. Pour garantir une fonctionnalité complète, utilisez les API Security Lake.

Pour plus d'informations sur la configuration des organisations, voir Création et gestion d'une organisation dans le Guide de AWS Organizations l'utilisateur.

Considérations importantes pour les administrateurs délégués de Security Lake

Prenez note des facteurs suivants qui définissent le comportement d'un administrateur délégué dans Security Lake :

L'administrateur délégué est le même dans toutes les régions.

- Lorsque vous créez l'administrateur délégué, celui-ci devient l'administrateur délégué pour chaque région dans laquelle vous activez Security Lake.

Nous vous recommandons de définir le compte Log Archive en tant qu'administrateur délégué de Security Lake.

- Le compte Log Archive est un Compte AWS compte dédié à l'ingestion et à l'archivage de tous les journaux liés à la sécurité. L'accès à ce compte est généralement limité à quelques utilisateurs, tels que les auditeurs et les équipes de sécurité pour les enquêtes de conformité. Nous vous recommandons de définir le compte Log Archive en tant qu'administrateur délégué de Security Lake afin que vous puissiez consulter les journaux et les événements liés à la sécurité avec un minimum de changement de contexte.

- En outre, nous recommandons que seul un nombre minimal d'utilisateurs ait un accès direct au compte Log Archive. En dehors de ce groupe de sélection, si un utilisateur a besoin d'accéder aux données collectées par Security Lake, vous pouvez l'ajouter en tant qu'abonné de Security Lake. Pour plus d'informations sur l'ajout d'un abonné, consultezGestion des abonnés dans Amazon Security Lake.

- Si vous n'utilisez pas le AWS Control Tower service, il se peut que vous n'ayez pas de compte Log Archive. Pour plus d'informations sur le compte Log Archive, voir Security OU — Compte Log Archive dans l'architecture AWS de référence de sécurité.

Une organisation ne peut avoir qu'un seul administrateur délégué.

- Vous ne pouvez avoir qu'un seul administrateur délégué de Security Lake par organisation.

Le compte de gestion de l'organisation ne peut pas être l'administrateur délégué.

- Sur la base des meilleures pratiques de AWS sécurité et du principe du moindre privilège, le compte de gestion de votre organisation ne peut pas être l'administrateur délégué.

L'administrateur délégué doit faire partie d'une organisation active.

> Lorsque vous supprimez une organisation, le compte d'administrateur délégué ne peut plus gérer Security Lake. Vous devez désigner un administrateur délégué d'une autre organisation ou utiliser Security Lake avec un compte autonome ne faisant pas partie d'une organisation.

Autorisations IAM requises pour désigner l'administrateur délégué

Lorsque vous désignez l'administrateur délégué de Security Lake, vous devez disposer des autorisations nécessaires pour activer Security Lake et utiliser certaines opérations d' AWS Organizations API répertoriées dans la déclaration de politique suivante.

Vous pouvez ajouter l'instruction suivante à la fin d'une politique AWS Identity and Access Management (IAM) pour accorder ces autorisations.

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

Désignation de l'administrateur délégué de Security Lake et ajout de comptes de membres

Choisissez votre méthode d'accès pour désigner le compte administrateur délégué de Security Lake pour votre organisation. Seul le compte de gestion de l'organisation peut désigner le compte d'administrateur délégué pour son organisation. Le compte de gestion de l'organisation ne peut pas être le compte d'administrateur délégué de leur organisation.

> **Note**
>
> - Le compte de gestion de l'organisation doit utiliser l'`RegisterDataLakeDelegatedAdministrator`opération Security Lake pour désigner le compte administrateur Security Lake délégué. La désignation de l'administrateur délégué de Security Lake via Organizations n'est pas prise en charge.
> - Si vous souhaitez modifier l'administrateur délégué de l'organisation, vous devez d'abord supprimer l'administrateur délégué actuel. Vous pouvez ensuite désigner un nouvel administrateur délégué.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous à l'aide des informations d'identification du compte de gestion de votre organisation.

2. - Si Security Lake n'est pas encore activé, sélectionnez Get Started, puis désignez l'administrateur délégué de Security Lake sur la page Activer Security Lake.
   - Si Security Lake est déjà activé, désignez l'administrateur délégué de Security Lake sur la page Paramètres.
3. Sous Déléguer l'administration à un autre compte, sélectionnez le compte qui fait déjà office d'administrateur délégué pour les autres services AWS de sécurité (recommandé). Vous pouvez également saisir l' Compte AWS identifiant à 12 chiffres du compte que vous souhaitez désigner comme administrateur délégué de Security Lake.
4. Choisisssez Delegate (Déléguer). Si Security Lake n'est pas déjà activé, la désignation de l'administrateur délégué activera Security Lake pour ce compte dans votre région actuelle.

API

Pour désigner l'administrateur délégué par programmation, utilisez le RegisterDataLakeDelegatedAdministratorfonctionnement de l'API Security Lake. Vous devez appeler l'opération depuis le compte de gestion de l'organisation. Si vous utilisez le AWS CLI, exécutez la register-data-lake-delegated-administratorcommande depuis le compte de gestion de l'organisation. Dans votre demande, utilisez le `accountId` paramètre pour spécifier l'ID

de compte à 12 chiffres du compte Compte AWS à désigner comme compte d'administrateur délégué pour l'organisation.

Par exemple, la AWS CLI commande suivante désigne l'administrateur délégué. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

L'administrateur délégué peut également choisir d'automatiser la collecte des données des AWS journaux et des événements pour les nouveaux comptes de l'organisation. Avec cette configuration, Security Lake est automatiquement activé dans les nouveaux comptes lorsque ceux-ci sont ajoutés à l'organisation dans AWS Organizations. En tant qu'administrateur délégué, vous pouvez activer cette configuration en utilisant CreateDataLakeOrganizationConfigurationl'API Security Lake ou, si vous utilisez l'interface de ligne de commande AWS, en exécutant la create-data-lake-organization-configurationcommande. Dans votre demande, vous pouvez également spécifier certains paramètres de configuration pour les nouveaux comptes.

Par exemple, la AWS CLI commande suivante active automatiquement Security Lake et la collecte des journaux de requêtes du résolveur Amazon Route 53, des AWS Security Hub résultats et des journaux de flux Amazon Virtual Private Cloud (Amazon VPC) dans les nouveaux comptes d'organisation. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Une fois que le compte de gestion de l'organisation a désigné l'administrateur délégué, celui-ci peut activer et configurer Security Lake pour l'organisation. Cela inclut l'activation et la configuration de Security Lake pour collecter les données des AWS journaux et des événements pour les comptes individuels de l'organisation. Pour plus d'informations, consultez Collecte de données auprès de AWS services.

Vous pouvez utiliser cette GetDataLakeOrganizationConfigurationopération pour obtenir des informations sur la configuration actuelle de votre organisation pour les nouveaux comptes membres.

Suppression de l'administrateur délégué de Security Lake

Seul le compte de gestion de l'organisation peut supprimer l'administrateur délégué de Security Lake pour son organisation. Si vous souhaitez modifier l'administrateur délégué de l'organisation, supprimez l'administrateur délégué actuel, puis désignez le nouvel administrateur délégué.

> **Important**
>
> La suppression de l'administrateur délégué de Security Lake supprime votre lac de données et désactive Security Lake pour les comptes de votre organisation.

Vous ne pouvez pas modifier ou supprimer l'administrateur délégué à l'aide de la console Security Lake. Ces tâches ne peuvent être effectuées que par programmation.

Pour supprimer l'administrateur délégué par programmation, utilisez le DeregisterDataLakeDelegatedAdministratorfonctionnement de l'API Security Lake. Vous devez appeler l'opération depuis le compte de gestion de l'organisation. Si vous utilisez le AWS CLI, exécutez la deregister-data-lake-delegated-administratorcommande depuis le compte de gestion de l'organisation.

Par exemple, la AWS CLI commande suivante supprime l'administrateur délégué de Security Lake.

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

Pour conserver la désignation d'administrateur délégué tout en modifiant les paramètres de configuration automatique des nouveaux comptes membres, utilisez l'DeleteDataLakeOrganizationConfigurationAPI Security Lake ou, si vous utilisez la AWS CLI, la delete-data-lake-organization-configurationcommande. Seul l'administrateur délégué peut modifier ces paramètres pour l'organisation.

Par exemple, la AWS CLI commande suivante arrête la collecte automatique des résultats du Security Hub à partir des nouveaux comptes membres qui rejoignent l'organisation. Les nouveaux comptes membres ne transmettront pas les résultats du Security Hub au lac de données une fois que l'administrateur délégué aura invoqué cette opération. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

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

Accès sécurisé à Security Lake

Une fois que vous avez configuré Security Lake pour une organisation, le compte AWS Organizations de gestion peut permettre un accès sécurisé avec Security Lake. L'accès sécurisé permet à Security Lake de créer un rôle lié au service IAM et d'effectuer des tâches au sein de votre organisation et de ses comptes en votre nom. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans le Guide de AWS Organizations l'utilisateur.

En tant qu'utilisateur du compte de gestion de l'organisation, vous pouvez désactiver l'accès sécurisé à Security Lake in AWS Organizations. Pour obtenir des instructions sur la désactivation de l'accès sécurisé, voir Comment activer ou désactiver l'accès sécurisé dans le Guide de l'AWS Organizations utilisateur.

Nous recommandons de désactiver l'accès sécurisé si celui de l'administrateur délégué Compte AWS est suspendu, isolé ou fermé.

Gestion des régions

Amazon Security Lake peut collecter les journaux de sécurité et Régions AWS les événements pour lesquels vous avez activé le service. Pour chaque région, vos données sont stockées dans un compartiment Amazon S3 différent. Vous pouvez spécifier différentes configurations de lac de données (par exemple, différentes sources et paramètres de rétention) pour différentes régions. Vous pouvez également définir une ou plusieurs régions cumulatives pour consolider les données de plusieurs régions.

Vérification de l'état de la région

Security Lake peut collecter des données sur plusieurs sites Régions AWS. Pour suivre l'état de votre lac de données, il peut être utile de comprendre comment chaque région est actuellement configurée. Choisissez votre méthode d'accès préférée et suivez ces étapes pour connaître le statut actuel d'une région.

Console

Pour vérifier le statut de la région

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, sélectionnez Regions. La page Régions apparaît et fournit un aperçu des régions dans lesquelles Security Lake est actuellement activé.
3. Sélectionnez une région, puis choisissez Modifier pour afficher les détails de cette région.

API

Pour connaître l'état de la collecte des journaux dans la région actuelle, utilisez le GetDataLakeSourcesfonctionnement du lac de sécuritéAPI. Si vous utilisez le AWS CLI, exécutez la get-data-lake-sourcescommande. Pour le `accounts` paramètre, spécifiez-en un ou plusieurs Compte AWS IDs sous forme de liste. Si votre demande aboutit, Security Lake renvoie un instantané de ces comptes dans la région actuelle, y compris les AWS sources auprès desquelles Security Lake collecte des données et le statut de chaque source. Si vous n'incluez pas le `accounts` paramètre, la réponse inclut l'état de la collecte des journaux pour tous les comptes dans lesquels Security Lake est configuré dans la région actuelle.

Par exemple, la AWS CLI commande suivante permet de récupérer l'état de collecte des journaux pour les comptes spécifiés dans la région actuelle. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

La AWS CLI commande suivante répertorie l'état de collecte des journaux pour tous les comptes et sources activées dans la région spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Pour déterminer si vous avez activé Security Lake pour une région, utilisez l'ListDataLakesopération. Si vous utilisez le AWS CLI, exécutez la list-data-lakescommande. Pour le `regions` paramètre, spécifiez le code de région de la région, par exemple, `us-east-1` pour la région de l'est des États-Unis (Virginie du Nord). Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS. L'`ListDataLakes`opération renvoie les paramètres de configuration du lac de données pour chaque région que vous spécifiez dans votre demande. Si vous ne spécifiez aucune région, Security Lake renvoie l'état et les paramètres de configuration de votre lac de données dans chaque région dans laquelle Security Lake est disponible.

Par exemple, la AWS CLI commande suivante indique l'état et les paramètres de configuration de votre lac de données dans la `eu-central-1` région. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Modification des paramètres de région

Choisissez votre méthode préférée et suivez ces instructions pour mettre à jour les paramètres de votre lac de données dans un ou plusieurs d'entre eux Régions AWS.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, sélectionnez Regions.
3. Sélectionnez une région, puis choisissez Modifier.
4. Cochez la case Remplacer les sources pour tous les comptes afin <Region>de confirmer que vos sélections ici remplacent les sélections précédentes pour cette région.
5. Pour Sélectionner les classes de stockage, choisissez Ajouter une transition pour ajouter de nouvelles classes de stockage pour vos données.
6. Pour les balises, attribuez ou modifiez éventuellement les balises pour la région. Une balise est une étiquette que vous pouvez définir et attribuer à certains types de AWS ressources, y compris la configuration du lac de données Compte AWS pour une région donnée. Pour en savoir plus, consultez Marquage des ressources d'Amazon Security Lake.
7. Pour transformer une région en région cumulative, choisissez Cumuler les régions (sous Paramètres) dans le volet de navigation. Ensuite, choisissez Modify (Modifier). Dans la section Sélectionner les régions cumulatives, choisissez Ajouter une région cumulative. Sélectionnez les régions contributrices et autorisez Security Lake à répliquer les données dans plusieurs régions. Lorsque vous avez terminé, choisissez Enregistrer pour enregistrer vos modifications.

API

Pour mettre à jour les paramètres régionaux de votre lac de données par programmation, utilisez UpdateDataLakele Security Lake. API Si vous utilisez le AWS CLI, exécutez la update-data-lakecommande. Pour le `region` paramètre, spécifiez le code de région pour lequel vous souhaitez modifier les paramètres, par exemple, `us-east-1` pour la région USA Est (Virginie du Nord). Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.

Utilisez des paramètres supplémentaires pour spécifier une nouvelle valeur pour chaque paramètre que vous souhaitez modifier, par exemple, la clé de chiffrement (`encryptionConfiguration`) et les paramètres de rétention (`lifecycleConfiguration`).

Par exemple, la AWS CLI commande suivante met à jour les paramètres d'expiration des données et de transition de classe de stockage pour la `us-east-1` région. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Configuration de régions cumulatives

Une région cumulative consolide les données d'une ou de plusieurs régions contributrices. La spécification d'une région cumulative peut vous aider à vous conformer aux exigences de conformité régionales.

Important

Si vous avez créé une source personnalisée, pour garantir que les données source personnalisées sont correctement répliquées vers la destination, Security Lake recommande de suivre les meilleures pratiques décrites dans Meilleures pratiques pour l'ingestion de sources personnalisées. La réplication ne peut pas être effectuée sur des données qui ne suivent pas le format du chemin de données de la partition S3 tel que décrit sur la page.

Avant d'ajouter une région cumulative, vous devez d'abord créer deux rôles différents dans AWS Identity and Access Management () IAM :

- IAMrôle pour la réplication des données
- IAMrôle pour enregistrer AWS Glue des partitions

Note

Security Lake crée ces IAM rôles ou utilise des rôles existants en votre nom lorsque vous utilisez la console Security Lake. Toutefois, vous devez créer ces rôles lorsque vous utilisez le Security Lake API ou AWS CLI.

IAMrôle pour la réplication des données

Ce IAM rôle autorise Amazon S3 à répliquer les journaux sources et les événements dans plusieurs régions.

Pour accorder ces autorisations, créez un IAM rôle commençant par le préfixe et `SecurityLake` associez l'exemple de politique suivant au rôle. Vous aurez besoin du nom de ressource Amazon (ARN) du rôle lorsque vous créerez une région cumulative dans Security Lake. Dans le cadre de cette politique, `sourceRegions` sont des régions contributrices et `destinationRegions` des régions cumulatives.

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

Associez la politique de confiance suivante à votre rôle pour permettre à Amazon S3 d'assumer ce rôle :

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

Si vous utilisez une clé gérée par le client provenant de AWS Key Management Service (AWS KMS) pour chiffrer votre lac de données Security Lake, vous devez accorder les autorisations suivantes en plus des autorisations définies dans la politique de réplication des données.

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

Pour plus d'informations sur les rôles de réplication, consultez la section Configuration des autorisations dans le guide de l'utilisateur d'Amazon Simple Storage Service.

IAMrôle pour enregistrer AWS Glue des partitions

Ce IAM rôle accorde des autorisations pour une AWS Lambda fonction de mise à jour de partition utilisée par Security Lake pour enregistrer AWS Glue des partitions pour les objets S3 répliqués

depuis d'autres régions. Sans créer ce rôle, les abonnés ne peuvent pas interroger les événements provenant de ces objets.

Pour accorder ces autorisations, créez un rôle nommé `AmazonSecurityLakeMetaStoreManager` (vous l'avez peut-être déjà créé lors de votre intégration à Security Lake). Pour plus d'informations sur ce rôle, y compris un exemple de politique, consultezÉtape 1 : créer des IAM rôles.

Dans la console Lake Formation, vous devez également accorder `AmazonSecurityLakeMetaStoreManager` des autorisations en tant qu'administrateur de lac de données en suivant les étapes suivantes :

1. Ouvrez la console Lake Formation à l'adresse https://console.aws.amazon.com/lakeformation/.
2. Connectez-vous en tant qu'utilisateur administratif.
3. Si une fenêtre Welcome to Lake Formation apparaît, choisissez l'utilisateur que vous avez créé ou sélectionné à l'étape 1, puis choisissez Get started.
4. Si la fenêtre Welcome to Lake Formation ne s'affiche pas, effectuez les étapes suivantes pour configurer un administrateur de Lake Formation.
    1. Dans le volet de navigation, sous Autorisations, sélectionnez Administrative Rôles et tâches. Dans la section Administrateurs du lac de données de la page de console, choisissez Choisir les administrateurs.
    2. Dans la boîte de dialogue Gérer les administrateurs des lacs de données, pour IAM les utilisateurs et les rôles, choisissez le AmazonSecurityLakeMetaStoreManagerIAMrôle que vous avez créé, puis cliquez sur Enregistrer.

Pour plus d'informations sur la modification des autorisations pour les administrateurs de lacs de données, voir Création d'un administrateur de lac de données dans le guide du AWS Lake Formation développeur.

Ajouter des régions cumulatives

Choisissez votre méthode d'accès préférée et suivez ces étapes pour ajouter une région cumulative.

> **Note**
>
> Une région peut fournir des données à plusieurs régions cumulées. Toutefois, une région cumulative ne peut pas être une région contributrice pour une autre région cumulative.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, sous Paramètres, choisissez Rollup Regions.
3. Choisissez Modifier, puis sélectionnez Ajouter une région cumulative.
4. Spécifiez la région cumulée et les régions contributrices. Répétez cette étape si vous souhaitez ajouter plusieurs régions cumulatives.
5. Si c'est la première fois que vous ajoutez une région cumulative, pour accéder au service, créez un nouveau IAM rôle ou utilisez un IAM rôle existant qui autorise Security Lake à répliquer les données dans plusieurs régions.
6. Lorsque vous avez terminé, choisissez Enregistrer.

Vous pouvez également ajouter une région cumulative lorsque vous embarquez à bord de Security Lake. Pour de plus amples informations, veuillez consulter Commencer à utiliser Amazon Security Lake.

API

Pour ajouter une région cumulative par programmation, utilisez le UpdateDataLakefonctionnement du lac de sécurité. API Si vous utilisez le AWS CLI, exécutez la update-data-lakecommande. Dans votre demande, utilisez le `region` champ pour spécifier la région dans laquelle vous souhaitez fournir des données à la région cumulative. Dans le `regions` tableau du `replicationConfiguration` paramètre, spécifiez le code de région pour chaque région cumulative. Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.

Par exemple, la commande suivante est définie `ap-northeast-2` comme une région cumulative. La `us-east-1` Région fournira des données à la `ap-northeast-2` Région. Cet exemple établit également une période d'expiration de 365 jours pour les objets ajoutés au lac de données. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Vous pouvez également ajouter une région cumulative lorsque vous embarquez à bord de Security Lake. Pour ce faire, utilisez l'CreateDataLakeopération (ou, si vous utilisez la AWS CLI, la create-data-lakecommande). Pour plus d'informations sur la configuration des régions cumulatives lors de l'intégration, consultez. Commencer à utiliser Amazon Security Lake

Mettre à jour ou supprimer des régions cumulatives

Choisissez votre méthode d'accès préférée et suivez ces étapes pour mettre à jour ou supprimer les régions cumulatives dans Security Lake.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, sous Paramètres, choisissez Rollup Regions.
3. Sélectionnez Modifier.
4. Pour modifier les régions contributrices d'une région cumulative, spécifiez les régions contributrices mises à jour dans la ligne correspondant à la région cumulative.
5. Pour supprimer une région de cumul, choisissez Supprimer dans la ligne correspondant à la région de cumul.
6. Lorsque vous avez terminé, choisissez Enregistrer.

API

Pour configurer les régions cumulatives par programmation, utilisez le UpdateDataLakefonctionnement du lac de sécurité. API Si vous utilisez le AWS CLI, exécutez la update-data-lakecommande. Dans votre demande, utilisez les paramètres pris en charge pour définir les paramètres cumulatifs :

- Pour ajouter une région contributrice, utilisez le `region` champ pour spécifier le code de région de la région à ajouter. Dans le `regions` tableau de l'`replicationConfiguration`objet, spécifiez le code de région pour chaque région cumulative à laquelle vous souhaitez fournir des données. Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.
- Pour supprimer une région contributrice, utilisez le `region` champ pour spécifier le code de région de la région à supprimer. Pour les `replicationConfiguration` paramètres, ne spécifiez aucune valeur.

Par exemple, la commande suivante permet de configurer les deux régions `us-east-1` et de les configurer `us-east-2` en tant que régions contributives. Les deux régions fourniront des données à la `ap-northeast-3` région récapitulative. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

gestion des sources dans Amazon Security Security Security Security Security Security Security Security

Les sources sont des journaux et des événements générés à partir d'un système unique qui correspondent à une classe d'événements spécifique dans leCadre de schéma de cybersécurité ouvert (OCSF) schéma. Amazon Security Lake peut collecter des journaux et des événements à partir de diverses sources, y compris des sources personnalisées tiercesAWS services et prises en charge de manière native.

Security Security Security permet Security. Une fois le traitement, Security Security Security Security Security Security Security Security Security Security Security Security permet Security Security Security Security Security Simple Storage Service (Amazon S3) Security Security Security Security Security Security Security Security SecurityCompte AWS Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security Security SecurityRégion AWS Security Security Security Security Security Security Security permet permet de créer un compartiment Amazon S3 Security. Chaque source reçoit un préfixe distinct dans votre compartiment S3, et Security Lake organise les données de chaque source dans un ensemble deAWS Lake Formation tables distinct.

Rubriques

Collecte de données auprès de AWS services

Amazon Security Lake peut collecter des journaux et des événements à partir des sites suivants pris en charge de manière native : AWS services

- AWS CloudTrail événements de gestion et de données (S3, Lambda)
- Journaux d'audit Amazon Elastic Kubernetes Service (Amazon EKS)

- Journaux de requête Amazon Route 53 Resolver
- AWS Security Hub résultats
- Journaux de flux Amazon Virtual Private Cloud (Amazon VPC)
- AWS WAF journaux v2

Security Lake transforme automatiquement ces données au Cadre de schéma de cybersécurité ouvert (OCSF) format Apache Parquet.

> **Tip**
>
> Pour ajouter un ou plusieurs des services précédents en tant que source de journal dans Security Lake, il n'est pas nécessaire de configurer séparément la connexion à ces services, à l'exception CloudTrail des événements de gestion. Si la journalisation est configurée dans ces services, vous n'avez pas besoin de modifier votre configuration de journalisation pour les ajouter en tant que sources de journalisation dans Security Lake. Security Lake extrait les données directement de ces services par le biais d'un flux d'événements indépendant et dupliqué.

Prérequis : vérifier les autorisations

Pour ajouter un en AWS service tant que source dans Security Lake, vous devez disposer des autorisations nécessaires. Vérifiez que la politique AWS Identity and Access Management (IAM) attachée au rôle que vous utilisez pour ajouter une source est autorisée à effectuer les actions suivantes :

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

Il est recommandé que le rôle réponde aux conditions et à l'étendue des ressources suivantes pour les `s3:PutObject` autorisations `S3:getObject` et.

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

Ces actions vous permettent de collecter des journaux et des événements à partir de l'an AWS service et de les envoyer à la AWS Glue base de données et à la table appropriées.

Si vous utilisez une AWS KMS clé pour le chiffrement côté serveur de votre lac de données, vous devez également obtenir une autorisation pour. `kms:DescribeKey`

CloudTrail journaux d'événements

AWS CloudTrail vous fournit un historique des appels d' AWS API pour votre compte, y compris les appels d'API effectués à l' AWS Management Console aide AWS des SDK, des outils de ligne de commande et de certains AWS services. CloudTrail vous permet également d'identifier les utilisateurs et les comptes appelés AWS API pour les services pris en charge CloudTrail, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Security Lake peut collecter les journaux associés aux événements CloudTrail de gestion et aux événements de CloudTrail données pour S3 et Lambda. CloudTrail les événements de gestion, les événements de données S3 et les événements de données Lambda sont trois sources distinctes

dans Security Lake. Par conséquent, ils ont des valeurs différentes `sourceName`lorsque vous ajoutez l'un d'entre eux en tant que source de journal ingérée. Les événements de gestion, également appelés événements du plan de contrôle, fournissent un aperçu des opérations de gestion effectuées sur les ressources de votre entreprise Compte AWS. CloudTrail les événements de données, également appelés opérations du plan de données, indiquent les opérations de ressources effectuées sur ou au sein des ressources de votre Compte AWS. Ces opérations sont souvent des activités à volume élevé.

Pour collecter les événements CloudTrail de gestion dans Security Lake, vous devez disposer d'au moins un journal d'organisation CloudTrail multirégional qui collecte les événements de CloudTrail gestion en lecture et en écriture. La journalisation doit être activée pour le parcours. Si la journalisation est configurée dans les autres services, vous n'avez pas besoin de modifier votre configuration de journalisation pour les ajouter en tant que sources de journalisation dans Security Lake. Security Lake extrait les données directement de ces services par le biais d'un flux d'événements indépendant et dupliqué.

Un suivi multirégional fournit des fichiers journaux provenant de plusieurs régions vers un seul compartiment Amazon Simple Storage Service (Amazon S3) pour un seul. Compte AWS Si vous avez déjà un parcours multirégional géré via CloudTrail la console AWS Control Tower, aucune autre action n'est requise.

- Pour plus d'informations sur la création et la gestion d'un parcours de CloudTrail suivi, consultez la section Création d'un parcours pour une organisation dans le guide de AWS CloudTrail l'utilisateur.
- Pour plus d'informations sur la création et la gestion d'un parcours de AWS Control Tower suivi, consultez la section Journalisation des AWS Control Tower actions AWS CloudTrail dans le guide de AWS Control Tower l'utilisateur.

Lorsque vous ajoutez CloudTrail des événements en tant que source, Security Lake commence immédiatement à collecter vos journaux CloudTrail d'événements. Il consomme les événements CloudTrail de gestion et de données directement CloudTrail par le biais d'un flux d'événements indépendant et dupliqué.

Security Lake ne gère pas vos CloudTrail événements et n'affecte pas vos CloudTrail configurations existantes. Pour gérer directement l'accès et la rétention de vos CloudTrail événements, vous devez utiliser la console CloudTrail de service ou l'API. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le Guide de AWS CloudTrail l'utilisateur.

La liste suivante fournit des liens de GitHub référentiel vers la référence de mappage expliquant comment Security Lake normalise les CloudTrail événements par rapport à OCSF.

GitHub Référentiel OCSF pour les événements CloudTrail

- Version 1 de la source (v1.0.0-rc.2)
- Version 2 de la source (v1.1.0)

Journaux d'audit Amazon EKS

Lorsque vous ajoutez les journaux d'audit Amazon EKS en tant que source, Security Lake commence à collecter des informations détaillées sur les activités effectuées sur les ressources Kubernetes exécutées dans vos clusters Elastic Kubernetes Service (EKS). Les journaux d'audit EKS vous aident à détecter les activités potentiellement suspectes dans vos clusters EKS au sein d'Amazon Elastic Kubernetes Service.

Security Lake utilise les événements du journal d'audit EKS directement depuis la fonction de journalisation du plan de contrôle Amazon EKS via un flux indépendant et duplicatif de journaux d'audit. Ce processus est conçu pour ne pas nécessiter de configuration supplémentaire ni affecter les configurations de journalisation du plan de contrôle Amazon EKS existantes que vous pourriez avoir. Pour plus d'informations, consultez la section Connexion au plan de contrôle Amazon EKS dans le guide de l'utilisateur Amazon EKS.

Les journaux d'audit Amazon EKS ne sont pris en charge que dans OCSF v1.1.0. Pour plus d'informations sur la façon dont Security Lake normalise les événements EKS Audit Logs en OCSF, consultez la référence de mappage dans le référentiel GitHub OCSF pour les événements Amazon EKS Audit Logs (v1.1.0).

Journaux de requête Route 53 Resolver

Les journaux de requêtes du résolveur Route 53 suivent les requêtes DNS effectuées par les ressources de votre Amazon Virtual Private Cloud (Amazon VPC). Cela vous permet de comprendre le fonctionnement de vos applications et de détecter les menaces de sécurité.

Lorsque vous ajoutez les journaux de requêtes du résolveur Route 53 en tant que source dans Security Lake, Security Lake commence immédiatement à collecter vos journaux de requêtes du résolveur directement depuis Route 53 via un flux d'événements indépendant et dupliqué.

Security Lake ne gère pas vos journaux Route 53 et n'affecte pas les configurations existantes de journalisation des requêtes de votre résolveur. Pour gérer les journaux de requêtes du résolveur, vous devez utiliser la console de service Route 53. Pour plus d'informations, consultez la section Gestion des configurations de journalisation des requêtes du résolveur dans le manuel du développeur Amazon Route 53.

La liste suivante fournit des liens de GitHub référentiel vers la référence cartographique expliquant comment Security Lake normalise les journaux Route 53 vers OCSF.

GitHub Référentiel OCSF pour les journaux de Route 53

- Version 1 de la source (v1.0.0-rc.2)
- Version 2 de la source (v1.1.0)

Conclusions du Security Hub

Les résultats du Security Hub vous aident à comprendre votre niveau de sécurité AWS et vous permettent de vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub collecte les résultats provenant de diverses sources, y compris les intégrations avec d'autres produits tiers AWS services, et effectue des vérifications par rapport aux contrôles du Security Hub. Security Hub traite les résultats dans un format standard appelé AWS Security Finding Format (ASFF).

Lorsque vous ajoutez les résultats de Security Hub en tant que source dans Security Lake, Security Lake commence immédiatement à collecter vos résultats directement auprès de Security Hub via un flux d'événements indépendant et dupliqué. Security Lake transforme également les résultats de l'ASFF au Cadre de schéma de cybersécurité ouvert (OCSF) (OCSF).

Security Lake ne gère pas les résultats de votre Security Hub et n'affecte pas les paramètres de votre Security Hub. Pour gérer les résultats du Security Hub, vous devez utiliser la console de service Security Hub, l'API ou AWS CLI. Pour plus d'informations, consultez la section Conclusions du guide de AWS Security Hub l'utilisateur. AWS Security Hub

La liste suivante fournit des liens de GitHub référentiel vers la référence cartographique expliquant comment Security Lake normalise les résultats de Security Hub par rapport à l'OCSF.

GitHub Référentiel OCSF pour les résultats de Security Hub

- Version 1 de la source (v1.0.0-rc.2)

- Version 2 de la source (v1.1.0)

Journaux de flux VPC

La fonctionnalité VPC Flow Logs d'Amazon VPC capture des informations sur le trafic IP à destination et en provenance des interfaces réseau au sein de votre environnement.

Lorsque vous ajoutez des journaux de flux VPC en tant que source dans Security Lake, Security Lake commence immédiatement à collecter vos journaux de flux VPC. Il consomme les journaux de flux VPC directement depuis Amazon VPC via un flux indépendant et dupliqué de journaux de flux.

Security Lake ne gère pas vos journaux de flux VPC et n'affecte pas vos configurations Amazon VPC. Pour gérer vos journaux de flux, vous devez utiliser la console de service Amazon VPC. Pour plus d'informations, consultez Work with Flow Logs dans le manuel Amazon VPC Developer Guide.

La liste suivante fournit des liens de GitHub référentiel vers la référence de mappage expliquant comment Security Lake normalise les journaux de flux VPC par rapport à OCSF.

GitHub Référentiel OCSF pour les journaux de flux VPC

- Version 1 de la source (v1.0.0-rc.2)
- Version 2 de la source (v1.1.0)

AWS WAF journaux

Lorsque vous les ajoutez en AWS WAF tant que source de journal dans Security Lake, Security Lake commence immédiatement à collecter les journaux. AWS WAF est un pare-feu d'applications Web que vous pouvez utiliser pour surveiller les requêtes Web que vos utilisateurs finaux envoient à vos applications et pour contrôler l'accès à votre contenu. Les informations enregistrées incluent l'heure à laquelle vous avez AWS WAF reçu une demande Web de votre AWS ressource, des informations détaillées sur la demande et des détails sur les règles auxquelles la demande correspondait.

Security Lake consomme AWS WAF des grumes directement AWS WAF par le biais d'un flux de grumes indépendant et dupliqué. Ce processus est conçu pour ne pas nécessiter de configuration supplémentaire ni affecter les AWS WAF configurations existantes que vous pourriez avoir. Pour plus d'informations sur la manière dont vous pouvez AWS WAF protéger les ressources de votre application, consultez la section AWS WAF Fonctionnement du guide du AWS WAF développeur.

> **Important**
>
> Si vous utilisez Amazon CloudFront Distribution comme type de ressource AWS WAF, vous devez sélectionner USA East (Virginie du Nord) pour ingérer les journaux globaux dans Security Lake.

AWS WAF les journaux ne sont pris en charge que dans OCSF v1.1.0. Pour plus d'informations sur la façon dont Security Lake normalise les événements des AWS WAF journaux en OCSF, consultez la référence de mappage dans le référentiel GitHub OCSF pour les AWS WAF journaux (v1.1.0).

Ajouter un AWS service en tant que source

Après avoir ajouté un AWS service en tant que source, Security Lake commence automatiquement à collecter des journaux et des événements de sécurité à partir de celui-ci. Ces instructions vous indiquent comment ajouter une source prise en charge nativement AWS service dans Security Lake. Pour obtenir des instructions sur l'ajout d'une source personnalisée, consultezCollecte de données à partir de sources personnalisées.

Console

Pour ajouter une source de AWS journal (console)

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Choisissez Sources dans le volet de navigation.
3. Sélectionnez AWS service celui à partir duquel vous souhaitez collecter les données, puis choisissez Configurer.
4. Dans la section Paramètres de la source, activez la source et sélectionnez la version de la source de données que vous souhaitez utiliser pour l'ingestion des données. Par défaut, la dernière version de la source de données est ingérée par Security Lake.

   > **Important**
   >
   > Si vous ne disposez pas des autorisations de rôle requises pour activer la nouvelle version de la source de AWS journal dans la région spécifiée, contactez votre administrateur Security Lake. Pour plus d'informations, consultez la section Mettre à jour les autorisations des rôles.

Pour que vos abonnés puissent ingérer la version sélectionnée de la source de données, vous devez également mettre à jour les paramètres de vos abonnés. Pour en savoir plus sur la modification d'un abonné, consultez la section Gestion des abonnés dans Amazon Security Lake.

Vous pouvez éventuellement choisir d'ingérer uniquement la dernière version et de désactiver toutes les versions source précédentes utilisées pour l'ingestion de données.

5. Dans la section Régions, sélectionnez les régions dans lesquelles vous souhaitez collecter des données pour la source. Security Lake collectera les données à la source à partir de tous les comptes des régions sélectionnées.
6. Sélectionnez Activer.

API

Pour ajouter une source de AWS journal (API)

Pour ajouter un AWS service en tant que source par programmation, utilisez le CreateAwsLogSourcefonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande create-aws-log-source. Les paramètres `sourceName` et `regions` sont obligatoires. Vous pouvez éventuellement limiter la portée de la source à un élément spécifique `accounts` ou spécifique`sourceVersion`.

> **Important**
>
> Lorsque vous ne fournissez aucun paramètre dans votre commande, Security Lake part du principe que le paramètre manquant fait référence à l'ensemble complet. Par exemple, si vous ne fournissez pas le `accounts` paramètre, la commande s'applique à l'ensemble des comptes de votre organisation.

L'exemple suivant ajoute les journaux de flux VPC en tant que source dans les comptes et régions désignés. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

> **Note**
>
> Si vous appliquez cette demande à une région dans laquelle vous n'avez pas activé Security Lake, vous recevrez un message d'erreur. Vous pouvez résoudre l'erreur en activant Security Lake dans cette région ou en utilisant le `regions` paramètre pour spécifier uniquement les régions dans lesquelles vous avez activé Security Lake.

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

Mettre à jour les autorisations des rôles

Si vous ne disposez pas des autorisations ou des ressources requises (nouvelle AWS Lambda fonction et file d'attente Amazon Simple Queue Service (Amazon SQS) pour ingérer les données d'une nouvelle version de la source de données, vous devez mettre à jour les autorisations de rôle et créer un nouvel ensemble de ressources pour traiter les données provenant de `AmazonSecurityLakeMetaStoreManagerV2` vos sources.

Choisissez votre méthode préférée et suivez les instructions pour mettre à jour les autorisations de votre rôle et créer de nouvelles ressources pour traiter les données d'une nouvelle version d'une source de AWS journal dans une région spécifiée. Il s'agit d'une action ponctuelle, car les autorisations et les ressources sont automatiquement appliquées aux futures versions des sources de données.

Console

Pour mettre à jour les autorisations des rôles (console)

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous avec les informations d'identification de l'administrateur délégué de Security Lake.
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Choisissez Mettre à jour les autorisations de rôle.
4. Dans la section Accès au service, effectuez l'une des opérations suivantes :

- Créer et utiliser un nouveau rôle de service : vous pouvez utiliser le rôle AmazonSecurityLakeMetaStoreManagerV2 créé par Security Lake.
- Utiliser un rôle de service existant : vous pouvez choisir un rôle de service existant dans la liste des noms de rôle de service.

5. Choisissez Appliquer.

API

Pour mettre à jour les autorisations de rôle (API)

Pour mettre à jour les autorisations par programmation, utilisez le UpdateDataLakefonctionnement de l'API Security Lake. Pour mettre à jour les autorisations à l'aide de AWS CLI, exécutez la update-data-lakecommande.

Pour mettre à jour les autorisations de votre rôle, vous devez associer la AmazonSecurityLakeMetastoreManagerpolitique au rôle.

Supprimer le AmazonSecurityLakeMetaStoreManager rôle

> **Important**
>
> Après avoir mis à jour les autorisations de votre rôle`AmazonSecurityLakeMetaStoreManagerV2`, vérifiez que le lac de données fonctionne correctement avant de supprimer l'ancien `AmazonSecurityLakeMetaStoreManager` rôle. Il est recommandé d'attendre au moins 4 heures avant de supprimer le rôle.

Si vous décidez de supprimer le rôle, vous devez d'abord le `AmazonSecurityLakeMetaStoreManager` supprimer de AWS Lake Formation.

Procédez comme suit pour supprimer le `AmazonSecurityLakeMetaStoreManager` rôle de la console Lake Formation.

1. Connectez-vous à la AWS Management Console console Lake Formation et ouvrez-la à l'adresse https://console.aws.amazon.com/lakeformation/.

2. Dans la console Lake Formation, dans le volet de navigation, sélectionnez Administrative roles and tasks.
3. Supprimer `AmazonSecurityLakeMetaStoreManager` de chaque région.

Supprimer un AWS service en tant que source

Choisissez votre méthode d'accès et suivez ces étapes pour supprimer une source Security Lake prise AWS service en charge nativement. Vous pouvez supprimer une source pour une ou plusieurs régions. Lorsque vous supprimez la source, Security Lake arrête de collecter les données de cette source dans les régions et les comptes spécifiés, et les abonnés ne peuvent plus consommer de nouvelles données provenant de la source. Toutefois, les abonnés peuvent toujours consommer les données collectées par Security Lake à la source avant leur suppression. Vous ne pouvez utiliser ces instructions que pour supprimer une source prise en charge nativement AWS service . Pour plus d'informations sur la suppression d'une source personnalisée, consultezCollecte de données à partir de sources personnalisées.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Choisissez Sources dans le volet de navigation.
3. Sélectionnez une source, puis choisissez Désactiver.
4. Sélectionnez une ou plusieurs régions dans lesquelles vous souhaitez arrêter de collecter des données à partir de cette source. Security Lake cessera de collecter les données à la source à partir de tous les comptes des régions sélectionnées.

API

Pour supprimer un AWS service en tant que source par programmation, utilisez le DeleteAwsLogSourcefonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande delete-aws-log-source. Les paramètres `sourceName` et `regions` sont obligatoires. Vous pouvez éventuellement limiter l'étendue de la suppression à un champ spécifique `accounts` ou spécifique`sourceVersion`.

> **Important**
>
> Lorsque vous ne fournissez aucun paramètre dans votre commande, Security Lake part du principe que le paramètre manquant fait référence à l'ensemble complet. Par exemple,

si vous ne fournissez pas le `accounts` paramètre, la commande s'applique à l'ensemble des comptes de votre organisation.

L'exemple suivant supprime les journaux de flux VPC en tant que source dans les comptes et régions désignés.

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

L'exemple suivant supprime Route 53 en tant que source dans le compte et les régions désignés.

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

Les exemples précédents sont formatés pour Linux, macOS ou Unix, et ils utilisent la barre oblique inverse (\) pour améliorer la lisibilité.

Obtenir le statut de la collection de sources

Choisissez votre méthode d'accès et suivez les étapes pour obtenir un aperçu des comptes et des sources pour lesquels la collecte de journaux est activée dans la région actuelle.

Console

Pour connaître l'état de la collecte des journaux dans la région actuelle

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, sélectionnez Accounts.
3. Passez le curseur sur le nombre dans la colonne Sources pour voir quels journaux sont activés pour le compte sélectionné.

API

Pour connaître l'état de la collecte de logs dans la région actuelle, utilisez le GetDataLakeSourcesfonctionnement de l'API Security Lake. Si vous utilisez le AWS CLI, exécutez la commande get-data-lake-sources. Pour le `accounts` paramètre, vous pouvez spécifier un ou plusieurs Compte AWS identifiants sous forme de liste. Si votre demande aboutit, Security Lake renvoie un instantané de ces comptes dans la région actuelle, y compris les AWS sources auprès desquelles Security Lake collecte des données et le statut de chaque source. Si vous n'incluez pas le `accounts` paramètre, la réponse inclut l'état de la collecte des journaux pour tous les comptes dans lesquels Security Lake est configuré dans la région actuelle.

Par exemple, la AWS CLI commande suivante permet de récupérer l'état de collecte des journaux pour les comptes spécifiés dans la région actuelle. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Collecte de données à partir de sources personnalisées

Amazon Security Lake peut collecter des journaux et des événements à partir de sources personnalisées tierces. Pour chaque source personnalisée, Security Lake gère les opérations suivantes :

- Fournit un préfixe unique pour la source dans votre compartiment Amazon S3.
- Crée un rôle dans AWS Identity and Access Management (IAM) qui permet à une source personnalisée d'écrire des données dans le lac de données. La limite des autorisations pour ce rôle est définie par une politique AWS gérée appelée `AmazonSecurityLakePermissionsBoundary`.
- Crée un AWS Lake Formation tableau pour organiser les objets que la source écrit dans Security Lake.
- Configure un AWS Glue robot d'exploration pour partitionner vos données sources. Le robot d'exploration remplit le AWS Glue Data Catalog avec le tableau. Il découvre également automatiquement les nouvelles données sources et extrait les définitions de schéma.

Pour ajouter une source personnalisée à Security Lake, celle-ci doit répondre aux exigences suivantes :

1. Destination — La source personnalisée doit être capable d'écrire des données dans Security Lake sous la forme d'un ensemble d'objets S3 sous le préfixe attribué à la source. Pour les sources contenant plusieurs catégories de données, vous devez fournir chaque classe d'événements Open Cybersecurity Schema Framework (OCSF) unique en tant que source distincte. Security Lake crée un IAM rôle qui permet à la source personnalisée d'écrire à l'emplacement spécifié dans votre compartiment S3.

   > **Note**
   >
   > Utilisez l'outil de OCSF validation pour vérifier si la source personnalisée est compatible avec`OCSF Schema 1.1`.

2. Format — Chaque objet S3 collecté à partir de la source personnalisée doit être formaté en tant que fichier Apache Parquet.
3. Schéma — La même classe OCSF d'événement doit s'appliquer à chaque enregistrement d'un objet au format Parquet.

Bonnes pratiques pour l'ingestion de sources personnalisées

Pour faciliter le traitement des données et les requêtes efficaces, nous vous recommandons de suivre les meilleures pratiques suivantes lors de l'ajout d'une source personnalisée à Security Lake :

Partitionnement

Les objets doivent être partitionnés par emplacement source, Région AWS Compte AWS, et date.

- Le chemin des données de partition est formaté comme suit :

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

  Un exemple de partition estaws-security-data-lake-*us-west-2-lake-uid*/ext/*custom-source-name*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/.
- Si vous avez ajouté une version source à une source personnalisée, le chemin des données de partition est formaté comme suit :

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

Un exemple de partition qui inclut la version source estaws-security-data-lake-*us-west-2-lake-uid*/ext/*custom-source-name*/*custom-source-version*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/.

La liste suivante décrit les paramètres utilisés dans la partition.

- `bucket-name`— Le nom du compartiment Amazon S3 dans lequel Security Lake stocke vos données source personnalisées.
- `source-location`— Préfixe pour la source personnalisée dans votre compartiment S3. Security Lake stocke tous les objets S3 d'une source donnée sous ce préfixe, et le préfixe est unique à la source donnée.
- `source-version`— Version source de la source personnalisée.
- `region`— Région AWS dans lequel les données sont écrites.
- `accountId`— Compte AWS Identifiant auquel se rapportent les enregistrements de la partition source.
- `eventDay`— Date à laquelle l'événement s'est produit, sous la forme d'une chaîne de huit caractères (`YYYYMMDD`).

Taille et débit de l'objet

Les fichiers envoyés à Security Lake doivent être envoyés par tranches entre 5 minutes et 1 jour d'événement. Les clients peuvent envoyer des fichiers plus de 5 minutes si la taille des fichiers est supérieure à 256 Mo. L'objet et la taille requis visent à optimiser le lac de sécurité pour les performances des requêtes. Le non-respect des exigences relatives aux sources personnalisées peut avoir un impact sur les performances de votre Security Lake.

Réglages du parquet

Security Lake prend en charge les versions 1.x et 2.x de Parquet. La taille de la page de données doit être limitée à 1 Mo (non compressée). La taille du groupe de lignes ne doit pas dépasser 256 Mo (compressé). Pour la compression au sein de l'objet Parquet, il est préférable d'utiliser zstandard.

Tri

Dans chaque objet au format Parquet, les enregistrements doivent être classés par ordre chronologique afin de réduire le coût des requêtes de données.

Conditions préalables à l'ajout d'une source personnalisée

Lors de l'ajout d'une source personnalisée, Security Lake crée un IAM rôle qui permet à la source d'écrire les données au bon emplacement dans le lac de données. Le nom du rôle suit le format`AmazonSecurityLake-Provider-{name of the custom source}-{region}`, où `region` est celui Région AWS dans lequel vous ajoutez la source personnalisée. Security Lake associe une politique au rôle qui autorise l'accès au lac de données. Si vous avez chiffré le lac de données à l'aide d'une AWS KMS clé gérée par le client, Security Lake associe également une politique `kms:Decrypt` et `kms:GenerateDataKey` des autorisations au rôle. La limite des autorisations pour ce rôle est définie par une politique AWS gérée appelée `AmazonSecurityLakePermissionsBoundary`.

Rubriques

Vérifier les autorisations

Avant d'ajouter une source personnalisée, vérifiez que vous êtes autorisé à effectuer les actions suivantes.

Pour vérifier vos autorisations, IAM consultez les IAM politiques associées à votre IAM identité. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions que vous devez être autorisé à effectuer pour ajouter une source personnalisée.

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StopCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`

- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

Ces actions vous permettent de collecter des journaux et des événements à partir d'une source personnalisée, de les envoyer vers la AWS Glue base de données et la table appropriées, et de les stocker dans Amazon S3.

Si vous utilisez une AWS KMS clé pour le chiffrement côté serveur de votre lac de données, vous devez également obtenir une autorisation pour `kms:CreateGrantkms:DescribeKey`, et. `kms:GenerateDataKey`

> **Important**
>
> Si vous prévoyez d'utiliser la console Security Lake pour ajouter une source personnalisée, vous pouvez ignorer l'étape suivante et passer àAjouter une source personnalisée. La console Security Lake propose un processus de démarrage simplifié et crée tous les IAM rôles nécessaires ou utilise les rôles existants en votre nom.
> Si vous prévoyez d'utiliser Security Lake API ou d' AWS CLI ajouter une source personnalisée, passez à l'étape suivante pour créer un IAM rôle permettant l'accès en écriture à l'emplacement du bucket Security Lake.

Créer un IAM rôle pour autoriser l'accès en écriture à l'emplacement du bucket Security Lake (APIet étape AWS CLI uniquement)

Si vous utilisez Security Lake API ou si vous AWS CLI souhaitez ajouter une source personnalisée, ajoutez ce IAM rôle pour AWS Glue autoriser l'analyse de vos données source personnalisées et l'identification des partitions dans les données. Ces partitions sont nécessaires pour organiser vos données et créer et mettre à jour des tables dans le catalogue de données.

Après avoir créé ce IAM rôle, vous aurez besoin du nom de ressource Amazon (ARN) du rôle pour ajouter une source personnalisée.

Vous devez joindre la politique `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS gérée.

Pour accorder les autorisations nécessaires, vous devez également créer et intégrer la politique en ligne suivante dans votre rôle afin de permettre AWS Glue crawler de lire les fichiers de données à partir de la source personnalisée et de créer/mettre à jour les tables dans le catalogue de données. AWS Glue

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

Joignez la politique de confiance suivante pour autoriser et en Compte AWS utilisant laquelle, il peut assumer le rôle en fonction de l'ID externe :

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

Si le compartiment S3 de la région dans laquelle vous ajoutez la source personnalisée est chiffré à l'aide d'un compartiment géré par le client AWS KMS key, vous devez également associer la politique suivante au rôle et à votre politique KMS clé :

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

Ajouter une source personnalisée

Après avoir créé le IAM rôle permettant d'invoquer le AWS Glue robot d'exploration, procédez comme suit pour ajouter une source personnalisée dans Security Lake.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez créer la source personnalisée.
3. Choisissez Sources personnalisées dans le volet de navigation, puis choisissez Créer une source personnalisée.
4. Dans la section Détails de la source personnalisée, entrez un nom unique au monde pour votre source personnalisée. Sélectionnez ensuite une classe d'OCSFévénements qui décrit le type de données que la source personnalisée enverra à Security Lake.
5. Si vous Compte AWS êtes autorisé à écrire des données, entrez l'Compte AWS ID et l'ID externe de la source personnalisée qui enregistrera les journaux et les événements dans le lac de données.
6. Pour l'accès aux services, créez et utilisez un nouveau rôle de service ou utilisez un rôle de service existant qui autorise Security Lake à invoquer AWS Glue.

7. Sélectionnez Create (Créer).

API

Pour ajouter une source personnalisée par programmation, utilisez le CreateCustomLogSourcefonctionnement du Security Lake. API Utilisez l'opération à l' Région AWS endroit où vous souhaitez créer la source personnalisée. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la create-custom-log-sourcecommande.

Dans votre demande, utilisez les paramètres pris en charge pour définir les paramètres de configuration de la source personnalisée :

- `sourceName`— Spécifiez le nom de la source. Le nom doit être une valeur unique au niveau régional.
- `eventClasses`— Spécifiez une ou plusieurs classes d'OCSFévénements pour décrire le type de données que la source enverra à Security Lake. Pour obtenir la liste des classes d'OCSFévénements prises en charge en tant que source dans Security Lake, consultez Open Cybersecurity Schema Framework (OCSF).
- `sourceVersion`— Spécifiez éventuellement une valeur pour limiter la collecte de journaux à une version spécifique de données source personnalisées.
- `crawlerConfiguration`— Spécifiez le nom de ressource Amazon (ARN) du IAM rôle que vous avez créé pour appeler le AWS Glue robot d'exploration. Pour les étapes détaillées de création d'un IAM rôle, voir Conditions préalables à l'ajout d'une source personnalisée
- `providerIdentity`— Spécifiez l' AWS identité et l'ID externe que la source utilisera pour écrire les journaux et les événements dans le lac de données.

L'exemple suivant ajoute une source personnalisée en tant que source de journal dans le compte du fournisseur de journaux désigné dans les régions désignées. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ 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”]
```

Maintien à jour des données source personnalisées dans AWS Glue

Après avoir ajouté une source personnalisée dans Security Lake, Security Lake crée un AWS Glue robot d'exploration. Le robot d'exploration se connecte à votre source personnalisée, détermine les structures de données et remplit le catalogue de AWS Glue données avec des tables.

Nous vous recommandons d'exécuter le robot manuellement pour maintenir votre schéma source personnalisé à jour et maintenir les fonctionnalités de requête dans Athena et les autres services de requête. Plus précisément, vous devez exécuter le robot si l'une des modifications suivantes se produit dans votre ensemble de données d'entrée pour une source personnalisée :

- L'ensemble de données comporte une ou plusieurs nouvelles colonnes de niveau supérieur.
- L'ensemble de données comporte un ou plusieurs nouveaux champs dans une colonne avec un type de `struct` données.

Pour obtenir des instructions sur l'exécution d'un robot d'exploration, consultez la section Planification d'un AWS Glue robot d'exploration dans le Guide du AWS Glue développeur.

Security Lake ne peut ni supprimer ni mettre à jour les robots d'exploration existants de votre compte. Si vous supprimez une source personnalisée, nous vous recommandons de supprimer le robot d'exploration associé si vous envisagez de créer une source personnalisée portant le même nom à l'avenir.

Supprimer une source personnalisée

Supprimez une source personnalisée pour arrêter d'envoyer des données de la source à Security Lake.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dont vous souhaitez supprimer la source personnalisée.
3. Dans le volet de navigation, sélectionnez Sources personnalisées.
4. Sélectionnez la source personnalisée que vous souhaitez supprimer.
5. Choisissez Désenregistrer la source personnalisée, puis sélectionnez Supprimer pour confirmer l'action.

API

Pour supprimer une source personnalisée par programmation, utilisez DeleteCustomLogSourcele Security Lake. API Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la delete-custom-log-sourcecommande. Utilisez l'opération dans Région AWS laquelle vous souhaitez supprimer la source personnalisée.

Dans votre demande, utilisez le `sourceName` paramètre pour spécifier le nom de la source personnalisée à supprimer. Vous pouvez également spécifier le nom de la source personnalisée et utiliser le `sourceVersion` paramètre pour limiter l'étendue de la suppression à une version spécifique des données de la source personnalisée.

L'exemple suivant supprime une source de journal personnalisée de Security Lake.

Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

Gestion des abonnés dans Amazon Security Lake

Un abonné Amazon Security Lake consomme les journaux et les événements de Security Lake. Pour contrôler les coûts et respecter les meilleures pratiques en matière d'accès au moindre privilège, vous permettez aux abonnés d'accéder aux données par source. Pour plus d'informations sur les sources, consultez gestion des sources dans Amazon Security Security Security Security Security Security Security Security.

Security Lake prend en charge deux types d'accès pour les abonnés :

- Accès aux données — Les abonnés sont informés de la présence de nouveaux objets Amazon S3 pour une source au fur et à mesure que les objets sont écrits dans le data lake de Security Lake. Les abonnés peuvent accéder directement aux objets S3 et recevoir des notifications concernant les nouveaux objets via un point de terminaison d'abonnement ou en interrogeant une file d'attente Amazon Simple Queue Service (Amazon SQS). Ce type d'abonnement est identifié comme `S3` dans le `accessTypes` paramètre de l'CreateSubscriberAPI.
- Accès aux requêtes : les abonnés interrogent les données sources à partir AWS Lake Formation des tables de votre compartiment S3 à l'aide de services tels qu'Amazon Athena. Ce type d'abonnement est identifié comme `LAKEFORMATION` dans le `accessTypes` paramètre de l'CreateSubscriberAPI.

Les abonnés ont uniquement accès aux données source Région AWS que vous sélectionnez lorsque vous créez l'abonné. Pour permettre à un abonné d'accéder aux données de plusieurs régions, vous pouvez spécifier la région dans laquelle vous créez l'abonné en tant que région cumulative et demander à d'autres régions de fournir des données. Pour plus d'informations sur les régions cumulatives et les régions contributrices, consultez. Gestion des régions

> **Important**
>
> Le nombre maximum de sources que Security Lake autorise à ajouter par abonné est de 10. Il peut s'agir d'une combinaison de AWS sources et de sources personnalisées.

Rubriques

- Gestion de l'accès aux données pour les abonnés de Security Lake
- Gestion de l'accès aux requêtes pour les abonnés de Security Lake

Gestion de l'accès aux données pour les abonnés de Security Lake

Les abonnés ayant accès aux données source dans Amazon Security Lake sont informés de la présence de nouveaux objets pour la source au fur et à mesure que les données sont écrites dans le compartiment S3. Par défaut, les abonnés sont informés des nouveaux objets via un point de terminaison HTTPS qu'ils fournissent. Les abonnés peuvent également être informés des nouveaux objets en interrogeant une file d'attente Amazon Simple Queue Service (Amazon SQS).

Conditions préalables à la création d'un abonné avec accès aux données

Vous devez remplir les conditions préalables suivantes avant de pouvoir créer un abonné ayant accès aux données dans Security Lake.

Rubriques

Vérifier les autorisations

Pour vérifier vos autorisations, utilisez IAM pour passer en revue les politiques IAM associées à votre identité IAM. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions (autorisations) que vous devez effectuer pour informer les abonnés lorsque de nouvelles données sont écrites dans le lac de données.

Vous aurez besoin d'une autorisation pour effectuer les actions suivantes :

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

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

Outre la liste précédente, vous devez également être autorisé à effectuer les actions suivantes :

- `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`

Obtenez l'identifiant externe de l'abonné

Pour créer un abonné, outre son Compte AWS identifiant, vous devez également obtenir son identifiant externe. L'identifiant externe est un identifiant unique que l'abonné vous fournit. Security Lake ajoute l'ID externe au rôle IAM d'abonné qu'il crée. Vous utilisez l'ID externe lorsque vous créez un abonné dans la console Security Lake, via l'API, ou AWS CLI.

Pour plus d'informations sur les identifiants externes, consultez la section Comment utiliser un identifiant externe lorsque vous accordez l'accès à vos AWS ressources à un tiers dans le guide de l'utilisateur IAM.

> **Important**
>
> Si vous prévoyez d'utiliser la console Security Lake pour ajouter un abonné, vous pouvez ignorer l'étape suivante et passer àCréation d'un abonné avec accès aux données. La console Security Lake propose un processus de démarrage rationalisé et crée tous les rôles IAM nécessaires ou utilise les rôles existants en votre nom.
> Si vous prévoyez d'utiliser l'API Security Lake ou d' AWS CLI ajouter un abonné, passez à l'étape suivante qui consiste à créer un rôle IAM pour appeler les destinations d' EventBridge API.

Créer un rôle IAM pour appeler des destinations EventBridge d'API (API et étape AWS CLI uniquement)

Si vous utilisez Security Lake via une API ou AWS CLI si vous créez un rôle dans AWS Identity and Access Management (IAM) qui autorise Amazon à invoquer des destinations EventBridge d'API et à envoyer des notifications d'objets aux points de terminaison HTTPS appropriés.

Après avoir créé ce rôle IAM, vous aurez besoin du nom de ressource Amazon (ARN) du rôle pour créer l'abonné. Ce rôle IAM n'est pas nécessaire si l'abonné interroge les données d'une file d'attente Amazon Simple Queue Service (Amazon SQS) ou interroge directement les données auprès de celle-ci. AWS Lake Formation Pour plus d'informations sur ce type de méthode d'accès aux données (type d'accès), consultezGestion de l'accès aux requêtes pour les abonnés de Security Lake.

Associez la politique suivante à votre rôle IAM :

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

```
        }
    ]
}
```

Associez la politique de confiance suivante à votre rôle IAM pour vous EventBridge permettre d'assumer ce rôle :

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

Security Lake crée automatiquement un rôle IAM qui permet à l'abonné de lire les données du lac de données (ou d'interroger les événements d'une file d'attente Amazon SQS s'il s'agit de la méthode de notification préférée). Ce rôle est protégé par une politique AWS gérée appelée `AmazonSecurityLakePermissionsBoundary`.

Création d'un abonné avec accès aux données

Choisissez l'une des méthodes d'accès suivantes pour créer un abonné ayant accès aux données actuelles Région AWS.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez créer l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, choisissez Créer un abonné.
5. Pour les détails de l'abonné, entrez le nom de l'abonné et une description facultative.

La région est automatiquement renseignée comme vous l'avez actuellement sélectionnée Région AWS et ne peut pas être modifiée.

6. Pour les sources de journaux et d'événements, choisissez les sources que l'abonné est autorisé à utiliser.
7. Pour la méthode d'accès aux données, choisissez S3 pour configurer l'accès aux données pour l'abonné.
8. Pour les informations d'identification de l'abonné, fournissez l' Compte AWS identifiant de l'abonné et l'identifiant externe.
9. (Facultatif) Pour les détails des notifications, si vous souhaitez que Security Lake crée une file d'attente Amazon SQS que l'abonné peut interroger pour les notifications d'objets, sélectionnez la file d'attente SQS. Si vous souhaitez que Security Lake envoie des notifications EventBridge à un point de terminaison HTTPS, sélectionnez Point de terminaison d'abonnement.

   Si vous sélectionnez Point de terminaison d'abonnement, procédez également comme suit :

   a. Entrez le point de terminaison de l'abonnement. Voici des exemples de formats de point de terminaison valides**`http://example.com`**. Facultativement, vous pouvez également fournir un nom de clé HTTPS et une valeur de clé HTTPS.
   b. Pour l'accès aux services, créez un nouveau rôle IAM ou utilisez un rôle IAM existant qui donne l' EventBridgeautorisation d'invoquer des destinations d'API et d'envoyer des notifications d'objets aux points de terminaison appropriés.

      Pour plus d'informations sur la création d'un nouveau rôle IAM, voir Créer un rôle IAM pour appeler des destinations d' EventBridge API.
10. (Facultatif) Pour Tags, entrez jusqu'à 50 tags à attribuer à l'abonné.

    Un tag est un label que vous pouvez définir et attribuer à certains types de AWS ressources. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières. Pour en savoir plus, veuillez consulter la section Marquage des ressources d'Amazon Security Lake.
11. Choisissez Créer.

API

Pour créer un abonné avec accès aux données par programmation, utilisez le CreateSubscriberfonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande create-subscriber.

Dans votre demande, utilisez ces paramètres pour définir les paramètres suivants pour l'abonné :

- Poursources, spécifiez chaque source à laquelle vous souhaitez que l'abonné accède.
- PoursubscriberIdentity, spécifiez l'ID de AWS compte et l'ID externe que l'abonné utilisera pour accéder aux données sources.
- Poursubscriber-name, spécifiez le nom de l'abonné.
- Pour accessTypes, spécifiez S3.

Exemple 1

L'exemple suivant crée un abonné ayant accès aux données de la AWS région actuelle pour l'identité d'abonné spécifiée pour une AWS source.

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

Exemple 2

L'exemple suivant crée un abonné ayant accès aux données de la AWS région actuelle pour l'identité d'abonné spécifiée pour une source personnalisée.

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

Les exemples précédents sont formatés pour Linux, macOS ou Unix, et ils utilisent le caractère de continuation de ligne inversée (\) pour améliorer la lisibilité.

(Facultatif) Après avoir créé un abonné, utilisez l'opération de CreateSubscribernotification pour spécifier comment avertir l'abonné lorsque de nouvelles données sont écrites dans le lac de données pour les sources auxquelles vous souhaitez que l'abonné accède. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande create-subscriber-notification.

- Pour remplacer la méthode de notification par défaut (point de terminaison HTTPS) et créer une file d'attente Amazon SQS, spécifiez des valeurs pour `sqsNotificationConfiguration` les paramètres.
- Si vous préférez une notification via un point de terminaison HTTPS, spécifiez des valeurs pour les `httpsNotificationConfiguration` paramètres.
- Pour le `targetRoleArn` champ, spécifiez l'ARN du rôle IAM que vous avez créé pour appeler les destinations d' EventBridge 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"}
```

Pour l'obtenir`subscriberID`, utilisez le ListSubscribersfonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande list-subscriber.

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

Pour modifier ultérieurement la méthode de notification (file d'attente Amazon SQS ou point de terminaison HTTPS) pour l'abonné, utilisez l'opération UpdateSubscriberNotification ou, si vous utilisez le AWS CLI, exécutez la commande update-subscriber-notification. Vous pouvez également modifier le mode de notification à l'aide de la console Security Lake : sélectionnez l'abonné sur la page Abonnés, puis choisissez Modifier.

Exemple de message de notification d'objet

```
{
  "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"
  }
}
```

Mettre à jour un abonné aux données

Vous pouvez mettre à jour un abonné en modifiant les sources à partir desquelles il consomme. Vous pouvez également attribuer ou modifier les tags d'un abonné. Un tag est un label que vous pouvez définir et attribuer à certains types de AWS ressources, y compris les abonnés. Pour en savoir plus, veuillez consulter la section Marquage des ressources d'Amazon Security Lake.

Choisissez l'une des méthodes d'accès et suivez ces étapes pour définir de nouvelles sources pour un abonnement existant.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, choisissez Subscribers.
3. Sélectionnez l'abonné.
4. Choisissez Modifier, puis effectuez l'une des opérations suivantes :
   - Pour mettre à jour les sources de l'abonné, entrez les nouveaux paramètres dans la section Log and event sources.
   - Pour attribuer ou modifier des balises à l'abonné, modifiez les balises selon les besoins dans la section Tags.
5. Lorsque vous avez terminé, choisissez Enregistrer.

API

Pour mettre à jour les sources d'accès aux données d'un abonné par programmation, utilisez le UpdateSubscriberfonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande update-subscriber. Dans votre demande, utilisez les `sources` paramètres pour spécifier chaque source à laquelle vous souhaitez que l'abonné accède.

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

Pour obtenir la liste des abonnés associés à une organisation Compte AWS ou à une organisation spécifique, utilisez l'ListSubscribersopération. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande list-subscribers.

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

Pour vérifier les paramètres actuels d'un abonné en particulier, utilisez l'GetSubscriberopération suivante : exécutez la commande get-subscriber. Security Lake renvoie ensuite le nom et la description de l'abonné, son identifiant externe et des informations supplémentaires. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande get-subscriber.

Pour mettre à jour la méthode de notification pour un abonné, utilisez l'opération UpdateSubscriberNotification. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande update-subscriber-notification. Par exemple, vous pouvez spécifier un nouveau point de terminaison HTTPS pour l'abonné ou passer d'un point de terminaison HTTPS à une file d'attente Amazon SQS.

Supprimer un abonné aux données

Si vous ne souhaitez plus qu'un abonné consomme les données de Security Lake, vous pouvez le supprimer en suivant ces étapes.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, choisissez Subscribers.
3. Sélectionnez l'abonné que vous souhaitez supprimer.

4. Choisissez Delete (Supprimer) et confirmez l'action. Cela supprimera l'abonné et tous les paramètres de notification associés.

API

Selon votre scénario, effectuez l'une des opérations suivantes :

- Pour supprimer l'abonné et tous les paramètres de notification associés, utilisez l'DeleteSubscriberAPI Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande delete-subscriber.
- Pour conserver l'abonné mais arrêter de lui envoyer de futures notifications, utilisez l'opération DeleteSubscriberNotification de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande run the delete-subscriber-notification.

Gestion de l'accès aux requêtes pour les abonnés de Security Lake

Les abonnés disposant d'un accès aux requêtes peuvent interroger les données collectées par Security Lake. Ces abonnés interrogent directement AWS Lake Formation les tables de votre compartiment S3 à l'aide de services tels qu'Amazon Athena. Bien que le moteur de requête principal de Security Lake soit Athena, vous pouvez également utiliser d'autres services, tels qu'Amazon Redshift Spectrum et Spark SQL, qui s'intègrent au. AWS Glue Data Catalog

> **Note**
>
> Cette section explique comment accorder l'accès aux requêtes à un abonné tiers. Pour plus d'informations sur l'exécution de requêtes sur votre propre lac de données, consultezÉtape 4 : Afficher et interroger vos propres données.

Conditions préalables à la création d'un abonné avec accès aux requêtes

Vous devez remplir les conditions préalables suivantes avant de pouvoir créer un abonné ayant accès aux données dans Security Lake.

Rubriques

- Vérifier les autorisations

- Créer un rôle IAM pour interroger les données de Security Lake (API et étape AWS CLI uniquement)
- Autorisations d'administrateur de Grant Lake Formation

Vérifier les autorisations

Avant de créer un abonné avec accès aux requêtes, vérifiez que vous êtes autorisé à effectuer la liste d'actions suivante.

Pour vérifier vos autorisations, utilisez IAM pour passer en revue les politiques IAM associées à votre identité IAM. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions que vous devez être autorisé à effectuer pour créer un abonné avec accès aux requêtes.

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

> **Important**
>
> Après avoir vérifié les autorisations :
>
> - Si vous prévoyez d'utiliser la console Security Lake pour ajouter un abonné ayant accès aux requêtes, vous pouvez ignorer l'étape suivante et passer àAutorisations d'administrateur de Grant Lake Formation. Security Lake crée tous les rôles IAM nécessaires ou utilise les rôles existants en votre nom.

- Si vous prévoyez d'utiliser l'API ou la CLI de Security Lake pour ajouter un abonné ayant accès aux requêtes, passez à l'étape suivante qui consiste à créer un rôle IAM pour interroger les données de Security Lake.

Créer un rôle IAM pour interroger les données de Security Lake (API et étape AWS CLI uniquement)

Lorsque vous utilisez l'API Security Lake ou AWS CLI pour accorder l'accès aux requêtes à un abonné, vous devez créer un rôle nomméAmazonSecurityLakeMetaStoreManager. Security Lake utilise ce rôle pour enregistrer les AWS Glue partitions et mettre à jour AWS Glue les tables. Vous avez peut-être déjà créé ce rôle lors de la création des rôles IAM nécessaires.

Autorisations d'administrateur de Grant Lake Formation

Vous devez également ajouter des autorisations d'administrateur de Lake Formation au rôle IAM que vous utilisez pour accéder à la console Security Lake et ajouter des abonnés.

Vous pouvez accorder des autorisations d'administrateur à Lake Formation pour accéder à votre rôle en suivant ces étapes :

1. Ouvrez la console Lake Formation à l'adresse https://console.aws.amazon.com/lakeformation/.
2. Connectez-vous en tant qu'utilisateur administratif.
3. Si une fenêtre Welcome to Lake Formation apparaît, choisissez l'utilisateur que vous avez créé ou sélectionné à l'étape 1, puis choisissez Get started.
4. Si la fenêtre Welcome to Lake Formation ne s'affiche pas, effectuez les étapes suivantes pour configurer un administrateur de Lake Formation.
    1. Dans le volet de navigation, sous Autorisations, sélectionnez Rôles et tâches administratifs. Dans la section Administrateurs du lac de données, choisissez Choisir les administrateurs.
    2. Dans la boîte de dialogue Gérer les administrateurs de lacs de données, pour les utilisateurs et les rôles IAM, choisissez le rôle d'administrateur utilisé lors de l'accès à la console Security Lake, puis sélectionnez Enregistrer.

Pour plus d'informations sur la modification des autorisations pour les administrateurs de lacs de données, voir Création d'un administrateur de lac de données dans le guide du AWS Lake Formation développeur.

Le rôle IAM doit disposer de `SELECT` privilèges sur la base de données et les tables auxquelles vous souhaitez accorder l'accès à un abonné. Pour savoir comment procéder, consultez la section Octroi d'autorisations au catalogue de données à l'aide de la méthode des ressources nommées dans le guide du AWS Lake Formation développeur.

Création d'un abonné avec accès aux requêtes

Choisissez votre méthode préférée pour créer un abonné avec accès aux requêtes en cours Région AWS. Un abonné ne peut interroger des données qu'à partir du Région AWS fichier dans lequel elles ont été créées. Pour créer un abonné, vous devez disposer de l' Compte AWS identifiant et de l'identifiant externe de l'abonné. L'identifiant externe est un identifiant unique que l'abonné vous fournit. Pour plus d'informations sur les identifiants externes, consultez la section Comment utiliser un identifiant externe lorsque vous accordez l'accès à vos AWS ressources à un tiers dans le guide de l'utilisateur IAM.

> **Note**
>
> Security Lake ne prend pas en charge le partage de données entre comptes Lake Formation version 1. Vous devez mettre à jour le partage de données entre comptes de Lake Formation vers la version 2 ou la version 3. Pour connaître les étapes de mise à jour des paramètres de version entre comptes via la AWS Lake Formation console ou la AWS CLI, voir Pour activer la nouvelle version dans le guide du AWS Lake Formation développeur.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous au compte d'administrateur délégué.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez créer l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, choisissez Créer un abonné.
5. Pour les détails de l'abonné, entrez un nom d'abonné et une description facultative.

   La région est automatiquement renseignée comme vous l'avez actuellement sélectionnée Région AWS et ne peut pas être modifiée.

6. Pour les sources de journaux et d'événements, choisissez les sources que Security Lake doit inclure lors du renvoi des résultats de requête.
7. Pour la méthode d'accès aux données, choisissez Lake Formation pour créer un accès aux requêtes pour l'abonné.
8. Pour les informations d'identification de l'abonné, fournissez l' Compte AWS identifiant de l'abonné et l'identifiant externe.
9. (Facultatif) Pour Tags, entrez jusqu'à 50 tags à attribuer à l'abonné.

   Un tag est un label que vous pouvez définir et attribuer à certains types de AWS ressources. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières. Pour en savoir plus, veuillez consulter la section Marquage des ressources d'Amazon Security Lake.
10. Choisissez Créer.

API

Pour créer un abonné avec accès aux requêtes par programmation, utilisez le CreateSubscriberfonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande create-subscriber.

Dans votre demande, utilisez ces paramètres pour définir les paramètres suivants pour l'abonné :

- Pour `accessTypes`, spécifiez `LAKEFORMATION`.
- Pour`sources`, spécifiez chaque source que vous souhaitez que Security Lake inclue lors du renvoi des résultats de requête.
- Pour`subscriberIdentity`, spécifiez l' AWS identité et l'ID externe que l'abonné utilise pour interroger les données source.

L'exemple suivant crée un abonné avec un accès aux requêtes dans la AWS région actuelle pour l'identité d'abonné spécifiée. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

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

```
--access-types LAKEFORMATION
```

Configuration du partage de tables entre comptes (étape réservée aux abonnés)

Security Lake utilise le partage de tables entre comptes de Lake Formation pour faciliter l'accès aux requêtes des abonnés. Lorsque vous créez un abonné doté d'un accès aux requêtes dans la console, l'API ou l'API de Security Lake AWS CLI, Security Lake partage des informations sur les tables Lake Formation pertinentes avec l'abonné en créant un partage de ressources dans AWS Resource Access Manager (AWS RAM).

Lorsque vous apportez certains types de modifications à un abonné ayant accès aux requêtes, Security Lake crée un nouveau partage de ressources. Pour plus d'informations, consultez Modification d'un abonné avec accès aux requêtes.

L'abonné doit suivre les étapes suivantes pour utiliser les données de vos tables de Lake Formation :

1. Accepter le partage de ressources — L'abonné doit accepter le partage de ressources qui contient le `resourceShareArn` et `resourceShareName` qui est généré lorsque vous créez ou modifiez l'abonné. Choisissez l'une des méthodes d'accès suivantes :
   - Pour la console et AWS CLI, voir Accepter une invitation de partage de ressources depuis AWS RAM.
   - Pour l'API, invoquez l'GetResourceShareInvitationsAPI. Filtrez par `resourceShareArn` et `resourceShareName` pour trouver le partage de ressources approprié. Acceptez l'invitation avec l'AcceptResourceShareInvitationAPI.

   L'invitation au partage de ressources expire dans 12 heures. Vous devez donc valider et accepter l'invitation dans les 12 heures. Si l'invitation expire, vous continuez à la voir dans son `PENDING` état actuel, mais l'accepter ne vous donnera pas accès aux ressources partagées. Lorsque plus de 12 heures se sont écoulées, supprimez l'abonné de Lake Formation et recréez-le pour recevoir une nouvelle invitation à partager des ressources.
2. Créer un lien de ressource vers des tables partagées — L'abonné doit créer un lien de ressource vers les tables partagées de Lake Formation dans AWS Lake Formation (s'il utilise la console) ou AWS Glue (s'il utilise API/AWS CLI). Ce lien de ressource pointe le compte de l'abonné vers les tables partagées. Choisissez l'une des méthodes d'accès suivantes :

- Pour la console et AWS CLI, voir Création d'un lien de ressource vers une table de catalogue de données partagée dans le manuel du AWS Lake Formation développeur.
- Pour l'API, invoquez l' AWS Glue CreateTableAPI. Nous recommandons aux abonnés de créer également une base de données unique avec l'CreateDatabaseAPI pour stocker les tables de liens vers les ressources.

3. Interrogez les tables partagées : des services tels qu'Amazon Athena peuvent se référer directement aux tables, et les nouvelles données collectées par Security Lake sont automatiquement disponibles pour être consultées. Les requêtes sont exécutées chez l'abonné Compte AWS, et les frais liés aux requêtes sont facturés à l'abonné. Vous pouvez contrôler l'accès en lecture aux ressources dans votre propre compte Security Lake.

Pour plus d'informations sur l'octroi d'autorisations entre comptes, consultez la section Partage de données entre comptes dans Lake Formation dans le guide du AWS Lake Formation développeur.

Modification d'un abonné avec accès aux requêtes

Security Lake permet d'apporter des modifications à un abonné ayant accès aux requêtes. Vous pouvez modifier le nom, la description, l'identifiant externe, le principal (Compte AWS ID) de l'abonné et les sources de journal que l'abonné est en mesure de consommer. Choisissez votre méthode préférée et suivez les étapes pour modifier un abonné ayant actuellement accès aux requêtes Région AWS.

> **Note**
>
> Security Lake ne prend pas en charge le partage de données entre comptes Lake Formation version 1. Vous devez mettre à jour le partage de données entre comptes de Lake Formation vers la version 2 ou la version 3. Pour connaître les étapes de mise à jour des paramètres de version entre comptes via la AWS Lake Formation console ou la AWS CLI, voir Pour activer la nouvelle version dans le guide du AWS Lake Formation développeur.

Console

En fonction des informations que vous souhaitez modifier, suivez les étapes indiquées pour cette action uniquement.

Pour modifier le nom de l'abonné

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous au compte d'administrateur délégué.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier les informations de l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, utilisez le bouton radio pour sélectionner l'abonné que vous souhaitez modifier. La méthode d'accès aux données pour l'abonné sélectionné doit être LAKEFORMATION.
5. Choisissez Modifier.
6. Entrez le nouveau nom d'abonné, puis choisissez Enregistrer.

Pour modifier la description de l'abonné

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous au compte d'administrateur délégué.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, utilisez le bouton radio pour sélectionner l'abonné que vous souhaitez modifier. La méthode d'accès aux données pour l'abonné sélectionné doit être LAKEFORMATION.
5. Choisissez Modifier.
6. Entrez la nouvelle description de l'abonné, puis choisissez Enregistrer.

Pour modifier l'ID externe

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous au compte d'administrateur délégué.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier les informations de l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, utilisez le bouton radio pour sélectionner l'abonné que vous souhaitez modifier. La méthode d'accès aux données pour l'abonné sélectionné doit être LAKEFORMATION.
5. Choisissez Modifier.
6. Entrez le nouvel ID externe fourni par l'abonné, puis choisissez Enregistrer.

   L'enregistrement du nouvel ID externe supprime automatiquement le partage de AWS RAM ressources précédent et crée un nouveau partage de ressources pour l'abonné.
7. L'abonné doit accepter le nouveau partage de ressources en suivant l'étape 1 dansConfiguration du partage de tables entre comptes (étape réservée aux abonnés). Assurez-vous que le nom Amazon Resource (ARN) qui apparaît dans les informations de l'abonné est le même que dans la console Lake Formation. Le lien de ressource vers les tables partagées reste tel quel, de sorte que l'abonné n'a pas à créer un nouveau lien de ressource.

Pour modifier le principal (Compte AWS ID)

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

   Connectez-vous au compte d'administrateur délégué.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier les informations de l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, utilisez le bouton radio pour sélectionner l'abonné que vous souhaitez modifier. La méthode d'accès aux données pour l'abonné sélectionné doit être LAKEFORMATION.
5. Choisissez Modifier.
6. Entrez le nouvel Compte AWS identifiant de l'abonné, puis choisissez Enregistrer.

   L'enregistrement du nouvel identifiant de compte supprime automatiquement le partage de AWS RAM ressources précédent afin que l'ancien principal ne puisse pas utiliser

le journal et les sources d'événements. Security Lake crée un nouveau partage de ressources.

7. À l'aide des informations d'identification du nouveau principal, l'abonné doit accepter le nouveau partage de ressources et créer un lien de ressource vers les tables partagées. Cela donne au nouveau principal accès aux ressources partagées. Pour obtenir des instructions, reportez-vous aux étapes 1 et 2 de[Configuration du partage de tables entre comptes (étape réservée aux abonnés)]. Assurez-vous que l'ARN qui apparaît dans les informations de l'abonné est le même que dans la console Lake Formation.

Pour modifier les sources du journal et des événements

1. Ouvrez la console Security Lake à l'[adresse https://console.aws.amazon.com/securitylake/].

   Connectez-vous au compte d'administrateur délégué.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier les informations de l'abonné.
3. Dans le volet de navigation, choisissez Subscribers.
4. Sur la page Abonnés, utilisez le bouton radio pour sélectionner l'abonné que vous souhaitez modifier. La méthode d'accès aux données pour l'abonné sélectionné doit être LAKEFORMATION.
5. Choisissez Modifier.
6. Désélectionnez les sources existantes ou sélectionnez les sources que vous souhaitez ajouter. Si vous désélectionnez une source, aucune autre action n'est requise de votre part. Si vous choisissez d'ajouter une source, aucune nouvelle invitation de partage de ressources n'est créée. Toutefois, Security Lake met à jour les tables partagées de Lake Formation en fonction des sources ajoutées. L'abonné doit créer un lien de ressource vers les tables partagées mises à jour afin de pouvoir interroger les données sources. Pour obtenir des instructions, reportez-vous à l'étape 2 de[Configuration du partage de tables entre comptes (étape réservée aux abonnés)].
7. Choisissez Enregistrer.

API

Pour modifier un abonné ayant accès aux requêtes par programmation, utilisez le [UpdateSubscriber]fonctionnement de l'API Security Lake. Si vous utilisez le AWS Command Line

Interface (AWS CLI), exécutez la commande update-subscriber. Dans votre demande, utilisez les paramètres pris en charge pour définir les paramètres suivants pour l'abonné :

- Pour `subscriberName`, spécifiez le nouveau nom d'abonné.
- Pour `subscriberDescription`, spécifiez la nouvelle description.
- Pour `subscriberIdentity`, spécifiez l'identifiant principal (Compte AWS ID) et l'identifiant externe que l'abonné utilisera pour interroger les données source. Vous devez fournir à la fois l'identifiant principal et l'identifiant externe. Si vous souhaitez conserver l'une de ces valeurs, transmettez la valeur actuelle.
  - Mettre à jour uniquement l'ID externe : cette action supprime le partage de AWS RAM ressources précédent et crée un nouveau partage de ressources pour l'abonné. L'abonné doit accepter le nouveau partage de ressources en suivant l'étape 1 dansConfiguration du partage de tables entre comptes (étape réservée aux abonnés). Le lien de ressource vers les tables partagées reste tel quel, de sorte que l'abonné n'a pas à créer un nouveau lien de ressource.
  - Mettre à jour le principal uniquement : cette action supprime le partage de AWS RAM ressources précédent afin que le principal précédent ne puisse pas consommer le journal et les sources d'événements. Security Lake crée un nouveau partage de ressources. À l'aide des informations d'identification du nouveau principal, l'abonné doit accepter le nouveau partage de ressources et créer un lien de ressource vers les tables partagées. Cela donne au nouveau principal accès aux ressources partagées. Pour obtenir des instructions, reportez-vous aux étapes 1 et 2 deConfiguration du partage de tables entre comptes (étape réservée aux abonnés).

  Pour mettre à jour l'ID externe et le principal, suivez les étapes 1 et 2 de la sectionConfiguration du partage de tables entre comptes (étape réservée aux abonnés).
- Pour `sources`, supprimez les sources existantes ou spécifiez les sources que vous souhaitez ajouter. Si vous supprimez une source, aucune autre action n'est requise de votre part. Si vous ajoutez une source, aucune nouvelle invitation de partage de ressources n'est créée. Toutefois, Security Lake met à jour les tables partagées de Lake Formation en fonction des sources ajoutées. L'abonné doit créer un lien de ressource vers les tables partagées mises à jour afin de pouvoir interroger les données sources. Pour obtenir des instructions, reportez-vous à l'étape 2 deConfiguration du partage de tables entre comptes (étape réservée aux abonnés).

Requêtes Security Lake

Vous pouvez interroger les données stockées par Security Lake dans des AWS Lake Formation bases de données et des tables. Vous pouvez également créer des abonnés tiers dans la console Security Lake, l'API ou AWS CLI. Les abonnés tiers peuvent également interroger les données de Lake Formation à partir des sources que vous spécifiez.

L'administrateur du lac de données de Lake Formation doit accorder `SELECT` des autorisations sur les bases de données et les tables pertinentes à l'identité IAM qui interroge les données. Un abonné doit également être créé dans Security Lake pour que celui-ci puisse interroger des données. Pour plus d'informations sur la création d'un abonné avec accès aux requêtes, consultezGestion de l'accès aux requêtes pour les abonnés de Security Lake.

Rubriques

- Requêtes Security Lake pour la version AWS source 1 (OCSF 1.0.0-rc.2)
- Requêtes Security Lake pour la version AWS source 2 (OCSF 1.1.0)

Requêtes Security Lake pour la version AWS source 1 (OCSF 1.0.0-rc.2)

La section suivante fournit des conseils sur l'interrogation de données à partir de Security Lake et inclut des exemples de requêtes pour des sources prises en charge en mode natif. AWS Ces requêtes sont conçues pour récupérer des données dans un domaine spécifique Région AWS. Ces exemples utilisent us-east-1 (USA East (Virginie du Nord)). En outre, les exemples de requêtes utilisent un `LIMIT 25` paramètre qui renvoie jusqu'à 25 enregistrements. Vous pouvez omettre ce paramètre ou le modifier en fonction de vos préférences. Pour plus d'exemples, consultez le GitHub répertoire Amazon Security Lake OCSF Queries.

Table des sources du journal

Lorsque vous interrogez les données de Security Lake, vous devez inclure le nom de la table Lake Formation dans laquelle se trouvent les données.

```
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
```

Les valeurs courantes de la table des sources du journal sont les suivantes :

- `cloud_trail_mgmt_1_0`— événements AWS CloudTrail de gestion
- `lambda_execution_1_0`— événements CloudTrail de données pour Lambda
- `s3_data_1_0`— événements CloudTrail de données pour S3
- `route53_1_0`— Journaux de requêtes du résolveur Amazon Route 53
- `sh_findings_1_0`— AWS Security Hub résultats
- `vpc_flow_1_0`— Journaux de flux Amazon Virtual Private Cloud (Amazon VPC)

Exemple : tous les résultats du Security Hub présentés dans le tableau **`sh_findings_1_0`** de la région 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
```

Région de base de données

Lorsque vous interrogez les données de Security Lake, vous devez inclure le nom de la région de base de données à partir de laquelle vous interrogez les données. Pour obtenir la liste complète des régions de base de données dans lesquelles Security Lake est actuellement disponible, consultez Amazon Security Lake endpoints.

Exemple : répertorier AWS CloudTrail l'activité à partir de l'adresse IP source

L'exemple suivant répertorie toutes les CloudTrail activités de l'adresse IP source 192.0.2.1 qui ont été enregistrées après 20230301 (1er mars 2023), dans la table cloud_trail_mgmt_1_0 du 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
```

Date de partition

En partitionnant vos données, vous pouvez limiter la quantité de données numérisées par chaque requête, améliorant ainsi les performances et réduisant les coûts. Security Lake implémente le partitionnement via `eventDay`, `region`, et `accountid` les paramètres. `eventDay` les partitions utilisent le format`YYYYMMDD`.

Voici un exemple de requête utilisant la `eventDay` partition :

```
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
```

Les valeurs communes pour `eventDay` sont les suivantes :

Événements survenus au cours de la dernière année

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

Événements survenus au cours du dernier mois

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

Événements survenus au cours des 30 derniers jours

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

Événements survenus au cours des 12 dernières heures

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

Événements survenus au cours des 5 dernières minutes

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

Événements survenus il y a 7 à 14 jours

```
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)
```

Événements survenant à une date précise ou après cette date

```
>= '20230301'
```

Exemple : liste de toutes les CloudTrail activités depuis l'adresse IP source **192.0.2.1** le 1er mars 2023 ou après cette date dans le tableau **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
```

Exemple : liste de toutes les CloudTrail activités depuis l'adresse IP source **192.0.2.1** au cours des 30 derniers jours dans le tableau **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
```

Exemples de requêtes de CloudTrail données

AWS CloudTrail suit l'activité des utilisateurs et l'utilisation des API dans AWS services. Les abonnés peuvent interroger CloudTrail des données pour connaître les types d'informations suivants :

Voici quelques exemples de requêtes de CloudTrail données :

Tentatives non autorisées AWS services au cours des 7 derniers jours

```
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
```

Liste de toutes les CloudTrail activités depuis l'adresse IP source **192.0.2.1** au cours des 7 derniers jours

```
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
```

Liste de toutes les activités de l'IAM au cours des 7 derniers jours

```
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
```

Instances où l'identifiant a **AIDACKCEVSQ6C2EXAMPLE** été utilisé au cours des 7 derniers jours

```
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
```

Liste des CloudTrail enregistrements ayant échoué au cours des 7 derniers jours

```
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
```

Exemples de requêtes pour les journaux de requêtes du résolveur Route 53

Les journaux de requêtes du résolveur Amazon Route 53 suivent les requêtes DNS effectuées par les ressources de votre Amazon VPC. Les abonnés peuvent consulter les journaux de requêtes du résolveur Route 53 pour connaître les types d'informations suivants :

Voici quelques exemples de requêtes des journaux de requêtes du résolveur Route 53 :

Liste des requêtes DNS CloudTrail des 7 derniers jours

```
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
```

Liste des requêtes DNS correspondant **`s3.amazonaws.com`** au cours des 7 derniers jours

```
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
```

Liste des requêtes DNS qui n'ont pas été résolues au cours des 7 derniers jours

```
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
```

Liste des requêtes DNS résolues **`192.0.2.1`** au cours des 7 derniers jours

```
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
```

Exemples de requêtes pour les résultats du Security Hub

Security Hub vous fournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub produit des résultats pour les contrôles de sécurité et reçoit les résultats de services tiers.

Voici quelques exemples de requêtes basées sur les résultats du Security Hub :

Nouveaux résultats présentant une gravité supérieure ou égale à celle observée **`MEDIUM`** au cours des 7 derniers jours

```
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
```

Résultats dupliqués au cours des 7 derniers jours

```
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
```

Tous les résultats non informatifs des 7 derniers jours

```
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
```

Résultats indiquant que la ressource est un compartiment Amazon S3 (aucune restriction de temps)

```
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
```

Les résultats obtenus avec un système commun de notation des vulnérabilités (CVSS) ont un score supérieur à **1** (aucune restriction de temps)

```
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
```

Résultats correspondant aux vulnérabilités et expositions courantes (CVE) **CVE-0000-0000** (aucune restriction de temps)

```
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
```

Nombre de produits ayant envoyé des résultats depuis Security Hub au cours des 7 derniers jours

```
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
```

Nombre de types de ressources dans les résultats des 7 derniers jours

```
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
```

Packages vulnérables suite à des découvertes au cours des 7 derniers jours

```
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
```

Résultats qui ont changé au cours des 7 derniers jours

```
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
```

Exemples de requêtes pour Amazon VPC Flow Logs

Amazon Virtual Private Cloud (Amazon VPC) fournit des informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC.

Voici quelques exemples de requêtes relatives aux journaux de flux Amazon VPC :

Trafic en particulier Régions AWS au cours des 7 derniers jours

```
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
```

Liste des activités depuis l'adresse IP **192.0.2.1** et le port source **22** au cours des 7 derniers jours

```
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
```

Nombre d'adresses IP de destination distinctes au cours des 7 derniers jours

```
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
```

Trafic provenant de 198.51.100.0/24 au cours des 7 derniers jours

```
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
```

Tout le trafic HTTPS des 7 derniers jours

```
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
```

Classer par nombre de paquets pour les connexions destinées au port **443** au cours des 7 derniers jours

```
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
```

Tout le trafic entre IP **192.0.2.1** et **192.0.2.2** au cours des 7 derniers jours

```
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
```

Tout le trafic entrant au cours des 7 derniers jours

```
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
```

Tout le trafic sortant des 7 derniers jours

```
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
```

Tout le trafic refusé au cours des 7 derniers jours

```
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
```

Requêtes Security Lake pour la version AWS source 2 (OCSF 1.1.0)

Vous pouvez interroger les données stockées par Security Lake dans des AWS Lake Formation bases de données et des tables. Vous pouvez également créer des abonnés tiers dans la console Security Lake, l'API ou AWS CLI. Les abonnés tiers peuvent également interroger les données de Lake Formation à partir des sources que vous spécifiez.

L'administrateur du lac de données de Lake Formation doit accorder `SELECT` des autorisations sur les bases de données et les tables pertinentes à l'identité IAM qui interroge les données. Un abonné doit également être créé dans Security Lake pour que celui-ci puisse interroger des données. Pour plus d'informations sur la création d'un abonné avec accès aux requêtes, consultezGestion de l'accès aux requêtes pour les abonnés de Security Lake.

La section suivante fournit des conseils sur l'interrogation de données à partir de Security Lake et inclut des exemples de requêtes pour des sources prises en charge en mode natif. AWS Ces requêtes sont conçues pour récupérer des données dans un domaine spécifique Région AWS. Ces exemples utilisent us-east-1 (USA East (Virginie du Nord)). En outre, les exemples de requêtes utilisent un `LIMIT 25` paramètre qui renvoie jusqu'à 25 enregistrements. Vous pouvez omettre ce paramètre ou le modifier en fonction de vos préférences. Pour plus d'exemples, consultez le GitHub répertoire Amazon Security Lake OCSF Queries.

Table des sources du journal

Lorsque vous interrogez les données de Security Lake, vous devez inclure le nom de la table Lake Formation dans laquelle se trouvent les données.

```
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
```

Les valeurs courantes de la table des sources du journal sont les suivantes :

- `cloud_trail_mgmt_2_0`— événements AWS CloudTrail de gestion
- `lambda_execution_2_0`— événements CloudTrail de données pour Lambda
- `s3_data_2_0`— événements CloudTrail de données pour S3
- `route53_2_0`— Journaux de requêtes du résolveur Amazon Route 53
- `sh_findings_2_0`— AWS Security Hub résultats
- `vpc_flow_2_0`— Journaux de flux Amazon Virtual Private Cloud (Amazon VPC)
- `eks_audit_2_0`— Journaux d'audit Amazon Elastic Kubernetes Service (Amazon EKS)
- `waf_2_0`— Journaux AWS WAF v2

Exemple : tous les résultats du Security Hub présentés dans le tableau **`sh_findings_2_0`** de la région 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
```

Région de base de données

Lorsque vous interrogez les données de Security Lake, vous devez inclure le nom de la région de base de données à partir de laquelle vous interrogez les données. Pour obtenir la liste complète des régions de base de données dans lesquelles Security Lake est actuellement disponible, consultez Amazon Security Lake endpoints.

Exemple : répertorier l'activité Amazon Virtual Private Cloud à partir de l'adresse IP source

L'exemple suivant répertorie toutes les activités Amazon VPC à partir de l'adresse IP source 192.0.2.1 qui ont été enregistrées après 20230301 (1er mars 2023), dans la table vpc_flow_2_0 du 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
```

Date de partition

En partitionnant vos données, vous pouvez limiter la quantité de données numérisées par chaque requête, améliorant ainsi les performances et réduisant les coûts. Les partitions fonctionnent légèrement différemment dans Security Lake 2.0 par rapport à Security Lake 1.0. Security Lake implémente désormais le partitionnement via `time_dtregion`, et`accountid`. Alors que Security Lake 1.0 a implémenté le partitionnement via `eventDayregion`, et `accountid` les paramètres.

L'interrogation `time_dt` produira automatiquement les partitions de date de S3 et peut être interrogée comme n'importe quel champ basé sur l'heure dans Athena.

Voici un exemple de requête utilisant la `time_dt` partition pour interroger les journaux après le 1er mars 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
```

Les valeurs communes pour `time_dt` sont les suivantes :

Événements survenus au cours de la dernière année

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

Événements survenus au cours du dernier mois

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

Événements survenus au cours des 30 derniers jours

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

Événements survenus au cours des 12 dernières heures

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

Événements survenus au cours des 5 dernières minutes

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

Événements survenus il y a 7 à 14 jours

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

Événements survenant à une date précise ou après

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

Exemple : liste de toutes les CloudTrail activités depuis l'adresse IP source **192.0.2.1** le 1er mars 2023 ou après cette date dans le tableau **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
```

Exemple : liste de toutes les CloudTrail activités depuis l'adresse IP source **192.0.2.1** au cours des 30 derniers jours dans le tableau **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
```

Interrogation des observables de Security Lake

Observables est une nouvelle fonctionnalité désormais disponible dans Security Lake 2.0. L'objet observable est un élément pivot qui contient des informations connexes trouvées à de nombreux endroits de l'événement. L'interrogation des observables permet aux utilisateurs d'obtenir des informations de sécurité de haut niveau à partir de leurs ensembles de données.

En interrogeant des éléments spécifiques dans les observables, vous pouvez limiter les ensembles de données à des éléments tels que des noms d'utilisateur spécifiques, des UID de ressource, des adresses IP, des hachages et d'autres informations de type CIO

Il s'agit d'un exemple de requête utilisant le tableau observables pour interroger les journaux des tables VPC Flow et Route53 contenant la valeur 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
```

Requêtes de CloudTrail données

AWS CloudTrail suit l'activité des utilisateurs et l'utilisation de l'API dans AWS services. Les abonnés peuvent interroger CloudTrail des données pour connaître les types d'informations suivants :

Voici quelques exemples de requêtes de CloudTrail données :

Tentatives non autorisées AWS services au cours des 7 derniers jours

```
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
```

Liste de toutes les CloudTrail activités depuis l'adresse IP source **192.0.2.1** au cours des 7 derniers jours

```
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
```

Liste de toutes les activités de l'IAM au cours des 7 derniers jours

```
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
```

Instances où l'identifiant a **`AIDACKCEVSQ6C2EXAMPLE`** été utilisé au cours des 7 derniers jours

```
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
```

Liste des CloudTrail enregistrements ayant échoué au cours des 7 derniers jours

```
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
```

Requêtes pour les journaux de requêtes du résolveur Route 53

Les journaux de requêtes du résolveur Amazon Route 53 suivent les requêtes DNS effectuées par les ressources de votre Amazon VPC. Les abonnés peuvent consulter les journaux de requêtes du résolveur Route 53 pour connaître les types d'informations suivants :

Voici quelques exemples de requêtes pour les journaux de requêtes du résolveur Route 53 :

Liste des requêtes DNS CloudTrail des 7 derniers jours

```
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
```

Liste des requêtes DNS correspondant **`s3.amazonaws.com`** au cours des 7 derniers jours

```
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
```

Liste des requêtes DNS qui n'ont pas été résolues au cours des 7 derniers jours

```
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
```

Liste des requêtes DNS résolues **`192.0.2.1`** au cours des 7 derniers jours

```
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
```

Requêtes concernant les résultats du Security Hub

Security Hub vous fournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub produit des résultats pour les contrôles de sécurité et reçoit les résultats de services tiers.

Voici quelques exemples de requêtes concernant les résultats du Security Hub :

Nouveaux résultats présentant une gravité supérieure ou égale à celle observée **MEDIUM** au cours des 7 derniers jours

```
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
```

Résultats dupliqués au cours des 7 derniers jours

```
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
```

Tous les résultats non informatifs des 7 derniers jours

```
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
```

Résultats indiquant que la ressource est un compartiment Amazon S3 (aucune restriction de temps)

```
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
```

Les résultats obtenus avec un système commun de notation des vulnérabilités (CVSS) ont un score supérieur à **1** (aucune restriction de temps)

```
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
```

Résultats correspondant aux vulnérabilités et expositions courantes (CVE) **`CVE-0000-0000`** (aucune restriction de temps)

```
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
```

Nombre de produits ayant envoyé des résultats depuis Security Hub au cours des 7 derniers jours

```
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
```

Nombre de types de ressources dans les résultats des 7 derniers jours

```
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
```

Packages vulnérables suite à des découvertes au cours des 7 derniers jours

```
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
```

Résultats qui ont changé au cours des 7 derniers jours

```
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
```

Requêtes pour les journaux de flux Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) fournit des informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC.

Voici quelques exemples de requêtes pour Amazon VPC Flow Logs :

Trafic en particulier Régions AWS au cours des 7 derniers jours

```
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
```

Liste des activités depuis l'adresse IP **192.0.2.1** et le port source **22** au cours des 7 derniers jours

```
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
```

Nombre d'adresses IP de destination distinctes au cours des 7 derniers jours

```
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
```

Trafic provenant de 198.51.100.0/24 au cours des 7 derniers jours

```
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
```

Tout le trafic HTTPS des 7 derniers jours

```
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
```

Classer par nombre de paquets pour les connexions destinées au port **443** au cours des 7 derniers jours

```
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
```

Tout le trafic entre IP **192.0.2.1** et **192.0.2.2** au cours des 7 derniers jours

```
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
```

Tout le trafic entrant au cours des 7 derniers jours

```
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
```

Tout le trafic sortant des 7 derniers jours

```
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
```

Tout le trafic refusé au cours des 7 derniers jours

```
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
```

Requêtes pour les journaux d'audit Amazon EKS

Les journaux Amazon EKS suivent l'activité du plan de contrôle et fournissent des journaux d'audit et de diagnostic directement depuis le plan de contrôle Amazon EKS vers CloudWatch les journaux de votre compte. Ces journaux vous permettent de sécuriser et d'exécuter facilement vos clusters. Les abonnés peuvent consulter les journaux EKS pour connaître les types d'informations suivants.

Voici quelques exemples de requêtes pour les journaux d'audit Amazon EKS :

Demandes adressées à une URL spécifique au cours des 7 derniers jours

```
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
```

Demandes de mise à jour de '10.0.97.167' au cours des 7 derniers jours

```
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
```

Demandes et réponses associées à la ressource « kube-controller-manager » au cours des 7 derniers jours

```
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
```

Requêtes pour les journaux de la AWS WAF version 2

AWS WAF est un pare-feu d'applications Web que vous pouvez utiliser pour surveiller les requêtes Web que vos utilisateurs finaux envoient à vos applications et pour contrôler l'accès à votre contenu.

Voici quelques exemples de requêtes pour les journaux de la AWS WAF version 2 :

Publier des requêtes depuis une adresse IP source spécifique au cours des 7 derniers jours

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

```
AND activity_name = 'Post'
LIMIT 25
```

Demandes correspondant à un type de pare-feu MANAGED_RULE_GROUP au cours des 7 derniers jours

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

Demandes correspondant à un REGEX dans une règle de pare-feu au cours des 7 derniers jours

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

```
AND firewall_rule.condition = 'REGEX'
LIMIT 25
```

Demandes d'accès aux AWS informations d'identification refusées qui ont déclenché la AWS WAF règle au cours des 7 derniers jours

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

Recevez des demandes AWS d'informations d'identification, regroupées par pays au cours des 7 derniers jours

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

```
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
```

Gestion du cycle de vie dans Security Lake

Vous pouvez personnaliser Security Lake pour stocker les données dans votre choix Régions AWS pendant la durée que vous préférez. La gestion du cycle de vie peut vous aider à vous conformer aux différentes exigences de conformité.

Gestion de la rétention

Pour gérer vos données de manière à ce qu'elles soient stockées de manière rentable, vous pouvez configurer les paramètres de conservation des données. Dans la mesure où Security Lake stocke vos données sous forme d'objets dans des compartiments Amazon Simple Storage Service (Amazon S3), les paramètres de conservation correspondent à une configuration du cycle de vie d'Amazon S3. En configurant ces paramètres, vous pouvez spécifier votre classe de stockage Amazon S3 préférée et la durée pendant laquelle les objets S3 doivent rester dans cette classe de stockage avant de passer à une autre classe de stockage ou d'expirer. Pour plus d'informations sur les configurations du cycle de vie d'Amazon S3, consultez Gérer votre cycle de vie de stockage dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Dans Security Lake, vous définissez les paramètres de rétention au niveau de la région. Par exemple, vous pouvez choisir de transférer tous les objets S3 d'une classe de stockage spécifique Région AWS vers la classe de stockage S3 Standard-IA 30 jours après leur écriture dans le lac de données. La classe de stockage Amazon S3 par défaut est S3 Standard.

> **Important**
>
> Security Lake ne prend pas en charge Amazon S3 Object Lock. Lorsque les compartiments du lac de données sont créés, S3 Object Lock est désactivé par défaut. L'activation de S3 Object Lock avec le mode de rétention par défaut interrompt la transmission des données de journal normalisées au lac de données.

Configuration des paramètres de rétention lors de l'activation de Security Lake

Suivez ces instructions pour configurer les paramètres de rétention pour une ou plusieurs régions lors de votre intégration à Security Lake. Si vous ne configurez pas les paramètres de rétention, Security

Lake utilise les paramètres par défaut pour une configuration Amazon S3 Lifecycle : stockez les données indéfiniment à l'aide de la classe de stockage S3 Standard.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Lorsque vous atteignez l'étape 2 : définir l'objectif cible du flux de travail d'intégration, choisissez Ajouter une transition sous Sélectionner les classes de stockage. Choisissez ensuite la classe de stockage Amazon S3 vers laquelle vous souhaitez transférer les objets S3. (La classe de stockage par défaut non répertoriée est S3 Standard.) Spécifiez également une période de conservation (en jours) pour cette classe de stockage. Pour transférer des objets vers une autre classe de stockage après cette période, choisissez Ajouter une transition et entrez les paramètres pour la classe de stockage et la période de conservation suivantes.
3. Pour spécifier à quel moment vous souhaitez que les objets S3 expirent, choisissez Ajouter une transition. Ensuite, pour la classe de stockage, choisissez Expire. Pour la période de rétention, entrez le nombre total de jours pendant lesquels vous souhaitez stocker des objets dans Amazon S3, quelle que soit la classe de stockage, une fois les objets créés. À la fin de cette période, les objets expirent et Amazon S3 les supprime.
4. Lorsque vous avez terminé, choisissez Suivant.

Vos modifications s'appliqueront à toutes les régions dans lesquelles vous avez activé Security Lake lors des étapes d'intégration précédentes.

API

Pour configurer les paramètres de rétention par programmation lors de votre intégration à Security Lake, utilisez le CreateDataLakefonctionnement de l'API Security Lake. Si vous utilisez le AWS CLI, exécutez la create-data-lakecommande. Spécifiez les paramètres de rétention que vous souhaitez dans les `lifecycleConfiguration` paramètres comme suit :

- Pour`transitions`, spécifiez le nombre total de jours (`days`) pendant lesquels vous souhaitez stocker des objets S3 dans une classe de stockage Amazon S3 spécifique (`storageClass`).
- Pour`expiration`, spécifiez le nombre total de jours pendant lesquels vous souhaitez stocker des objets dans Amazon S3, en utilisant n'importe quelle classe de stockage, après la création des objets. À la fin de cette période, les objets expirent et Amazon S3 les supprime.

Security Lake applique les paramètres à la région que vous spécifiez dans le `region` champ de l'`configurations`objet.

Par exemple, la commande suivante active Security Lake dans la `us-east-1` région. Dans cette région, les objets expirent au bout de 365 jours et les objets passent à la classe de stockage `ONEZONE_IA` S3 au bout de 60 jours. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ 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"
```

Mise à jour des paramètres de rétention

Suivez ces instructions pour mettre à jour les paramètres de rétention pour une ou plusieurs régions après avoir activé Security Lake.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, choisissez Regions
3. Sélectionnez une région, puis choisissez Modifier.
4. Dans la section Sélectionner les classes de stockage, entrez les paramètres souhaités. Pour la classe de stockage, choisissez la classe de stockage Amazon S3 vers laquelle vous souhaitez transférer les objets S3. (La classe de stockage par défaut non répertoriée est S3 Standard.) Pour la période de conservation, entrez le nombre de jours pendant lesquels vous souhaitez stocker les objets dans cette classe de stockage. Vous pouvez spécifier plusieurs transitions.

   Pour spécifier également à quel moment vous souhaitez que les objets S3 expirent, choisissez Expire pour la classe de stockage. Ensuite, pour la période de rétention, entrez le nombre total de jours pendant lesquels vous souhaitez stocker des objets dans Amazon S3, quelle que soit la classe de stockage, une fois les objets créés. À la fin de cette période, les objets expirent et Amazon S3 les supprime.

5. Lorsque vous avez terminé, choisissez Enregistrer.

API

Pour mettre à jour les paramètres de rétention par programmation, UpdateDataLakeutilisez l'API Security Lake. Si vous utilisez la AWS CLI, exécutez la commande. update-data-lake Dans votre demande, utilisez le `lifecycleConfiguration` paramètre pour définir les nouveaux paramètres :

- Pour modifier les paramètres de transition, `transitions` utilisez-les pour spécifier chaque nouvelle période en jours (`days`) pendant laquelle vous souhaitez stocker des objets S3 dans une classe de stockage Amazon S3 spécifique (`storageClass`).
- Pour modifier la période de rétention globale, utilisez le `expiration` paramètre pour spécifier le nombre total de jours pendant lesquels vous souhaitez stocker les objets S3, quelle que soit leur classe de stockage, après leur création. À la fin de cette période de rétention, les objets expirent et Amazon S3 les supprime.

Security Lake applique les paramètres à la région que vous spécifiez dans le `region` champ de l'`configurations`objet.

Par exemple, la AWS CLI commande suivante met à jour les paramètres d'expiration des données et les paramètres de transition de stockage pour la `us-east-1` région. Dans cette région, les objets expirent au bout de 500 jours et les objets passent à la classe de stockage `ONEZONE_IA` S3 au bout de 30 jours. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ 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"
```

Régions cumulatives

Une région cumulative consolide les données d'une ou de plusieurs régions contributrices. Cela peut vous aider à respecter les exigences régionales en matière de conformité des données.

Pour obtenir des instructions sur la configuration des régions cumulatives, consultez. Configuration de régions cumulatives

Cadre de schéma de cybersécurité ouvert (OCSF)

Qu'est-ce que l'OCSF ?

L'Open Cybersecurity Schema Framework (OCSF) est un effort collaboratif AWS et open source mené par des partenaires de premier plan dans le secteur de la cybersécurité. L'OCSF fournit un schéma standard pour les événements de sécurité courants, définit des critères de version pour faciliter l'évolution du schéma et inclut un processus d'autogouvernance pour les producteurs et les consommateurs de journaux de sécurité. Le code source public de l'OCSF est hébergé sur GitHub.

Security Lake convertit automatiquement les journaux et les événements provenant du schéma OCSF pris en charge AWS services de manière native. Après la conversion au format OCSF, Security Lake stocke les données dans un compartiment Amazon Simple Storage Service (Amazon S3) (un compartiment Région AWS par compartiment) dans votre. Compte AWS Les journaux et les événements écrits dans Security Lake à partir de sources personnalisées doivent respecter le schéma OCSF et le format Apache Parquet. Les abonnés peuvent traiter les journaux et les événements comme des enregistrements Parquet génériques ou appliquer la classe d'événements du schéma OCSF pour interpréter plus précisément les informations contenues dans un enregistrement.

Cours d'événements OCSF

Les journaux et les événements provenant d'une source Security Lake donnée correspondent à une classe d'événements spécifique définie dans OCSF. L'activité DNS, l'activité SSH et l'authentification sont des exemples de classes d'événements dans OCSF. Vous pouvez spécifier à quelle classe d'événements correspond une source donnée.

Identification de la source OCSF

L'OCSF utilise différents champs pour vous aider à déterminer l'origine d'un ensemble spécifique de journaux ou d'événements. Il s'agit des valeurs des champs pertinents AWS services qui sont prises en charge nativement en tant que sources dans Security Lake.

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

Source	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	nom_classe	métadonnées.version
CloudTrail Événements relatifs aux données Lambda	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail Événements de gestion	CloudTrail	AWS	Management	API Activity, Authentication ou Account Change	1.0.0-rc.2
CloudTrail Événements liés aux données 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	Correspond à la ProductName valeur du Security Hub	Security Finding	1.0.0-rc.2
Journaux de flux 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.

Source	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	nom_classe	métadonnées.version
CloudTrail Événements relatifs aux données Lambda	CloudTrail	AWS	Data	API Activity	1.1.0
CloudTrail Événements de gestion	CloudTrail	AWS	Management	API Activity, Authentication ou Account Change	1.1.0
CloudTrail Événements liés aux données S3	CloudTrail	AWS	Data	API Activity	1.1.0
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
Security Hub	Correspond à AWS la valeur du format de recherche de sécurité (ASFF) ProductName	Correspond à AWS la valeur du format de recherche de sécurité (ASFF) CompanyName	Correspond à featureName la valeur d'ASFF ProductFields	Vulnerability Finding, Compliance Finding, or Detection Finding	1.1.0
Journaux de flux VPC	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0

Source	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	nom_classe	métadonnées.version
Journaux d'audit EKS	`Amazon EKS`	`AWS`	`Elastic Kubernetes Service`	`API Activity`	`1.1.0`
AWS WAF Journaux v2	`AWS WAF`	`AWS`	—	`HTTP Activity`	`1.1.0`

Intégrations avec Security Lake

Amazon Security Lake s'intègre à AWS services d'autres produits tiers. Les intégrations peuvent envoyer des données à Security Lake en tant que source ou consommer des données dans Security Lake en tant qu'abonné. Les rubriques suivantes expliquent quels produits AWS services et quels produits tiers s'intègrent à Security Lake.

Rubriques

AWS service intégrations avec Security Lake

Amazon Security Lake s'intègre à d'autres AWS services. Un service peut fonctionner soit comme une intégration de source, soit comme une intégration d'abonnés, soit les deux.

Les intégrations de source présentent les propriétés suivantes :

- Envoyer des données vers Security Lake
- Les données arrivent dans le Cadre de schéma de cybersécurité ouvert (OCSF) schéma
- Les données arrivent au format Apache Parquet

Les intégrations d'abonnés présentent les propriétés suivantes : elles peuvent lire les données source depuis Security Lake sur un HTTPS point de terminaison ou dans la file d'attente Amazon Simple Queue Service (AmazonSQS), ou en interrogeant directement les données sources auprès de AWS Lake Formation

La section suivante explique à quel AWS services Security Lake s'intègre et comment fonctionne chaque intégration.

Intégration avec AWS AppFabric

Type d'intégration : Source

AWS AppFabricest un service sans code qui connecte les applications SaaS (software as a service) au sein de votre organisation, afin que les équipes informatiques et de sécurité puissent gérer et sécuriser les applications à l'aide d'un schéma standard et d'un référentiel central.

Comment Security Lake reçoit AppFabric les résultats

Vous pouvez envoyer les données du journal AppFabric d'audit à Security Lake en sélectionnant Amazon Kinesis Data Firehose comme destination et en configurant Kinesis Data Firehose pour OCSF fournir les données au format schéma et au format Apache Parquet à Security Lake.

Prérequis

Avant de pouvoir envoyer des journaux AppFabric d'audit à Security Lake, vous devez générer vos journaux d'audit OCSF normalisés vers un flux Kinesis Data Firehose. Vous pouvez ensuite configurer Kinesis Data Firehose pour envoyer la sortie vers votre compartiment Amazon S3 Security Lake. Pour plus d'informations, consultez Choisir Amazon S3 pour votre destination dans le manuel Amazon Kinesis Developer Guide.

Envoyez vos AppFabric résultats à Security Lake

Pour envoyer des journaux AppFabric d'audit à Security Lake après avoir rempli les conditions préalables précédentes, vous devez activer les deux services et les ajouter en AppFabric tant que source personnalisée dans Security Lake. Pour obtenir des instructions sur l'ajout d'une source personnalisée, consultezCollecte de données à partir de sources personnalisées.

Arrêter de recevoir AppFabric des journaux dans Security Lake

Pour arrêter de recevoir des journaux AppFabric d'audit, vous pouvez utiliser la console Security Lake, Security LakeAPI, ou AWS CLI les supprimer AppFabric en tant que source personnalisée. Pour obtenir des instructions, consultez Supprimer une source personnalisée.

Intégration à Amazon Detective

Type d'intégration : Abonné

Amazon Detective vous permet d'analyser, d'enquêter et d'identifier rapidement la cause racine des résultats de sécurité ou des activités suspectes. Detective collecte automatiquement les données du journal à partir de vos AWS ressources. Detective utilise ensuite le machine learning, l'analyse statistique et la théorie des graphes pour générer des visualisations qui vous aideront à mener des investigations de sécurité plus rapides et plus efficaces. Les agrégations de données, les résumés et le contexte prédéfinis de Detective vous aident à analyser et à déterminer rapidement la nature et l'étendue des éventuels problèmes de sécurité.

Lorsque vous intégrez Security Lake et Detective, vous pouvez interroger les données brutes du journal stockées par Security Lake auprès de Detective. Pour plus d'informations, consultez la section Intégration à Amazon Security Lake.

Intégration à Amazon OpenSearch Service

Type d'intégration : Abonné

Amazon OpenSearch Service est un service géré qui facilite le déploiement, l'exploitation et le dimensionnement des clusters OpenSearch de services dans le AWS Cloud. En utilisant OpenSearch Service Ingestion pour ingérer des données dans votre cluster OpenSearch Service Service, vous pouvez obtenir des informations plus rapidement pour les enquêtes de sécurité urgentes. Vous pouvez réagir rapidement aux incidents de sécurité, ce qui vous aide à protéger les données et les systèmes critiques de votre entreprise.

OpenSearch Tableau de bord des services

Après avoir intégré OpenSearch Service à Security Lake, vous pouvez configurer Security Lake pour envoyer des données de sécurité provenant de différentes sources à OpenSearch Service Service par le biais d'une ingestion de OpenSearch service sans serveur. Pour plus d'informations sur la façon de configurer l'ingestion de OpenSearch services pour traiter les données de sécurité, consultez Générer des informations de sécurité à partir des données Amazon Security Lake à l'aide d'Amazon OpenSearch Service Ingestion.

Une fois que OpenSearch Service Ingestion commence à écrire vos données dans votre domaine OpenSearch Service Service. Pour visualiser les données à l'aide des tableaux de bord prédéfinis, accédez aux tableaux de bord et choisissez l'un des tableaux de bord installés.

Intégration avec Amazon QuickSight

Type d'intégration : Abonné

Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud que vous pouvez utiliser pour fournir easy-to-understand des informations aux personnes avec lesquelles vous travaillez, où qu'elles se trouvent. Amazon QuickSight se connecte à vos données dans le cloud et combine des données provenant de nombreuses sources différentes. Amazon QuickSight donne aux décideurs la possibilité d'explorer et d'interpréter les informations dans un environnement visuel interactif. Ils ont un accès sécurisé aux tableaux de bord depuis n'importe quel appareil de votre réseau et depuis des appareils mobiles.

Tableau de QuickSight bord Amazon

Pour visualiser vos données Amazon Security Lake dans Amazon QuickSight, créer les AWS objets requis et déployer des sources de données de base, des ensembles de données, des analyses, des tableaux de bord et des groupes d'utilisateurs sur Amazon en ce qui QuickSight concerne Security Lake. Pour obtenir des instructions détaillées, consultez la section Intégration à Amazon QuickSight.

Intégration avec Amazon SageMaker

Type d'intégration : Abonné

Amazon SageMaker est un service d'apprentissage automatique (ML) entièrement géré. Avec Security Lake, les data scientists et les développeurs peuvent créer, former et déployer rapidement et en toute confiance des modèles de machine learning dans un environnement hébergé prêt pour la production. Il fournit une interface utilisateur pour exécuter des flux de travail ML qui rend les outils de SageMaker ML disponibles dans plusieurs environnements de développement intégrés (IDEs).

SageMaker aperçus

Vous pouvez générer des informations d'apprentissage automatique pour Security Lake à l'aide de SageMaker Studio. SageMaker Studio est un environnement de développement intégré au Web (IDE) pour l'apprentissage automatique qui fournit des outils aux scientifiques des données pour préparer, créer, former et déployer des modèles d'apprentissage automatique. Avec cette solution, vous pouvez déployer rapidement un ensemble de blocs-notes Python centrés sur les AWS Security Hub résultats de Security Lake, qui peuvent également être étendus pour intégrer d'autres AWS sources ou des sources de données personnalisées dans Security Lake. Pour plus de détails, consultez Générer des informations d'apprentissage automatique pour les données Amazon Security Lake à l'aide d'Amazon SageMaker.

Intégration avec Amazon Bedrock

Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via un système unifié. API Grâce à l'expérience sans serveur d'Amazon Bedrock, vous pouvez démarrer rapidement, personnaliser en privé les modèles de base avec vos propres données, les intégrer et les déployer facilement et en toute sécurité dans vos applications à l'aide d' AWS outils sans avoir à gérer d'infrastructure.

IA générative

Vous pouvez utiliser les fonctionnalités d'intelligence artificielle générative d'Amazon Bedrock et la saisie en langage naturel dans SageMaker Studio pour analyser les données dans Security Lake, réduire les risques de votre entreprise et améliorer votre niveau de sécurité. Vous pouvez réduire le temps nécessaire pour mener une enquête en identifiant automatiquement les sources de données appropriées, en générant et en invoquant des SQL requêtes, et en visualisant les données issues de votre enquête. Pour plus de détails, consultez Générer des informations basées sur l'IA pour Amazon Security Lake à l'aide d'Amazon SageMaker Studio et d'Amazon Bedrock.

Intégration avec AWS Security Hub

Type d'intégration : Source

AWS Security Hubvous fournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub collecte des données de sécurité provenant de l'ensemble Comptes AWS des services et des produits partenaires tiers pris en charge et vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires.

Lorsque vous activez Security Hub et que vous ajoutez les résultats de Security Hub en tant que source dans Security Lake, Security Hub commence à envoyer de nouveaux résultats et des mises à jour des résultats existants à Security Lake.

Comment Security Lake reçoit les conclusions du Security Hub

Dans Security Hub, les problèmes de sécurité sont suivis en tant que findings. (résultats) Certains résultats proviennent de problèmes détectés par d'autres AWS services ou par des partenaires tiers. Security Hub génère également ses propres conclusions en effectuant des contrôles de sécurité automatisés et continus par rapport aux règles. Les règles sont représentées par des contrôles de sécurité.

Tous les résultats de Security Hub utilisent un JSON format standard appelé AWS Security Finding Format (ASFF).

Security Lake reçoit les résultats du Security Hub et les transforme enCadre de schéma de cybersécurité ouvert (OCSF).

Envoyez les résultats de votre Security Hub à Security Lake

Pour envoyer les résultats du Security Hub à Security Lake, vous devez activer les deux services et ajouter les résultats du Security Hub en tant que source dans Security Lake. Pour obtenir des instructions sur l'ajout d'une AWS source, consultezAjouter un AWS service en tant que source.

Si vous souhaitez que Security Hub génère des résultats de contrôle et les envoie à Security Lake, vous devez activer les normes de sécurité pertinentes et activer l'enregistrement des ressources sur une base régionale dans AWS Config. Pour plus d'informations, consultez la section Activation et configuration AWS Config dans le guide de AWS Security Hub l'utilisateur.

Arrêtez de recevoir les résultats du Security Hub dans Security Lake

Pour ne plus recevoir les résultats du Security Hub, vous pouvez utiliser la console Security Hub, Security Hub API ou AWS CLI.

Consultez la section Désactivation et activation du flux de résultats d'une intégration (console) ou Désactivation du flux de résultats d'une intégration (Security Hub API AWSCLI) dans le guide de l'AWS Security Hub utilisateur.

Intégrations tierces avec Security Lake

Amazon Security Lake s'intègre à plusieurs fournisseurs tiers. Un fournisseur peut proposer une intégration de source, une intégration d'abonnés ou une intégration de service. Les fournisseurs peuvent proposer un ou plusieurs types d'intégration.

Les intégrations de source présentent les propriétés suivantes :

- Envoyer des données vers Security Lake
- Les données arrivent au format Apache Parquet
- Les données arrivent dans le Cadre de schéma de cybersécurité ouvert (OCSF) schéma

Les intégrations d'abonnés présentent les propriétés suivantes :

- Lisez les données source depuis Security Lake sur un HTTPS terminal ou dans la file d'attente Amazon Simple Queue Service (AmazonSQS), ou en interrogeant directement les données sources auprès de AWS Lake Formation
- Capable de lire des données au format Apache Parquet

- Capable de lire les données dans le OCSF schéma

Les intégrations de services peuvent vous aider à implémenter Security Lake et d'autres solutions AWS services au sein de votre organisation. Ils peuvent également fournir une assistance en matière de rapports, d'analyses et d'autres cas d'utilisation.

Pour rechercher un fournisseur partenaire spécifique, consultez le Partner Solutions Finder. Pour acheter un produit tiers, consultez le AWSMarketplace.

Pour demander à être ajouté en tant que partenaire d'intégration ou pour devenir partenaire de Security Lake, envoyez un e-mail à <securitylake-partners@amazon.com>.

Si vous utilisez des intégrations tierces qui envoient des résultats à AWS Security Hub, vous pouvez également consulter ces résultats dans Security Lake si l'intégration Security Hub pour Security Lake est activée. Pour obtenir des instructions sur l'activation de l'intégration, consultezIntégration avec AWS Security Hub. Pour obtenir la liste des intégrations tierces qui envoient des résultats à Security Hub, consultez la section Intégrations de produits partenaires tiers disponibles dans le guide de l'AWS Security Hub utilisateur.

Avant de configurer vos abonnés, vérifiez que le OCSF journal de vos abonnés est pris en charge. Pour obtenir les informations les plus récentes, consultez la documentation de votre abonné.

Intégration des requêtes

Vous pouvez interroger les données stockées par Security Lake dans des AWS Lake Formation bases de données et des tables. Vous pouvez également créer des abonnés tiers dans la console Security LakeAPI, ou AWS Command Line Interface.

L'administrateur du lac de données de Lake Formation doit accorder SELECT des autorisations sur les bases de données et les tables pertinentes à l'IAMidentité qui interroge les données. Vous devez créer un abonné dans Security Lake avant de demander des données. Pour plus d'informations sur la création d'un abonné avec accès aux requêtes, consultezGestion de l'accès aux requêtes pour les abonnés de Security Lake.

Vous pouvez configurer l'intégration des requêtes avec Security Lake pour les partenaires tiers suivants.

- Cribl – Search
- Palo Alto Networks – XSOAR

- IBM – QRadar
- Query.AI – Query Federated Search
- SOC Prime
- Tego Cyber

Accenture – MxDR

Type d'intégration : Abonné, Service

Accenture'sL'intégration de MxDR à Security Lake permet d'ingérer les données en temps réel des journaux et des événements, de gérer la détection des anomalies, de rechercher les menaces et d'effectuer des opérations de sécurité. Cela facilite l'analyse et la gestion de la détection et de la réponse (MDR).

En tant qu'intégration de services, Accenture elle peut également vous aider à implémenter Security Lake dans votre organisation.

Documentation d'intégration

Aqua Security

Type d'intégration : Source

Aqua Securitypeut être ajoutée en tant que source personnalisée pour envoyer des événements d'audit à Security Lake. Les événements d'audit sont convertis au OCSF schéma et au format Parquet.

Documentation d'intégration

Barracuda – Email Protection

Type d'intégration : Source

Barracuda Email Protectionpeut envoyer des événements à Security Lake lorsque de nouvelles attaques par e-mail de phishing sont détectées. Vous pouvez recevoir ces événements ainsi que d'autres données de sécurité dans votre lac de données.

Documentation d'intégration

Booz Allen Hamilton

Type d'intégration : Service

En tant qu'intégration de services, Booz Allen Hamilton utilise une approche de cybersécurité axée sur les données en fusionnant les données et les analyses avec le service Security Lake.

Lien vers le partenaire

Bosch Software and Digital Solutions – AIShield

Type d'intégration : Source

AIShieldpowered by Bosch fournit une analyse automatique des vulnérabilités et une protection des terminaux pour les actifs d'IA grâce à son intégration à Security Lake.

Documentation d'intégration

ChaosSearch

Type d'intégration : Abonné

ChaosSearchoffre un accès aux données multi-modèles aux utilisateurs avec des solutions ouvertes APIs telles qu'Elasticsearch et/ou avec Kibana et SQL Superset inclus en mode natif. UIs Vous pouvez utiliser vos données Security Lake ChaosSearch sans limite de conservation pour surveiller, alerter et traquer les menaces. Cela vous permet de faire face aux environnements de sécurité complexes et aux menaces persistantes d'aujourd'hui.

Documentation d'intégration

Cisco Security – Secure Firewall

Type d'intégration : Source

En Cisco Secure Firewall intégrant Security Lake, vous pouvez stocker les journaux de pare-feu de manière structurée et évolutive. Le eNcore client de Cisco diffuse les journaux de pare-feu depuis le Firewall Management Center, effectue la conversion OCSF du schéma en schéma et les stocke dans Security Lake.

Documentation d'intégration

Claroty – xDome

Type d'intégration : Source

Claroty xDomeenvoie les alertes détectées au sein des réseaux à Security Lake avec une configuration minimale. Les options de déploiement flexibles et rapides aident à xDome protéger les actifs étendus de l'Internet des objets (XIoT), notamment l'IoT et les BMS actifsIIoT, au sein de votre réseau, tout en détectant automatiquement les premiers indicateurs de menaces.

Documentation d'intégration

CMD Solutions

Type d'intégration : Service

CMD Solutionsaide les entreprises à accroître leur agilité en intégrant la sécurité de manière précoce et continue par le biais de processus de conception, d'automatisation et d'assurance continue. En tant qu'intégration de services, CMD Solutions elle peut vous aider à implémenter Security Lake dans votre organisation.

Lien vers le partenaire

Confluent – Amazon S3 Sink Connector

Type d'intégration : Source

Confluentconnecte, configure et orchestre automatiquement les intégrations de données grâce à des connecteurs prédéfinis entièrement gérés. Il vous Confluent S3 Sink Connector permet de prendre des données brutes et de les intégrer dans Security Lake à grande échelle au format de parquet natif.

Documentation d'intégration

Contrast Security

Type d'intégration : Source

Produit partenaire pour l'intégration : Contrast Assess

Contrast Security Assessest un IAST outil permettant de détecter les vulnérabilités en temps réel dans les applications Web et APIs les microservices. Assess s'intègre à Security Lake pour fournir une visibilité centralisée sur toutes vos charges de travail.

Documentation d'intégration

Cribl – Search

Type d'intégration : Abonné

Vous pouvez l'utiliser Cribl Search pour rechercher les données de Security Lake.

Documentation d'intégration

Cribl – Stream

Type d'intégration : Source

Vous pouvez l'utiliser Cribl Stream pour envoyer des données depuis n'importe quelle source tierce Cribl prise en charge vers Security Lake dans OCSF le schéma.

Documentation d'intégration

CrowdStrike – Falcon Data Replicator

Type d'intégration : Source

Cette intégration extrait les données CrowdStrike Falcon Data Replicator en continu, les transforme en OCSF schéma et les envoie à Security Lake.

Documentation d'intégration

CyberArk – Unified Identify Security Platform

Type d'intégration : Source

CyberArk Audit Adapter, une AWS Lambda fonction, collecte les événements de sécurité CyberArk Identity Security Platform et envoie les données à Security Lake sous forme de OCSF schéma.

Documentation d'intégration

Cyber Security Cloud – Cloud Fastener

Type d'intégration : Abonné

CloudFastenerutilise Security Lake pour faciliter la consolidation des données de sécurité issues de vos environnements cloud.

Documentation d'intégration

DataBahn

Type d'intégration : Source

Centralisez vos données de sécurité dans Security Lake à l'aide DataBahn's de Security Data Fabric.

Documentation d'intégration (connectez-vous au DataBahn portail pour consulter la documentation)

Darktrace – Cyber AI Loop

Type d'intégration : Source

L'Darktraceintégration avec Security Lake apporte le pouvoir de l'Darktraceauto-apprentissage à Security Lake. Les informations recueillies Cyber AI Loop peuvent être corrélées à d'autres flux de données et à des éléments du système de sécurité de votre entreprise. L'intégration enregistre les violations de Darktrace modèle en tant que résultats de sécurité.

Documentation d'intégration (connectez-vous au Darktrace portail pour consulter la documentation)

Datadog

Type d'intégration : Abonné

Datadog Cloud SIEMdétecte les menaces en temps réel qui pèsent sur votre environnement cloud, y compris les données de Security Lake, et unifie les DevOps équipes de sécurité sur une seule plateforme.

Documentation d'intégration

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

Type d'intégration : Abonné, Service

Deloitte MXDR CAEvous permet de stocker, d'analyser et de visualiser rapidement vos données de sécurité standardisées. La CAE suite de fonctionnalités d'analyse, d'intelligence artificielle et de machine learning personnalisées fournit automatiquement des informations exploitables basées sur des modèles qui s'exécutent avec les données OCSF formatées de Security Lake.

En tant qu'intégration de services, Deloitte elle peut également vous aider à implémenter Security Lake dans votre organisation.

Documentation d'intégration

Devo

Type d'intégration : Abonné

Le Devo collecteur pour l'ingestion de AWS supports provenant de Security Lake. Cette intégration peut vous aider à analyser et à traiter divers cas d'utilisation de la sécurité, tels que la détection des menaces, les enquêtes et la réponse aux incidents.

Documentation d'intégration

DXC – SecMon

Type d'intégration : Abonné, Service

DXC SecMoncollecte les événements de sécurité provenant de Security Lake et les surveille afin de détecter les menaces de sécurité potentielles et d'en avertir. Cela permet aux entreprises de mieux comprendre leur posture de sécurité et d'identifier les menaces et d'y répondre de manière proactive.

En tant qu'intégration de services, DXC elle peut également vous aider à implémenter Security Lake dans votre organisation.

Documentation d'intégration

Eviden— AIsaac (anciennementAtos)

Type d'intégration : Abonné

La AIsaac MDR plateforme utilise les journaux de VPC flux ingérés dans le OCSF schéma de Security Lake et utilise des modèles d'IA pour détecter les menaces.

Documentation d'intégration

ExtraHop – Reveal(x) 360

Type d'intégration : Source

Vous pouvez améliorer la sécurité de votre charge de travail et de vos applications en intégrant dans le schéma les données réseau, y compris les détections de IOCs Security LakeExtraHop Reveal(x) 360, en provenance ou en OCSF provenance de

Documentation d'intégration

Falcosidekick

Type d'intégration : Source

Falcosidekickcollecte et envoie les événements Falco à Security Lake. Cette intégration exporte les événements de sécurité à l'aide du OCSF schéma.

Documentation d'intégration

Fortinet - Cloud Native Firewall

Type d'intégration : Source

Lorsque vous créez FortiGate CNF des instances dans AWS, vous pouvez spécifier Amazon Security Lake comme destination de sortie du journal.

Documentation d'intégration

Gigamon – Application Metadata Intelligence

Type d'intégration : Source

Gigamon Application Metadata Intelligence (AMI)dote vos outils d'observabilité et de surveillance des performances du réseau d'attributs de métadonnées essentiels. SIEM Cela permet d'améliorer la visibilité des applications afin que vous puissiez identifier les goulots d'étranglement liés aux performances, les problèmes de qualité et les risques potentiels pour la sécurité du réseau.

Documentation d'intégration

Hoop Cyber

Type d'intégration : Service

Hoop Cyber FastStartinclut une évaluation des sources de données, une priorisation, l'intégration des sources de données et aide les clients à interroger leurs données à l'aide des outils et des intégrations existants proposés par Security Lake.

Lien vers le partenaire

IBM – QRadar

Type d'intégration : Abonné

IBM Security QRadar SIEM with UAXintègre Security Lake à une plateforme d'analyse qui identifie et prévient les menaces sur les clouds hybrides. Cette intégration prend en charge à la fois l'accès aux données et l'accès aux requêtes.

Documentation d'intégration sur la consommation de AWS CloudTrail journaux

Documentation d'intégration sur l'utilisation d'Amazon Athena pour les requêtes

Infosys

Type d'intégration : Service

Infosysvous aide à personnaliser la mise en œuvre de Security Lake en fonction des besoins de votre organisation et fournit des informations personnalisées.

Lien vers le partenaire

Insbuilt

Type d'intégration : Service

Insbuiltest spécialisé dans les services de conseil en cloud et peut vous aider à comprendre comment implémenter Security Lake dans votre organisation.

Lien vers le partenaire

Kyndryl – AIOps

Type d'intégration : Abonné, Service

Kyndryls'intègre à Security Lake pour assurer l'interopérabilité des cyberdonnées, des renseignements sur les menaces et des analyses basées sur l'IA. En tant qu'abonné à l'accès aux données, il Kyndryl ingère les événements de AWS CloudTrail gestion de Security Lake à des fins d'analyse.

En tant qu'intégration de services, Kyndryl elle peut également vous aider à implémenter Security Lake dans votre organisation.

Documentation d'intégration

Lacework – Polygraph

Type d'intégration : Source

Lacework Polygraph® Data Platforms'intègre à Security Lake en tant que source de données et fournit des informations de sécurité concernant les vulnérabilités, les erreurs de configuration et les menaces connues et inconnues dans votre AWS environnement.

Documentation d'intégration

Laminar

Type d'intégration : Source

Laminarenvoie les événements de sécurité des données à Security Lake sous forme de OCSF schéma, les rendant disponibles pour des cas d'utilisation analytiques supplémentaires, tels que la réponse aux incidents et les enquêtes.

Documentation d'intégration

MegazoneCloud

Type d'intégration : Service

MegazoneCloudest spécialisé dans les services de conseil en cloud et peut vous aider à comprendre comment implémenter Security Lake dans votre organisation. Nous connectons Security Lake à ISV des solutions intégrées pour créer des tâches personnalisées et obtenir des informations personnalisées liées aux besoins des clients.

Documentation d'intégration

Monad

Type d'intégration : Source

Monadtransforme automatiquement vos données en OCSF schéma et les envoie à votre lac de données Security Lake.

Documentation d'intégration

NETSCOUT – Omnis Cyber Intelligence

Type d'intégration : Source

En s'intégrant à Security Lake, NETSCOUT devenez une source personnalisée de résultats de sécurité et d'informations détaillées sur ce qui se passe dans votre entreprise, notamment les cybermenaces, les risques de sécurité et l'évolution des surfaces d'attaque. Ces résultats sont produits dans le compte client par NETSCOUT CyberStreams etOmnis Cyber Intelligence, puis envoyés à Security Lake sous forme de OCSF schéma. Les données ingérées répondent également à d'autres exigences et meilleures pratiques pour une source Security Lake, notamment en ce qui concerne le format, le schéma, le partitionnement et les aspects liés aux performances.

Documentation d'intégration

Netskope – CloudExchange

Type d'intégration : Source

Netskopevous aide à renforcer votre posture de sécurité en partageant les journaux liés à la sécurité et les informations sur les menaces avec Security Lake. Netskopeles résultats sont envoyés à Security Lake à l'aide d'un CloudExchange plugin, qui peut être lancé en tant qu'environnement basé sur Docker au sein AWS ou dans un centre de données local.

Documentation d'intégration

New Relic ONE

Type d'intégration : Abonné

New Relic ONEest une application d'abonnement basée sur Lambda. Il est déployé sur votre compte, déclenché par AmazonSQS, et envoie des données à New Relic l'aide de clés New Relic de licence

Documentation d'intégration

Okta – Workforce Identity Cloud

Type d'intégration : Source

Oktaenvoie des journaux d'identité à Security Lake sous OCSF forme de schéma via une EventBridge intégration Amazon. Okta System Logsin OCSF schema aidera les équipes de sécurité

et de data scientists à interroger les événements de sécurité selon un standard open source. La génération de OCSF journaux standardisés à partir d'Okta vous permet d'effectuer des activités d'audit et de générer des rapports relatifs à l'authentification, à l'autorisation, aux modifications de compte et aux modifications d'entité selon un schéma cohérent.

Documentation d'intégration

AWS CloudFormation modèle à ajouter Okta en tant que source personnalisée dans Security Lake

Orca – Cloud Security Platform

Type d'intégration : Source

La plateforme de sécurité cloud Orca sans agent AWS s'intègre à Security Lake en envoyant des événements Cloud Detection and Response (CDR) sous forme de OCSF schéma.

Documentation d'intégration (connectez-vous au Orca portail pour consulter la documentation)

Palo Alto Networks – Prisma Cloud

Type d'intégration : Source

Palo Alto Networks Prisma Cloudregroupe les données de détection des vulnérabilités VMs dans vos environnements cloud natifs et les envoie à Security Lake.

Documentation d'intégration

Palo Alto Networks – XSOAR

Type d'intégration : Abonné

Palo Alto Networks XSOARa créé une intégration des abonnés avec XSOAR Security Lake.

Documentation d'intégration

Panther

Type d'intégration : Abonné

Pantherprend en charge l'ingestion des journaux de Security Lake à des fins de recherche et de détection.

Documentation d'intégration

Ping Identity – PingOne

Type d'intégration : Source

PingOneenvoie des alertes de modification de compte à Security Lake sous forme de OCSF schéma et de format Parquet, ce qui vous permet de découvrir les modifications de compte et d'agir en conséquence.

Documentation d'intégration

PwC – Fusion center

Type d'intégration : Abonné, Service

PwC apporte ses connaissances et son expertise pour aider ses clients à mettre en place un centre de fusion répondant à leurs besoins individuels. Construit sur Amazon Security Lake, un centre de fusion permet de combiner des données provenant de diverses sources pour créer une vue centralisée en temps quasi réel.

Documentation d'intégration

Query.AI – Query Federated Search

Type d'intégration : Abonné

Query Federated Searchpeut interroger directement n'importe quelle table de Security Lake via Amazon Athena pour faciliter la réponse aux incidents, les enquêtes, la recherche des menaces et la recherche générale sur une variété d'observables, d'événements et d'objets du schéma. OCSF

Documentation d'intégration

Rapid7 – InsightIDR

Type d'intégration : Abonné

InsightIDR, la XDR solution Rapid7SIEM/, peut ingérer des journaux dans Security Lake à des fins de détection des menaces et d'investigation en cas d'activité suspecte.

Documentation d'intégration

RipJar – Labyrinth for Threat Investigations

Type d'intégration : Abonné

Labyrinth for Threat Investigationspropose une approche à l'échelle de l'entreprise pour l'exploration des menaces à grande échelle basée sur la fusion des données, avec une sécurité précise, des flux de travail adaptables et des rapports.

Documentation d'intégration

Sailpoint

Type d'intégration : Source

Produit partenaire pour l'intégration : SailPoint IdentityNow

Cette intégration permet aux clients de transformer les données d'événements à partir deSailPoint IdentityNow. L'intégration vise à fournir un processus automatisé permettant d'intégrer IdentityNow l'activité des utilisateurs et les événements de gouvernance dans Security Lake afin d'améliorer les informations issues des produits de surveillance des incidents et des événements de sécurité.

Documentation d'intégration

Securonix

Type d'intégration : Abonné

Securonix Next-Gen SIEMs'intègre à Security Lake, permettant aux équipes de sécurité d'ingérer les données plus rapidement et d'étendre leurs capacités de détection et de réponse.

Documentation d'intégration

SentinelOne

Type d'intégration : Abonné

La SentinelOne Singularity™ XDR plateforme étend la détection et la réponse en temps réel aux charges de travail des terminaux, des identités et du cloud exécutées sur des infrastructures de cloud public et sur site, notamment Amazon Elastic Compute Cloud EC2 (Amazon), Amazon Elastic Container Service (AmazonECS) et Amazon Elastic Kubernetes Service (Amazon). EKS

Documentation d'intégration (connectez-vous au SentinelOne portail pour consulter la documentation)

Sentra – Data Lifecyle Security Platform

Type d'intégration : Source

Après avoir déployé l'infrastructure de Sentra numérisation dans votre compte, Sentra récupérez les résultats et intégrez-les dans votre SaaS. Ces résultats sont des métadonnées qui sont Sentra stockées puis transmises à Security Lake sous forme de OCSF schéma pour les requêtes.

Documentation d'intégration

SOC Prime

Type d'intégration : Abonné

SOC Primes'intègre à Security Lake via Amazon OpenSearch Service et Amazon Athena pour faciliter l'orchestration intelligente des données et la détection des menaces sur la base d'objectifs de confiance zéro. SOC Primepermet aux équipes de sécurité d'accroître la visibilité des menaces et d'enquêter sur les incidents sans générer un volume impressionnant d'alertes. Vous pouvez gagner du temps de développement grâce à des règles et requêtes réutilisables qui sont automatiquement convertibles en Athena et OpenSearch Service dans le OCSF schéma.

Documentation d'intégration

Splunk

Type d'intégration : Abonné

Le Splunk AWS module complémentaire pour Amazon Web Services (AWS) prend en charge l'ingestion depuis Security Lake. Cette intégration vous permet d'accélérer la détection, l'investigation et la réponse aux menaces en vous abonnant aux données du OCSF schéma de Security Lake.

Documentation d'intégration

Stellar Cyber

Type d'intégration : Abonné

Stellar Cyberconsomme les journaux de Security Lake et ajoute les enregistrements au lac de Stellar Cyber données. Ce connecteur utilise OCSF un schéma.

Documentation d'intégration

Sumo Logic

Type d'intégration : Abonné

Sumo Logicconsomme les données de Security Lake et offre une visibilité étendue sur AWS les environnements cloud hybrides et sur site. Sumo Logic offre aux équipes de sécurité une visibilité complète, une automatisation et une surveillance des menaces sur l'ensemble de leurs outils de sécurité.

Documentation d'intégration

Swimlane – Turbine

Type d'intégration : Abonné

Swimlaneingère les données de Security Lake sous forme de OCSF schéma et les envoie par le biais de playbooks low-code et de gestion de cas pour accélérer la détection des menaces, les enquêtes et la réponse aux incidents.

Documentation d'intégration (connectez-vous au Swimlane portail pour consulter la documentation)

Sysdig Secure

Type d'intégration : Source

Sysdig Secure'sune plateforme de protection des applications native dans le cloud (CNAPP) envoie les événements de sécurité à Security Lake afin d'optimiser la supervision, de rationaliser les enquêtes et de simplifier la conformité.

Documentation d'intégration

Talon

Type d'intégration : Source

Produit partenaire pour l'intégration : Talon Enterprise Browser

Talon's Enterprise Browser, un environnement de point de terminaison sécurisé et isolé basé sur un navigateur, envoie les Talon accès, la protection des données, les actions SaaS et les événements

de sécurité à Security Lake, offrant ainsi une visibilité et des options permettant de corréler les événements à des fins de détection, de criminalistique et d'investigation.

Documentation d'intégration (connectez-vous au Talon portail pour consulter la documentation)

Tanium

Type d'intégration : Source

Tanium Unified Cloud Endpoint Detection, Management, and SecurityLa plateforme fournit des données d'inventaire à Security Lake sous forme de OCSF schéma.

Documentation d'intégration

TCS

Type d'intégration : Service

Elle TCS AWS Business Unit offre innovation, expérience et talent. Cette intégration est le fruit d'une décennie de création de valeur conjointe, de connaissances approfondies du secteur, d'expertise technologique et de sagesse en matière de livraison. En tant qu'intégration de services, TCS elle peut vous aider à implémenter Security Lake dans votre organisation.

Documentation d'intégration

Tego Cyber

Type d'intégration : Abonné

Tego Cybers'intègre à Security Lake pour vous aider à détecter et à étudier rapidement les menaces de sécurité potentielles. En corrélant divers indicateurs de menaces sur de longues périodes et dans des sources de log étendues, Tego Cyber découvre les menaces cachées. La plateforme est enrichie de renseignements sur les menaces hautement contextuels, fournissant précision et informations pour la détection des menaces et les enquêtes.

Documentation d'intégration

Tines – No-code security automation

Type d'intégration : Abonné

Tines No-code security automationvous aide à prendre des décisions plus précises en exploitant les données de sécurité centralisées dans Security Lake.

Documentation d'intégration

Torq – Enterprise Security Automation Platform

Type d'intégration : Source, Abonné

Torqs'intègre parfaitement à Security Lake en tant que source personnalisée et en tant qu'abonné. Torqvous aide à mettre en œuvre l'automatisation et l'orchestration à l'échelle de l'entreprise grâce à une plate-forme simple sans code.

Documentation d'intégration

Trellix – XDR

Type d'intégration : Source, Abonné

En tant que XDR plate-forme ouverte, Trellix XDR prend en charge l'intégration de Security Lake. Trellix XDRpeut exploiter les données du OCSF schéma pour les cas d'utilisation de l'analyse de sécurité. Vous pouvez également compléter votre lac de données Security Lake en y ajoutant plus de 1 000 sources d'événements de sécurité. Trellix XDR Cela vous permet d'étendre les capacités de détection et de réponse de votre AWS environnement. Les données ingérées sont corrélées à d'autres risques de sécurité, vous fournissant ainsi les outils nécessaires pour répondre à un risque en temps opportun.

Documentation d'intégration

Trend Micro – CloudOne

Type d'intégration : Source

Trend Micro CloudOne Workload Securityenvoie les informations suivantes à Security Lake depuis vos instances Amazon Elastic Compute Cloud (EC2) :

- DNSActivité de requête
- Activité des fichiers
- Activité du réseau
- Activité du processus

- Activité relative à la valeur du registre
- Activité du compte utilisateur

Documentation d'intégration

Uptycs – Uptycs XDR

Type d'intégration : Source

Uptycsenvoie une multitude de données sous forme de OCSF schéma à partir d'actifs sur site et dans le cloud vers Security Lake. Les données incluent les détections de menaces comportementales provenant des terminaux et des charges de travail dans le cloud, les détections d'anomalies, les violations des politiques, les politiques risquées, les erreurs de configuration et les vulnérabilités.

Documentation d'intégration

Vectra AI – Vectra Detect for AWS

Type d'intégration : Source

En utilisantVectra Detect for AWS, vous pouvez envoyer des alertes haute fidélité à Security Lake en tant que source personnalisée à l'aide d'un AWS CloudFormation modèle dédié.

Documentation d'intégration

VMware Aria Automation for Secure Clouds

Type d'intégration : Source

Grâce à cette intégration, vous pouvez détecter les erreurs de configuration du cloud et les envoyer à Security Lake pour une analyse avancée.

Documentation d'intégration

Wazuh

Type d'intégration : Abonné

Wazuhvise à gérer en toute sécurité les données des utilisateurs, à fournir un accès aux requêtes pour chaque source et à optimiser les coûts d'interrogation.

Documentation d'intégration

Wipro

Type d'intégration : Source, Service

Cette intégration vous permet de collecter des données à partir de la Wipro Cloud Application Risk Governance (CARG) plateforme afin de fournir une vue unifiée de vos applications cloud et des postures de conformité au sein de l'entreprise.

En tant qu'intégration de services, Wipro elle peut également vous aider à implémenter Security Lake dans votre organisation.

Documentation d'intégration

Wiz – CNAPP

Type d'intégration : Source

L'intégration entre Security Lake Wiz et Security Lake facilite la collecte des données de sécurité du cloud dans un seul lac de données de sécurité en tirant parti du OCSF schéma, une norme open source conçue pour un échange de données de sécurité extensible et normalisé.

Documentation d'intégration (connectez-vous au Wiz portail pour consulter la documentation)

Zscaler – Zscaler Posture Control

Type d'intégration : Source

Zscaler Posture Control™, une plateforme de protection des applications native dans le cloud, envoie les résultats de sécurité à Security Lake sous forme de OCSF schéma.

Documentation d'intégration

Sécurité dans Amazon Security Lake

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Security Lake, consultez AWSServices classés par programme de conformité AWS .
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Security Lake. Les rubriques suivantes expliquent comment configurer Security Lake pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Security Lake.

Rubriques

Gestion des identités et des accès pour Amazon Security Lake

AWS Identity and Access Management (IAM) est un outil AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de Security Lake. IAMest un AWS service outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Security Lake.

Utilisateur du service : si vous utilisez le service Security Lake pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Security Lake pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Security Lake, consultezRésolution des problèmes d'identité et d'accès à Amazon Security Lake.

Administrateur de services — Si vous êtes responsable des ressources de Security Lake au sein de votre entreprise, vous avez probablement un accès complet à Security Lake. Il vous incombe de déterminer les fonctionnalités et les ressources de Security Lake auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la manière dont votre

entreprise peut utiliser IAM Security Lake, consultezComment fonctionne Amazon Security Lake avec IAM.

IAMadministrateur : si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Security Lake. Pour consulter des exemples de politiques basées sur l'identité de Security Lake que vous pouvez utiliserIAM, consultez. Exemples de politiques basées sur l'identité pour Amazon Security Lake

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des AWS API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes AWS services les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide AWS services d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies AWS services par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons

de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir Quand créer un IAM utilisateur (au lieu d'un rôle) dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.

- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains AWS services cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- Accès multiservices — Certains AWS services utilisent des fonctionnalités dans d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui font AWS CLI des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation

d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment fonctionne Amazon Security Lake avec IAM

Avant de commencer IAM à gérer l'accès à Security Lake, découvrez quelles IAM fonctionnalités peuvent être utilisées avec Security Lake.

IAMfonctionnalités que vous pouvez utiliser avec Amazon Security Lake

IAMfonctionnalité	Support de Security Lake
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACLs	Non
ABAC(balises dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble du fonctionnement de Security Lake et AWS des autres services avec la plupart des IAM fonctionnalités, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour Security Lake

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Security Lake prend en charge les politiques basées sur l'identité. Pour de plus amples informations, veuillez consulter Exemples de politiques basées sur l'identité pour Amazon Security Lake.

Politiques basées sur les ressources au sein de Security Lake

Prend en charge les politiques basées sur les ressources : Oui

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. AWS services

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Le service Security Lake crée des politiques basées sur les ressources pour les compartiments Amazon S3 qui stockent vos données. Vous n'associez pas ces politiques basées sur les ressources à vos compartiments S3. Security Lake crée automatiquement ces politiques en votre nom.

Un exemple de ressource est un compartiment S3 dont le nom de ressource Amazon (ARN) est `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`. Dans cet

exemple, `region` il s'agit d'une chaîne alphanumérique spécifique à Région AWS laquelle vous avez activé Security Lake. `bucket-identifier` Il s'agit d'une chaîne alphanumérique unique au niveau régional que Security Lake attribue au bucket. Security Lake crée le compartiment S3 pour stocker les données de cette région. La politique de ressources définit les principaux autorisés à effectuer des actions sur le compartiment. Voici un exemple de politique basée sur les ressources (stratégie de compartiment) que Security Lake attache au compartiment :

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

Pour en savoir plus sur les politiques basées sur les ressources, consultez les sections Politiques basées sur l'identité et politiques basées sur les ressources dans le Guide de l'utilisateur. IAM

Actions politiques pour Security Lake

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour obtenir la liste des actions de Security Lake, consultez la section Actions définies par Amazon Security Lake dans le Service Authorization Reference.

Les actions de politique dans Security Lake utilisent le préfixe suivant avant l'action :

```
securitylake
```

Par exemple, pour autoriser un utilisateur à accéder aux informations concernant un abonné spécifique, incluez l'`securitylake:GetSubscriber`action dans la politique attribuée à cet utilisateur. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. Security Lake définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour consulter des exemples de politiques basées sur l'identité de Security Lake, consultez. Exemples de politiques basées sur l'identité pour Amazon Security Lake

Ressources relatives aux politiques pour Security Lake

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Security Lake définit les types de ressources suivants : abonné et configuration du lac de données pour une ressource Compte AWS en particulier Région AWS. Vous pouvez spécifier ces types de ressources dans les politiques en utilisantARNs.

Pour obtenir la liste des types de ressources Security Lake et la ARN syntaxe de chacun d'entre eux, consultez la section Types de ressources définis par Amazon Security Lake dans le Service Authorization Reference. Pour savoir quelles actions vous pouvez spécifier pour chaque type

de ressource, consultez la section Actions définies par Amazon Security Lake dans le Service Authorization Reference.

Pour consulter des exemples de politiques basées sur l'identité de Security Lake, consultez. Exemples de politiques basées sur l'identité pour Amazon Security Lake

Clés de condition des politiques pour Security Lake

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour obtenir la liste des clés de condition de Security Lake, consultez la section Clés de condition pour Amazon Security Lake dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Amazon Security Lake dans le Service Authorization Reference. Pour des exemples de politiques

utilisant des clés de condition, consultezExemples de politiques basées sur l'identité pour Amazon Security Lake.

Listes de contrôle d'accès (ACLs) dans Security Lake

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Security Lake n'est pas compatibleACLs, ce qui signifie que vous ne pouvez pas associer un ACL à une ressource Security Lake.

Contrôle d'accès basé sur les attributs (ABAC) avec Security Lake

Supports ABAC (balises dans les politiques) : Oui

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Vous pouvez associer des balises aux ressources de Security Lake : les abonnés et la configuration du lac de données pour un Compte AWS utilisateur individuel. Régions AWS Vous pouvez également contrôler l'accès à ces types de ressources en fournissant des informations de balise dans l'`Condition`élément d'une politique. Pour plus d'informations sur le balisage des ressources de Security Lake, consultezMarquage des ressources d'Amazon Security Lake. Pour un exemple de politique basée sur l'identité qui contrôle l'accès à une ressource en fonction des balises associées à cette ressource, consultez. Exemples de politiques basées sur l'identité pour Amazon Security Lake

Utilisation d'informations d'identification temporaires avec Security Lake

Prend en charge les informations d'identification temporaires : oui

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui AWS services fonctionnent avec des informations d'identification temporaires, consultez AWS services la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Security Lake prend en charge l'utilisation d'informations d'identification temporaires.

Sessions d'accès direct pour Security Lake

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une

action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Certaines actions de Security Lake nécessitent des autorisations pour des actions supplémentaires dépendantes dans d'autres AWS services. Pour obtenir la liste de ces actions, consultez la section Actions définies par Amazon Security Lake dans le Service Authorization Reference.

Rôles de service pour Security Lake

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

Security Lake n'assume ni n'utilise de rôles de service. Toutefois, les services connexes tels qu'Amazon EventBridge et Amazon S3 assument des rôles de service lorsque vous utilisez Security Lake. AWS Lambda Pour effectuer des actions en votre nom, Security Lake utilise un rôle lié à un service.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut entraîner des problèmes opérationnels liés à votre utilisation de Security Lake. Modifiez les rôles de service uniquement lorsque Security Lake fournit des instructions à cet effet.

Rôles liés à un service pour Security Lake

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre

Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Security Lake utilise un rôle IAM lié à un service nommé. `AWSServiceRoleForAmazonSecurityLake` Le rôle lié au service Security Lake accorde les autorisations nécessaires pour exploiter un service de lac de données de sécurité pour le compte des clients. Ce rôle lié à un service est un IAM rôle directement lié à Security Lake. Il est prédéfini par Security Lake et inclut toutes les autorisations dont Security Lake a besoin pour appeler d'autres personnes AWS services en votre nom. Security Lake utilise ce rôle lié au service partout Régions AWS où Security Lake est disponible.

Pour plus de détails sur la création ou la gestion du rôle lié au service Security Lake, consultez. Rôle lié à un service pour Amazon Security Lake

Exemples de politiques basées sur l'identité pour Amazon Security Lake

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources de Security Lake. Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par Security Lake, y compris le format ARNs de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Security Lake dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Security Lake
- Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations
- Exemple : autoriser le compte de gestion de l'organisation à désigner et supprimer un administrateur délégué
- Exemple : autoriser les utilisateurs à évaluer les abonnés en fonction des balises

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources Security Lake de votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique AWS service, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles respectent le langage des politiques (JSON) et IAM les IAM meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire.

Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console Security Lake

Pour accéder à la console Amazon Security Lake, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources Security Lake de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent utiliser la console Security Lake, créez des IAM politiques qui leur fournissent un accès à la console. Pour plus d'informations, consultez la section IAMIdentités dans le Guide de IAM l'utilisateur.

Si vous créez une politique qui autorise les utilisateurs ou les rôles à utiliser la console Security Lake, assurez-vous qu'elle inclut les actions appropriées pour les ressources auxquelles ces utilisateurs ou rôles doivent accéder sur la console. Dans le cas contraire, ils ne pourront pas accéder à ces ressources ou les afficher sur la console.

Par exemple, pour ajouter une source personnalisée à l'aide de la console, un utilisateur doit être autorisé à effectuer les actions suivantes :

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

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

Exemple : Autoriser les utilisateurs à afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : autoriser le compte de gestion de l'organisation à désigner et supprimer un administrateur délégué

Cet exemple montre comment créer une politique qui permet à l'utilisateur d'un compte de AWS Organizations gestion de désigner et de supprimer l'administrateur délégué de Security Lake pour son organisation.

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

Exemple : autoriser les utilisateurs à évaluer les abonnés en fonction des balises

Dans les politiques basées sur l'identité, vous pouvez utiliser des conditions pour contrôler l'accès aux ressources de Security Lake en fonction de balises. Cet exemple montre comment créer une politique qui permet à un utilisateur d'évaluer les abonnés à l'aide de la console Security Lake ou du Security LakeAPI. Toutefois, l'autorisation n'est accordée que si la valeur du `Owner` tag pour un abonné est le nom d'utilisateur de l'utilisateur.

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

Dans cet exemple, si un utilisateur possédant le nom d'utilisateur `richard-roe` tente de consulter les informations relatives à des abonnés individuels, un abonné doit être étiqueté `Owner=richard-roe` ou`owner=richard-roe`. Dans le cas contraire, l'utilisateur se voit refuser l'accès. La clé de condition de balise `Owner` correspond à la fois à `Owner` et à `owner`, car les noms de clé de condition ne sont pas sensibles à la casse. Pour plus d'informations sur l'utilisation des clés de condition, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur. Pour plus d'informations sur le balisage des ressources de Security Lake, consultezMarquage des ressources d'Amazon Security Lake.

AWS politiques gérées pour Amazon Security Lake

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle AWS service est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonSecurityLakeMetastoreManager

Amazon Security Lake utilise une AWS Lambda fonction pour gérer les métadonnées de votre lac de données. Grâce à cette fonction, Security Lake peut indexer les partitions Amazon Simple Storage Service (Amazon S3) contenant vos données et vos fichiers de données dans les tables AWS Glue du catalogue de données. Cette politique gérée contient toutes les autorisations permettant à la fonction Lambda d'indexer les partitions S3 et les fichiers de données dans les AWS Glue tables.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `logs`— Permet aux principaux de consigner la sortie de la fonction Lambda dans Amazon CloudWatch Logs.
- `glue`— Permet aux principaux d'effectuer des actions d'écriture spécifiques pour les tables du catalogue de AWS Glue données. Cela permet également aux AWS Glue robots d'exploration d'identifier les partitions de vos données.
- `sqs`— Permet aux principaux d'effectuer des actions de lecture et d'écriture spécifiques pour les files d'attente Amazon SQS qui envoient des notifications d'événements lorsque des objets sont ajoutés ou mis à jour dans votre lac de données.
- `s3`— Permet aux principaux d'effectuer des actions de lecture et d'écriture spécifiques pour le compartiment Amazon S3 qui contient vos données.

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

```
    {
      "Sid": "AllowWriteLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowGlueManage",
      "Effect": "Allow",
      "Action": [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowToReadFromSqs",
      "Effect": "Allow",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
```

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

```
  ]
}
```

AWS politique gérée : AmazonSecurityLakePermissionsBoundary

Amazon Security Lake crée des rôles IAM pour les sources personnalisées tierces afin d'écrire des données dans le lac de données et pour les abonnés personnalisés tiers pour consommer les données du lac de données, et utilise cette politique lors de la création de ces rôles afin de définir les limites de leurs autorisations. Il n'est pas nécessaire de prendre des mesures pour utiliser cette politique. Si le lac de données est chiffré à l'aide d'une AWS KMS clé gérée par le client `kms:Decrypt` et que `kms:GenerateDataKey` des autorisations sont ajoutées.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsForSecurityLake",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsForSecurityLake",
      "Effect": "Deny",
      "NotAction": [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeBucket",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeSQS",
      "Effect": "Deny",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
```

```
      "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "kms:ViaService": [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:s3:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:s3:arn": [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:sqs:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:sqs:arn": [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

AWS politique gérée : AmazonSecurityLakeAdministrator

Vous pouvez associer la `AmazonSecurityLakeAdministrator` politique à un mandant avant qu'il n'active Amazon Security Lake pour son compte. Cette politique accorde des autorisations administratives qui permettent un accès complet principal à toutes les actions de Security Lake. Le principal peut ensuite intégrer Security Lake, puis configurer les sources et les abonnés dans Security Lake.

Cette politique inclut les actions que les administrateurs de Security Lake peuvent effectuer sur d'autres AWS services via Security Lake.

La `AmazonSecurityLakeAdministrator` politique ne prend pas en charge la création des rôles utilitaires requis par Security Lake pour gérer la réplication interrégionale d'Amazon S3, l'enregistrement de nouvelles partitions de données AWS Glue, l'exécution d'un robot Glue sur les données ajoutées à des sources personnalisées ou la notification des nouvelles données aux abonnés des points de terminaison HTTPS. Vous pouvez créer ces rôles à l'avance, comme décrit dansCommencer à utiliser Amazon Security Lake.

Outre la politique `AmazonSecurityLakeAdministrator` gérée, Security Lake nécessite des `lakeformation:PutDataLakeSettings` autorisations pour les fonctions d'intégration et de configuration. `PutDataLakeSettings`permet de définir un directeur IAM en tant qu'administrateur de toutes les ressources régionales de Lake Formation présentes dans le compte. Ce `iam:CreateRole permission` rôle doit être assorti d'une `AmazonSecurityLakeAdministrator` politique.

Les administrateurs de Lake Formation ont un accès complet à la console Lake Formation et contrôlent la configuration initiale des données et les autorisations d'accès. Security Lake attribue le principal qui active Security Lake et le `AmazonSecurityLakeMetaStoreManager` rôle (ou tout autre rôle spécifié) en tant qu'administrateurs de Lake Formation afin qu'ils puissent créer des tables, mettre à jour le schéma des tables, enregistrer de nouvelles partitions et configurer des autorisations sur les tables. Vous devez inclure les autorisations suivantes dans la politique relative à l'utilisateur ou au rôle d'administrateur de Security Lake :

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

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `securitylake`— Permet aux principaux un accès complet à toutes les actions de Security Lake.
- `organizations`— Permet aux directeurs de récupérer des informations auprès des AWS Organizations concernant les comptes d'une organisation. Si un compte appartient à une organisation, ces autorisations permettent à la console Security Lake d'afficher les noms et numéros de compte.
- `iam`— Permet aux principaux de créer des rôles liés aux services pour Security Lake et, AWS Lake Formation comme étape obligatoire Amazon EventBridge, lors de l'activation de ces services. Permet également de créer et de modifier des politiques pour les rôles d'abonné et de source

personnalisée, les autorisations associées à ces rôles étant limitées à ce qui est autorisé par la `AmazonSecurityLakePermissionsBoundary` politique.

- `ram`— Permet aux principaux de configurer l'accès aux requêtes Lake Formation basé sur les requêtes par les abonnés aux sources de Security Lake.
- `s3`— Permet aux directeurs de créer et de gérer des compartiments Security Lake, et de lire le contenu de ces compartiments.
- `lambda`— Permet aux principaux de gérer les partitions Lambda utilisées pour mettre à jour les partitions de AWS Glue table après la livraison de la AWS source et la réplication entre régions.
- `glue`— Permet aux principaux de créer et de gérer la base de données et les tables de Security Lake.
- `lakeformation`— Permet aux principaux de gérer les Lake Formation autorisations pour les tables Security Lake.
- `events`— Permet aux principaux de gérer les règles utilisées pour informer les abonnés des nouvelles données dans les sources de Security Lake.
- `sqs`— Permet aux principaux de créer et de gérer les Amazon SQS files d'attente utilisées pour informer les abonnés des nouvelles données dans les sources de Security Lake.
- `kms`— Permet aux principaux d'autoriser Security Lake à écrire des données à l'aide d'une clé gérée par le client.
- `secretsmanager`— Permet aux principaux de gérer les secrets utilisés pour informer les abonnés des nouvelles données dans les sources de Security Lake via des points de terminaison 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 politique gérée : SecurityLakeServiceLinkedRole

Vous ne pouvez pas associer la politique `SecurityLakeServiceLinkedRole` gérée à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Security Lake d'effectuer des actions en votre nom. Pour plus d'informations, consultez Rôle lié à un service pour Amazon Security Lake.

AWS politique gérée : AWS GlueService rôle

La politique `AWS GlueServiceRole` gérée appelle le AWS Glue robot d'exploration et permet d' AWS Glue explorer les données source personnalisées et d'identifier les métadonnées de partition. Ces métadonnées sont nécessaires pour créer et mettre à jour des tables dans le catalogue de données.

Pour plus d'informations, consultez Collecte de données à partir de sources personnalisées.

Mises à jour des politiques AWS gérées par Security Lake

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour Security Lake depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents de Security Lake.

Modification	Description	Date
Rôle lié à un service pour Amazon Security Lake — Mise à jour des autorisations de rôle liées à un service existantes	Nous avons ajouté AWS WAF des actions à la stratégie AWS gérée pour la `SecurityLakeServiceLinkedRole` stratégie. Les actions supplémentaires permettent à Security Lake de collecter AWS WAF des journaux lorsqu'il est activé en tant que source de journaux dans Security Lake.	22 mai 2024
AmazonSecurityLakePermissionsBoundary – Mise à jour d'une politique existante	Security Lake a ajouté des actions SID à la politique.	13 mai 2024
AmazonSecurityLakeMetastoreManager – Mise à jour d'une politique existante	Security Lake a mis à jour la politique pour ajouter une action de nettoyage des métadonnées qui vous permet de supprimer les métadonnées de votre lac de données.	27 mars 2024

Modification	Description	Date
AmazonSecurityLakeAdministrator – Mise à jour d'une politique existante	Security Lake a mis à jour la politique pour autoriser `iam:PassRole` le nouveau `AmazonSecurityLakeMetastoreManagerV2` rôle et permet à Security Lake de déployer ou de mettre à jour les composants du lac de données.	23 février 2024
AmazonSecurityLakeMetastoreManager : nouvelle politique	Security Lake a ajouté une nouvelle politique gérée qui autorise Security Lake à gérer les métadonnées de votre lac de données.	23 janvier 2024
AmazonSecurityLakeAdministrator : nouvelle politique	Security Lake a ajouté une nouvelle politique gérée qui accorde un accès complet principal à toutes les actions de Security Lake.	30 mai 2023
Security Lake a commencé à suivre les modifications	Security Lake a commencé à suivre les modifications apportées AWS à ses politiques gérées.	29 novembre 2022

Rôle lié à un service pour Amazon Security Lake

Security Lake utilise un rôle lié à un service AWS Identity and Access Management (IAM) nommé. `AWSServiceRoleForSecurityLake` Ce rôle lié à un service est un rôle IAM directement lié à Security Lake. Il est prédéfini par Security Lake et inclut toutes les autorisations dont Security Lake a besoin pour appeler d'autres AWS services personnes en votre nom et exploiter le service Security Data Lake. Security Lake utilise ce rôle lié au service partout Régions AWS où Security Lake est disponible.

Le rôle lié au service élimine le besoin d'ajouter manuellement les autorisations nécessaires lors de la configuration de Security Lake. Security Lake définit les autorisations de ce rôle lié au service et, sauf indication contraire, seul Security Lake peut assumer le rôle. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM. Vous ne pouvez supprimer un rôle lié à un service qu'après avoir supprimé les ressources associées. Vos ressources sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Cliquez sur Oui avec un lien pour consulter la documentation relative aux rôles liés à un service pour ce service.

Rubriques

- Autorisations de rôle liées à un service pour Security Lake
- Création du rôle lié au service Security Lake
- Modification du rôle lié au service Security Lake
- Suppression du rôle lié au service Security Lake
- Pris en charge Régions AWS pour le rôle lié au service Security Lake

Autorisations de rôle liées à un service pour Security Lake

Security Lake utilise le rôle lié au service nommé. `AWSServiceRoleForSecurityLake` Ce rôle lié au service fait confiance au `securitylake.amazonaws.com` service pour assumer le rôle. Pour plus d'informations sur les politiques AWS gérées pour Amazon Security Lake, consultez la section AWS Gérer les politiques pour Amazon Security Lake.

La politique d'autorisations pour le rôle, qui est une stratégie AWS gérée nommée`SecurityLakeServiceLinkedRole`, permet à Security Lake de créer et d'exploiter le lac de données de sécurité. Cela permet également à Security Lake d'effectuer des tâches telles que les suivantes sur les ressources spécifiées :

- Utiliser AWS Organizations des actions pour récupérer des informations sur les comptes associés
- Utilisez Amazon Elastic Compute Cloud (Amazon EC2) pour récupérer des informations sur Amazon VPC Flow Logs
- Utiliser AWS CloudTrail des actions pour récupérer des informations sur le rôle lié au service
- Utiliser AWS WAF des actions pour collecter AWS WAF des journaux, lorsqu'il est activé en tant que source de journaux dans Security Lake
- Utilisez l'`LogDelivery`action pour créer ou supprimer un abonnement de livraison de AWS WAF journaux.

Le rôle est configuré selon la politique d'autorisation suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "OrganizationsPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DescribeOrgAccounts",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount"
            ],
            "Resource": [
                "arn:aws:organizations::*:account/o-*/*"
            ]
        },
        {
            "Sid": "AllowManagementOfServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateServiceLinkedChannel",
                "cloudtrail:DeleteServiceLinkedChannel",
```

```
                "cloudtrail:GetServiceLinkedChannel",
                "cloudtrail:UpdateServiceLinkedChannel"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
        },
        {
            "Sid": "AllowListServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:ListServiceLinkedChannels"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DescribeAnyVpc",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListDelegatedAdmins",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securitylake.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowWafLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration",
                "wafv2:GetLoggingConfiguration",
                "wafv2:ListLoggingConfigurations",
                "wafv2:DeleteLoggingConfiguration"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "wafv2:LogScope": "SecurityLake"
                }
            }
        },
        {
            "Sid": "AllowPutLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-
security-lake-*"
                }
            }
        },
        {
            "Sid": "ListWebACLs",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LogDelivery",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "wafv2.amazonaws.com"
                    ]
                }
            }
```

```
        }

    ]
}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle lié au service Security Lake

Il n'est pas nécessaire de créer manuellement le rôle `AWSServiceRoleForSecurityLake` lié à un service pour Security Lake. Lorsque vous activez Security Lake pour votre Compte AWS, Security Lake crée automatiquement le rôle lié au service pour vous.

Modification du rôle lié au service Security Lake

Security Lake ne vous permet pas de modifier le rôle `AWSServiceRoleForSecurityLake` lié au service. Une fois qu'un rôle lié à un service est créé, vous ne pouvez pas modifier le nom du rôle car différentes entités peuvent y faire référence. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression du rôle lié au service Security Lake

Vous ne pouvez pas supprimer le rôle lié au service dans Security Lake. Vous pouvez plutôt supprimer le rôle lié au service de la console IAM, de l'API ou. AWS CLI Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Avant de pouvoir supprimer le rôle lié à un service, vous devez d'abord confirmer qu'aucune session n'est active pour le rôle et supprimer toutes les ressources qui `AWSServiceRoleForSecurityLake` l'utilisent.

> **Note**
>
> Si Security Lake utilise le `AWSServiceRoleForSecurityLake` rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Dans ce cas, attendez quelques minutes, puis recommencez l'opération.

Si vous supprimez le rôle `AWSServiceRoleForSecurityLake` lié au service et que vous devez le créer à nouveau, vous pouvez le créer à nouveau en activant Security Lake pour votre compte. Lorsque vous réactivez Security Lake, Security Lake crée automatiquement le rôle lié au service pour vous.

Pris en charge Régions AWS pour le rôle lié au service Security Lake

Security Lake prend en charge l'utilisation du rôle `AWSServiceRoleForSecurityLake` lié au service partout Régions AWS où Security Lake est disponible. Pour obtenir la liste des régions dans lesquelles Security Lake est actuellement disponible, consultezAmazon Security.

Protection des données dans Amazon Security Lake

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans Amazon Security Lake. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.

- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Security Lake ou un autre utilisateur AWS services à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas y inclure d'informations d'identification URL pour valider votre demande auprès de ce serveur.

Chiffrement au repos

Amazon Security Lake stocke vos données au repos en toute sécurité à l'aide de solutions de AWS chiffrement. Les données brutes du journal de sécurité et des événements sont stockées dans un bucket Amazon Simple Storage Service (Amazon S3) multi-tenant dans un compte géré par Security Lake. Security Lake chiffre ces données brutes à l'aide d'une cléAWS détenue par AWS Key Management Service (AWS KMS). AWS les clés détenues sont un ensemble de AWS KMS clés qu'un AWS service (dans ce cas Security Lake) possède et gère pour une utilisation dans plusieurs comptes. AWS

Security Lake exécute des tâches d'extraction, de transformation et de chargement (ETL) sur les données brutes des journaux et des événements. Les données traitées restent cryptées dans le compte de service Security Lake.

Une fois les ETL tâches terminées, Security Lake crée des compartiments S3 à locataire unique dans votre compte (un compartiment pour chacun des compartiments dans Région AWS lesquels vous avez activé Security Lake). Les données ne sont stockées dans le compartiment S3 à locataire multiple que temporairement jusqu'à ce que Security Lake puisse les fournir de manière fiable aux compartiments S3 à locataire unique. Les compartiments à locataire unique incluent une politique basée sur les ressources qui autorise Security Lake à écrire des données de journal et d'événement dans les compartiments. Pour chiffrer les données de votre compartiment S3, vous pouvez choisir une clé de chiffrement gérée par S3 ou une clé gérée par le client (à partir de). AWS KMS Les deux options utilisent le chiffrement symétrique.

Utilisation d'une KMS clé pour le chiffrement de vos données

Par défaut, les données fournies par Security Lake à votre compartiment S3 sont chiffrées par chiffrement côté serveur Amazon avec des clés de chiffrement gérées par Amazon S3 (-S3). SSE Pour fournir une couche de sécurité que vous gérez directement, vous pouvez plutôt utiliser le chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) pour vos données Security Lake.

SSE- KMS n'est pas pris en charge dans la console Security Lake. À utiliser SSE : KMS avec le Security Lake API ouCLI, vous devez d'abord créer une KMS clé ou utiliser une clé existante. Vous attachez une politique à la clé qui détermine quels utilisateurs peuvent utiliser la clé pour chiffrer et déchiffrer les données de Security Lake.

Si vous utilisez une clé gérée par le client pour chiffrer les données écrites dans votre compartiment S3, vous ne pouvez pas choisir une clé multirégionale. Pour les clés gérées par le client, Security Lake crée une subvention en votre nom en envoyant une `CreateGrant` demande à AWS KMS. Les subventions AWS KMS sont utilisées pour donner à Security Lake l'accès à une KMS clé dans un compte client.

Security Lake a besoin de l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez `GenerateDataKey` des demandes AWS KMS à pour générer des clés de données chiffrées par votre clé gérée par le client.
- Envoyez vos `RetireGrant` demandes à AWS KMS. Lorsque vous mettez à jour votre lac de données, cette opération permet de retirer la subvention qui a été ajoutée à la AWS KMS clé pour ETL traitement.

Security Lake n'a pas besoin d'`Decrypt`autorisations. Lorsque les utilisateurs autorisés de la clé lisent les données de Security Lake, S3 gère le déchiffrement et les utilisateurs autorisés peuvent lire les données sous forme non cryptée. Toutefois, un abonné a besoin `Decrypt` d'autorisations pour utiliser les données sources. Pour plus d'informations sur les autorisations des abonnés, consultezGestion de l'accès aux données pour les abonnés de Security Lake.

Si vous souhaitez utiliser une KMS clé existante pour chiffrer les données de Security Lake, vous devez modifier la politique de clé associée à cette KMS clé. La politique clé doit autoriser le IAM rôle associé à l'emplacement du lac de données de Lake Formation à utiliser la KMS clé pour déchiffrer les données. Pour savoir comment modifier la politique clé d'une KMS clé, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur.

Votre KMS clé peut accepter des demandes de subvention, ce qui permet à Security Lake d'accéder à la clé, lorsque vous créez une politique clé ou que vous utilisez une politique clé existante avec les autorisations appropriées. Pour obtenir des instructions sur la création d'une politique clé, consultez la section Création d'une politique clé dans le Guide du AWS Key Management Service développeur.

Attachez la politique clé suivante à votre KMS clé :

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

IAMAutorisations requises lors de l'utilisation d'une clé gérée par le client

Consultez la section Mise en route : conditions préalables pour obtenir un aperçu des IAM rôles que vous devez créer pour utiliser Security Lake.

Lorsque vous ajoutez une source personnalisée ou un abonné, Security Lake crée IAM des rôles dans votre compte. Ces rôles sont destinés à être partagés avec d'autres IAM identités. Ils permettent à une source personnalisée d'écrire des données dans le lac de données et à un abonné de consommer les données du lac de données. Une politique AWS gérée appelée `AmazonSecurityLakePermissionsBoundary` définit les limites d'autorisation pour ces rôles.

Chiffrer les files d'attente Amazon SQS

Lorsque vous créez votre lac de données, Security Lake crée deux files d'attente Amazon Simple Queue Service (AmazonSQS) non cryptées dans le compte administrateur délégué de Security Lake. Vous devez chiffrer ces files d'attente pour protéger vos données. Le chiffrement côté serveur par défaut (SSE) fourni par Amazon Simple Queue Service n'est pas suffisant. Vous devez créer une clé gérée par le client dans AWS Key Management Service (AWS KMS) pour chiffrer les files d'attente et accorder au service Amazon S3 les autorisations principales pour travailler avec les files d'attente chiffrées. Pour obtenir des instructions sur l'octroi de ces autorisations, consultez Pourquoi

les notifications d'événements Amazon S3 ne sont-elles pas envoyées à une SQS file d'attente Amazon qui utilise le chiffrement côté serveur ? dans le AWS Knowledge Center.

Étant donné que Security Lake prend AWS Lambda en charge les tâches d'extraction, de transfert et de chargement (ETL) sur vos données, vous devez également accorder à Lambda des autorisations pour gérer les messages dans vos files d'attente AmazonSQS. Pour plus d'informations, consultez la section Autorisations relatives aux rôles d'exécution dans le Guide du AWS Lambda développeur.

Chiffrement en transit

Security Lake chiffre toutes les données en transit entre les AWS services. Security Lake protège les données en transit, lorsqu'elles sont acheminées vers et depuis le service, en chiffrant automatiquement toutes les données interréseaux à l'aide du protocole de cryptage Transport Layer Security (TLS) 1.2. Les HTTPS demandes directes envoyées au Security Lake APIs sont signées à l'aide de l'algorithme AWS Signature version 4 pour établir une connexion sécurisée.

Refus d'utiliser vos données pour améliorer le service

Vous pouvez choisir de refuser que vos données soient utilisées pour développer et améliorer Security Lake et d'autres services de AWS sécurité en utilisant la politique de AWS Organizations désinscription. Vous pouvez choisir de vous désinscrire même si Security Lake ne collecte actuellement aucune donnée de ce type. Pour plus d'informations sur la procédure de désactivation, veuillez consulter Politiques de désactivation des services IA dans le Guide de l'utilisateur AWS Organizations .

À l'heure actuelle, Security Lake ne collecte aucune des données de sécurité traitées en votre nom, ni les données de sécurité que vous téléchargez dans votre lac de données de sécurité créé par ce service. Pour développer et améliorer le service Security Lake et les fonctionnalités d'autres services de sécurité, AWS Security Lake peut collecter de telles données à l'avenir, y compris les données que vous téléchargez à partir de sources de données tierces. Nous mettrons à jour cette page lorsque Security Lake aura l'intention de collecter de telles données et décrirons comment cela fonctionnera. Vous aurez toujours la possibilité de vous désinscrire à tout moment.

> **Note**
>
> Pour que vous puissiez utiliser la politique de désinscription, vos AWS comptes doivent être gérés de manière centralisée par AWS Organizations. Si vous n'avez pas encore

créé d'organisation pour vos AWS comptes, consultez la section Création et gestion d'une organisation dans le Guide de AWS Organizations l'utilisateur.

Les effets de la désactivation sont les suivants :

- Security Lake supprimera les données collectées et stockées avant votre désinscription (le cas échéant).
- Une fois que vous vous êtes désinscrit, Security Lake ne collectera ni ne stockera ces données.

Validation de conformité pour Amazon Security Lake

Pour savoir si un programme AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation AWS services est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne AWS services sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.

- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation AWS services et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela AWS service fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela AWS service détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous AWS service permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Bonnes pratiques de sécurité pour Security Lake

Consultez les bonnes pratiques suivantes pour travailler avec Amazon Security Lake.

Accordez aux utilisateurs de Security Lake les autorisations minimales possibles

Respectez le principe du moindre privilège en accordant l'ensemble minimal d'autorisations de politique d'accès à vos utilisateurs AWS Identity and Access Management (IAM), à vos groupes d'utilisateurs et à vos rôles. Par exemple, vous pouvez autoriser un utilisateur IAM à consulter la liste des sources de journaux dans Security Lake, mais pas à créer des sources ou des abonnés. Pour de plus amples informations, consultez Exemples de politiques basées sur l'identité pour Amazon Security Lake.

Vous pouvez également l'utiliser AWS CloudTrail pour suivre l'utilisation des API dans Security Lake. CloudTrailfournit un enregistrement des actions d'API effectuées par un utilisateur, un groupe ou un rôle dans Security Lake. Pour plus d'informations, veuillez consulter Journalisation des appels d'API Amazon Security Lake à l'aide AWS CloudTrail.

Afficher la page de résumé

La page Résumé de la console Security Lake fournit une vue d'ensemble des problèmes survenus au cours des 14 derniers jours qui ont un impact sur le service Security Lake et les compartiments Amazon S3 dans lesquels vos données sont stockées. Vous pouvez approfondir ces problèmes pour vous aider à atténuer les éventuels impacts liés à la sécurité.

Intégration à Security Hub

Intégrez Security Lake et AWS Security Hub recevez les résultats du Security Hub dans Security Lake. Security Hub génère des résultats à partir de nombreuses intégrations différentes AWS services et tierces. La réception des résultats du Security Hub vous permet d'avoir une vue d'ensemble de votre niveau de conformité et de savoir si vous respectez les meilleures pratiques AWS de sécurité.

Pour plus d'informations, veuillez consulter Intégration avec AWS Security Hub.

Surveillez les événements liés à Security Lake

Vous pouvez surveiller Security Lake à l'aide CloudWatch des métriques Amazon. CloudWatchcollecte les données brutes de Security Lake chaque minute et les traite en métriques. Vous pouvez définir des alarmes qui déclenchent des notifications lorsque les métriques atteignent des seuils spécifiés.

Pour plus d'informations, veuillez consulter CloudWatchMétriques pour Amazon Security Lake.

Résilience dans Amazon Security Lake

L'infrastructure mondiale d'AWS est construite autour de zones de disponibilité et de Régions AWS. Les Régions AWSfournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Ces zones de disponibilité vous offrent un moyen efficace de concevoir et d'exploiter des applications et des bases de données. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande

capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

La disponibilité de Security Lake est liée à la disponibilité de la région. La distribution sur plusieurs zones de disponibilité permet au service de tolérer les défaillances dans chaque zone de disponibilité.

La disponibilité du plan de données Security Lake n'est liée à la disponibilité d'aucune région. Cependant, la disponibilité du plan de contrôle de Security Lake est étroitement liée à la disponibilité dans la région de l'Est des États-Unis (Virginie du Nord).

Pour plus d'informations sur les Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Outre l'infrastructure AWS mondiale, Security Lake, dans lequel les données sont soutenues par Amazon Simple Storage Service (Amazon S3), propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Configuration du cycle de vie

Une configuration du cycle de vie est un ensemble de règles qui définit des action qu'Amazon S3 applique à un groupe d'objets. Avec des règles de configuration du cycle de vie, vous pouvez indiquer à Amazon S3 de passer à des classes de stockage moins onéreuses, de les archiver ou de les supprimer. Pour plus d'informations, veuillez consulter Gestion du cycle de vie des objets dans le Guide de l'utilisateur Amazon S3.

Contrôle de version

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser le contrôle de version pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à vous remettre à la fois des actions involontaires de l'utilisateur et des défaillances d'applications. Pour plus d'informations, consultez la section Utilisation du versionnement dans les compartiments S3 dans le guide de l'utilisateur Amazon S3.

Classes de stockage

Amazon S3 offre une gamme de classes de stockage à choisir en fonction des exigences de votre charge de travail. Les classes de stockage S3 standard – Accès peu fréquent et S3 unizone – Accès peu fréquent sont conçues pour les données auxquelles vous accédez environ une fois par mois et nécessitent un accès en millisecondes. La classe de stockage S3 Glacier Instant

Retrieval est conçue pour les données d'archivage de longue durée accessibles avec un accès en millisecondes auxquelles vous accédez environ une fois par trimestre. Pour les données d'archivage qui ne nécessitent pas d'accès immédiat, telles que les sauvegardes, vous pouvez utiliser les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour plus d'informations, consultez la section Utilisation des classes de stockage Amazon S3 dans le guide de l'utilisateur Amazon S3.

Sécurité de l'infrastructure dans Amazon Security Lake

En tant que service géré, Amazon Security Lake est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez les API appels AWS publiés pour accéder à Security Lake via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Analyse de la configuration et des vulnérabilités dans Security Lake

La configuration et les contrôles informatiques sont une responsabilité partagée entre AWS et vous, notre client. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée AWS.

Surveillez Amazon.

Security s'intègre avecAWS CloudTrail, un service qui fournit un registre des actions effectuées dans Amazon, un rôle ou un autreAWS service. Cela inclut les actions depuis la console Security Lake et les appels programmatiques aux opérations de l'API Security Lake. À l'aide des informations collectées parCloudTrail, vous pouvez déterminer quelles demandes ont été adressées à Security Lake. Pour chaque demande, vous pouvez identifier le moment où elle a été faite, l'adresse IP à partir de laquelle elle a été faite, qui l'a faite, ainsi que des détails supplémentaires. Pour plus d'informations, veuillez consulter Journalisation des appels d'API Amazon Security Lake à l'aide AWS CloudTrail.

Amazon et Amazon CloudWatch étant intégrés, vous pouvez collecter, afficher et analyser des métriques pour les journaux que Amazon. CloudWatchles métriques de votre lac de données Security Lake sont automatiquement collectées et transmises CloudWatch toutes les minutes. Vous pouvez également définir une alarme qui vous envoie une notification si un seuil défini est atteint pour une métrique Amazon. Pour obtenir la liste de toutes les métriques auxquelles Security Lake envoie des donnéesCloudWatch, consultezMétriques et dimensions de Security Lake.

CloudWatchMétriques pour Amazon Security Lake

Vous pouvez surveiller Security Lake à l'aide d'AmazonCloudWatch, qui collecte les données brutes chaque minute et les transforme en métriques lisibles et disponibles presque en temps réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et mieux comprendre les données de votre data lake. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints.

Rubriques

- Métriques et dimensions de Security Lake
- Affichage CloudWatch des métriques pour Security Lake
- Configuration d'CloudWatchalarmes pour les métriques de Security Lake

Métriques et dimensions de Security Lake

L'espace de noms `AWS/SecurityLake` inclut les métriques suivantes.

Métrique	Description
`ProcessedSize`	Le volume de données provenant d'un support natif AWS services qui est actuellement stocké dans votre lac de données. Unités : octets

Les dimensions suivantes sont disponibles pour les métriques de Security Lake.

Dimension	Description
`Account`	`ProcessedSize` métrique pour une valeur spécifiqueCompte AWS. Cette dimension n'est disponible que lorsque vous affichez l'icône `Per-Account Source Version Metrics` activéeCloudWatch.
`Region`	`ProcessedSize` métrique pour une valeur spécifiqueRégion AWS.
`Source`	`ProcessedSize` métrique pour une source de AWS journal spécifique.
`SourceVersion`	`ProcessedSize` métrique pour une version spécifique d'une source de AWS journal.

Vous pouvez consulter les statistiques pour des comptes spécifiques Comptes AWS (`Per-Account Source Version Metrics`) ou pour tous les comptes d'une organisation (`Per-Source Version Metrics`).

Affichage CloudWatch des métriques pour Security Lake

Vous pouvez surveiller les métriques pour Security Lake à l'aide de la CloudWatch console, CloudWatch de l'interface de ligne de commande (CLI) CLI) CLI) CLI) par programmation à l'aide de l'API. CloudWatch Choisissez votre méthode préférée et suivez les étapes pour accéder aux métriques de Security Lake.

CloudWatch console

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, choisissez Métriques, toutes les métriques.
3. Dans l'onglet Parcourir, choisissez Security Lake.
4. Choisissez Mesures de version source par compte ou Mesures de version source par compte.
5. Sélectionnez une métrique pour l'afficher en détail. Vous pouvez également choisir d'effectuer les opérations suivantes :

   - Pour trier les métriques, utilisez l'en-tête de colonne.
   - Pour représenter graphiquement une métrique, sélectionnez le nom de la métrique, puis une option de représentation graphique.
   - Pour filtrer par métrique, sélectionnez le nom de la métrique, puis Add to search.

CloudWatch API

Pour accéder aux métriques de Security Lake à l'aide de l'CloudWatchAPI, utilisez l'`GetMetricStatistics`action.

AWS CLI

Pour accéder aux métriques de Security Lake à l'aide deAWS CLI, exécutez la `get-metric-statistics`commande.

Pour plus d'informations sur la surveillance à l'aide de métriques, consultez la section Utiliser CloudWatch les métriques Amazon dans le Guide de CloudWatch l'utilisateur Amazon.

Configuration d'CloudWatchalarmes pour les métriques de Security Lake

CloudWatch vous permet également de définir des alarmes lorsqu'un seuil est atteint pour une métrique. Par exemple, vous pouvez définir une alarme pour la ProcessedSizemétrique afin d'être averti lorsque le volume de données provenant d'une source spécifique dépasse un seuil spécifique.

Pour obtenir des instructions sur la configuration des alarmes, consultez la section Utilisation des CloudWatch alarmes Amazon dans le Guide de CloudWatch l'utilisateur Amazon.

Journalisation des appels d'API Amazon Security Lake à l'aide AWS CloudTrail

Amazon Security Lake s'intègre AWS CloudTrail à un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Security Lake. CloudTrailcapture les appels d'API pour Security Lake sous forme d'événements. Les appels capturés incluent des appels provenant de la console Security Lake et des appels de code vers les opérations de l'API Security Lake. Si vous créez un journal, vous pouvez activer la diffusion continue d'CloudTrailévénements vers un compartiment Amazon S3, y compris des événements pour Security Lake. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. À l'aide des informations collectées parCloudTrail, vous pouvez déterminer la demande qui a été faite à Security Lake, l'adresse IP à partir de laquelle la demande a été faite, qui l'a faite, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus sur CloudTrail, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Informations sur Security Lake dans CloudTrail

CloudTrail est activé sur votre Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Security Lake, elle est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements enregistrés dans votre compteCompte AWS, y compris des événements liés à Security Lake, créez un historique. Un journal permet CloudTrail de transmettre les événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité

- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Les actions de Security Lake sont enregistrées CloudTrail et documentées dans la référence de l'API Security Lake. Par exemple, les appels adressés aux actions `UpdateDataLake` `ListLogSources`, `CreateSubscriber` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter Élément CloudTrail userIdentity.

Comprendre les entrées du fichier journal de Security Lake

Les fichiers journaux CloudTrail contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de CloudTrail journal pour l'`GetSubscriber`action 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"
}
```

Marquage des ressources d'Amazon Security Lake

Une balise est une étiquette facultative que vous pouvez définir et attribuer aux AWS ressources, notamment à certains types de ressources Amazon Security Lake. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Par exemple, vous pouvez utiliser des balises pour appliquer des politiques, répartir les coûts, distinguer les ressources ou identifier les ressources qui répondent à certaines exigences de conformité ou à certains flux de travail.

Vous pouvez attribuer des balises aux types de ressources Security Lake suivants : les abonnés et la configuration du lac de données pour votre Compte AWS compte individuel Régions AWS.

Rubriques

Principes fondamentaux du balisage

Une ressource peut avoir jusqu'à 50 balises. Chaque balise est constituée d'une clé de balise obligatoire et d'une valeur de balise facultative que vous définissez. Une clé de balise est une étiquette générale qui fait office de catégorie pour une valeur de balise plus spécifique. Une valeur de balise tient lieu de descripteur pour une clé de balise.

Par exemple, si vous ajoutez des abonnés pour analyser les données de sécurité provenant de différents environnements (un ensemble d'abonnés pour les données dans le cloud et un autre pour les données locales), vous pouvez attribuer une clé de `Environment` balise à ces abonnés. La valeur de balise associée peut être `Cloud` destinée aux abonnés qui analysent les données provenant de AWS services et `On-Premises` pour les autres.

Lorsque vous définissez et attribuez des balises aux ressources Amazon Security Lake, gardez les points suivants à l'esprit :

- Chaque ressource peut avoir un maximum de 50 balises.
- Pour chaque ressource, chaque clé de balise doit être unique et ne peut avoir qu'une seule valeur de balise.
- Les clés et valeurs de balise sont sensibles à la casse. À titre de bonne pratique, nous vous recommandons de définir une stratégie de capitalisation des balises et de mettre en œuvre cette stratégie de manière cohérente dans l'ensemble de vos ressources.
- Une clé de balise peut comporter au maximum 128 caractères UTF-8. La valeur d'une balise peut comporter au maximum 256 caractères UTF-8. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @
- Le `aws:` préfixe est réservé à l'usage de AWS. Vous ne pouvez pas l'utiliser dans les clés ou les valeurs de balise que vous définissez. En outre, vous ne pouvez pas modifier ou supprimer les clés de balise ou les valeurs qui utilisent ce préfixe. Les balises qui utilisent ce préfixe ne sont pas comptabilisées dans le quota de 50 balises par ressource.
- Tous les tags que vous attribuez ne sont disponibles que pour vous Compte AWS et uniquement dans le pays Région AWS dans lequel vous les attribuez.
- Si vous attribuez des balises à une ressource à l'aide de Security Lake, les balises ne sont appliquées qu'à la ressource stockée directement dans Security Lake dans le cas applicable Région AWS. Ils ne s'appliquent à aucune ressource de support associée que Security Lake crée, utilise ou gère pour vous dans d'autres domaines AWS services. Par exemple, si vous attribuez des balises à votre lac de données, les balises ne sont appliquées qu'à la configuration de votre lac de données dans Security Lake pour la région spécifiée. Ils ne sont pas appliqués au compartiment Amazon Simple Storage Service (Amazon S3) qui stocke les données de votre journal et de vos événements. Pour attribuer également des balises à une ressource associée, vous pouvez utiliser AWS Resource Groups ou AWS service celle qui stocke la ressource, par exemple Amazon S3 pour un compartiment S3. L'attribution de balises aux ressources associées peut vous aider à identifier les ressources de support pour votre lac de données.
- Si vous supprimez une ressource, toutes les balises qui lui sont attribuées sont également supprimées.

Pour obtenir des restrictions supplémentaires, des conseils et des meilleures pratiques, consultez la section Marquage de vos AWS ressources dans le Guide de l'utilisateur AWS des ressources de balisage.

> **Important**
>
> Ne stockez pas de données confidentielles ou d'autres types de données sensibles dans des balises. Les tags sont accessibles depuis de nombreuses personnes AWS services, notamment AWS Billing and Cost Management. Ils ne sont pas destinés à être utilisés pour des données sensibles.

Pour ajouter et gérer des balises pour les ressources de Security Lake, vous pouvez utiliser la console Security Lake ou l'API Security Lake.

Utilisation de balises dans les politiques IAM

Une fois que vous avez commencé à baliser les ressources, vous pouvez définir des autorisations basées sur des balises au niveau des ressources dans les politiques AWS Identity and Access Management (IAM). En utilisant les balises de cette manière, vous pouvez mettre en œuvre un contrôle granulaire des utilisateurs et des rôles autorisés à créer et à étiqueter des ressources, et des utilisateurs et rôles autorisés à ajouter, modifier et supprimer des balises de manière plus générale. Compte AWS Pour contrôler l'accès en fonction des balises, vous pouvez utiliser les clés de condition associées aux balises dans l'élément Condition des politiques IAM.

Par exemple, vous pouvez créer une politique qui permet à un utilisateur d'avoir un accès complet à toutes les ressources Amazon Security Lake, si le `Owner` tag de la ressource indique son nom d'utilisateur :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Si vous définissez des autorisations au niveau des ressources basées sur des balises, les autorisations prennent effet immédiatement. Vos ressources sont ainsi plus sécurisées dès leur création et vous pouvez rapidement commencer à appliquer l'utilisation des balises pour les nouvelles ressources. Vous pouvez également utiliser des autorisations au niveau des ressources afin de contrôler les clés et les valeurs de balise qui peuvent être associés à des ressources nouvelles et existantes. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises dans le guide de l'utilisateur IAM.

Ajouter des balises aux ressources Amazon Security Lake

Pour ajouter des balises à une ressource Amazon Security Lake, vous pouvez utiliser la console Security Lake ou l'API Security Lake.

> **Important**
>
> L'ajout de balises à une ressource peut affecter l'accès à celle-ci. Avant d'ajouter une balise à une ressource, passez en revue les politiques AWS Identity and Access Management (IAM) susceptibles d'utiliser des balises pour contrôler l'accès aux ressources.

Console

Lorsque vous activez Security Lake pour un abonné Région AWS ou que vous en créez un, la console Security Lake propose des options permettant d'ajouter des balises à la ressource, qu'il s'agisse de la configuration du lac de données pour la région ou pour l'abonné. Suivez les instructions de la console pour ajouter des balises à la ressource lors de sa création.

Pour ajouter une ou plusieurs balises à une ressource existante à l'aide de la console Security Lake, procédez comme suit.

Ajout d'une balise à une ressource

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Selon le type de ressource auquel vous souhaitez ajouter une balise, effectuez l'une des opérations suivantes :

   - Pour une configuration de lac de données, choisissez Regions dans le volet de navigation. Ensuite, dans le tableau Régions, sélectionnez la Région.

- Pour un abonné, choisissez Subscribers dans le volet de navigation. Ensuite, dans le tableau Mes abonnés, sélectionnez l'abonné.

  Si l'abonné n'apparaît pas dans le tableau, utilisez le Région AWS sélecteur dans le coin supérieur droit de la page pour sélectionner la région dans laquelle vous l'avez créé. Le tableau répertorie les abonnés existants uniquement pour la région actuelle.

3. Choisissez Modifier.
4. Développez la section identification. Cette section répertorie toutes les balises actuellement attribuées à la ressource.
5. Dans la section Balises, choisissez Ajouter une balise.
6. Dans le champ Clé, entrez la clé de balise pour la balise à ajouter à la ressource. Ensuite, dans le champ Valeur, entrez éventuellement une valeur de balise pour la clé.

   Une clé de balise peut contenir jusqu'à 128 caractères. Une valeur de balise peut contenir jusqu'à 256 caractères. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @
7. Pour ajouter une autre balise à la ressource, choisissez Ajouter une nouvelle balise, puis répétez l'étape précédente. Vous pouvez attribuer jusqu'à 50 balises à une ressource.
8. Lorsque vous avez fini d'ajouter des balises, choisissez Enregistrer.

API

Pour créer une ressource et y ajouter une ou plusieurs balises par programmation, utilisez l'`Create`opération appropriée au type de ressource que vous souhaitez créer :

- Configuration du lac de données : utilisez l'CreateDataLakeopération ou, si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la create-data-lakecommande.
- Abonné : utilisez l'CreateSubscriberopération ou, si vous utilisez le AWS CLI, exécutez la commande create-subscriber.

Dans votre demande, utilisez le `tags` paramètre pour spécifier la clé de balise (`key`) et la valeur de balise facultative (`value`) pour chaque balise à ajouter à la ressource. Le `tags` paramètre spécifie un tableau d'objets. Chaque objet spécifie une clé de balise et la valeur de balise associée.

Pour ajouter une ou plusieurs balises à une ressource existante, utilisez TagResourcel'API Security Lake ou, si vous utilisez la AWS CLI, exécutez la commande tag-resource. Dans votre demande, spécifiez le Amazon Resource Name (ARN) de la ressource à laquelle vous souhaitez ajouter une balise. Utilisez le `tags` paramètre pour spécifier la clé de balise (`key`) et la valeur de balise facultative (`value`) pour chaque balise à ajouter. Comme c'est le cas pour les `Create` opérations et les commandes, le `tags` paramètre spécifie un tableau d'objets, un objet pour chaque clé de balise et sa valeur de balise associée.

Par exemple, la AWS CLI commande suivante ajoute une clé de `Environment` balise avec une valeur de `Cloud` balise à l'abonné spécifié. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

Où :

- `resource-arn`spécifie l'ARN de l'abonné auquel ajouter un tag.
- *`Environment`*est la clé du tag à ajouter à l'abonné.
- *`Cloud`*est la valeur de balise pour la clé de balise spécifiée (*`Environment`*).

Dans l'exemple suivant, la commande ajoute plusieurs balises à l'abonné.

```
$ 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
```

Pour chaque objet d'un `tags` tableau, les `value` arguments `key` et sont obligatoires. Toutefois, la valeur de l'`value`argument peut être une chaîne vide. Si vous ne souhaitez pas associer une valeur de balise à une clé de balise, ne spécifiez pas de valeur pour l'`value`argument. Par exemple, la commande suivante ajoute une clé de `Owner` balise sans valeur de balise associée :

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
--tags key=Owner,value=
```

Si une opération de balisage réussit, Security Lake renvoie une réponse HTTP 200 vide. Sinon, Security Lake renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Révision des balises pour les ressources Amazon Security Lake

Vous pouvez consulter les balises (clés de balise et valeurs de balise) d'une ressource Amazon Security Lake à l'aide de la console Security Lake ou de l'API Security Lake.

Console

Procédez comme suit pour consulter les balises d'une ressource à l'aide de la console Security Lake.

Pour consulter les balises d'une ressource

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Selon le type de ressource dont vous souhaitez vérifier les balises, effectuez l'une des opérations suivantes :

   - Pour une configuration de lac de données, choisissez Regions dans le volet de navigation. Dans le tableau Régions, sélectionnez la région, puis choisissez Modifier. Développez ensuite la section Tags.
   - Pour un abonné, choisissez Subscribers dans le volet de navigation. Ensuite, dans le tableau Mes abonnés, choisissez le nom de l'abonné.

     Si l'abonné n'apparaît pas dans le tableau, utilisez le Région AWS sélecteur dans le coin supérieur droit de la page pour sélectionner la région dans laquelle vous l'avez créé. Le tableau répertorie les abonnés existants uniquement pour la région actuelle.

La section Balises répertorie toutes les balises actuellement attribuées à la ressource.

API

Pour récupérer et examiner les balises d'une ressource existante par programmation, utilisez le ListTagsForResourcefonctionnement de l'API Security Lake. Dans votre demande, utilisez le `resourceArn` paramètre pour spécifier le nom de ressource Amazon (ARN) de la ressource.

Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la list-tags-for-resourcecommande et utilisez le `resource-arn` paramètre pour spécifier l'ARN de la ressource. Par exemple :

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

Dans l'exemple précédent, *arn:aws:securitylake:us-east-*1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab est l'ARN d'un abonné existant.

Si l'opération aboutit, Security Lake renvoie un `tags` tableau. Chaque objet du tableau spécifie une balise (clé de balise et valeur de balise) actuellement attribuée à la ressource. Par exemple :

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Où `Environment``CostCenter`, et `Owner` sont les clés de balise attribuées à la ressource. `Cloud`est la valeur de balise associée à la clé de `Environment` balise. `12345`est la valeur de balise associée à la clé de `CostCenter` balise. Aucune valeur de `Owner` balise n'est associée à la clé de balise.

Modification des balises pour les ressources Amazon Security Lake

Pour modifier les balises (clés de balise ou valeurs de balise) d'une ressource Amazon Security Lake, vous pouvez utiliser la console Security Lake ou l'API Security Lake.

> **Important**
>
> La modification des balises d'une ressource peut avoir une incidence sur l'accès à cette ressource. Avant de modifier une clé ou une valeur de balise pour une ressource, passez en revue les politiques AWS Identity and Access Management (IAM) susceptibles d'utiliser la balise pour contrôler l'accès aux ressources.

Console

Procédez comme suit pour modifier les balises d'une ressource à l'aide de la console Security Lake.

Pour modifier les balises d'une ressource

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Selon le type de ressource dont vous souhaitez modifier les balises, effectuez l'une des opérations suivantes :

   - Pour une configuration de lac de données, choisissez Regions dans le volet de navigation. Ensuite, dans le tableau Régions, sélectionnez la Région.
   - Pour un abonné, choisissez Subscribers dans le volet de navigation. Ensuite, dans le tableau Mes abonnés, sélectionnez l'abonné.

     Si l'abonné n'apparaît pas dans le tableau, utilisez le Région AWS sélecteur dans le coin supérieur droit de la page pour sélectionner la région dans laquelle vous l'avez créé. Le tableau répertorie les abonnés existants uniquement pour la région actuelle.
3. Choisissez Modifier.
4. Développez la section identification. La section Balises répertorie toutes les balises actuellement attribuées à la ressource.
5. Effectuez l'une des actions suivantes :

   - Pour ajouter une valeur de balise à une clé de balise existante, entrez la valeur dans le champ Valeur à côté de la clé de balise.
   - Pour modifier une clé de balise existante, choisissez Supprimer à côté de la balise. Choisissez ensuite Ajouter une nouvelle étiquette. Dans le champ Clé qui apparaît, entrez la nouvelle clé de balise. Entrez éventuellement une valeur de balise associée dans le champ Valeur.

- Pour modifier la valeur d'une balise existante, choisissez X dans la zone Valeur qui contient la valeur. Entrez ensuite la nouvelle valeur de balise dans le champ Valeur.
- Pour supprimer une valeur de balise existante, choisissez X dans la zone Valeur qui contient la valeur.
- Pour supprimer une balise existante (clé et valeur de balise), choisissez Supprimer à côté de la balise.

Une ressource peut avoir jusqu'à 50 balises. Une clé de balise peut contenir jusqu'à 128 caractères. Une valeur de balise peut contenir jusqu'à 256 caractères. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @

6. Lorsque vous avez terminé de modifier les balises, choisissez Enregistrer.

API

Lorsque vous modifiez une balise pour une ressource par programmation, vous remplacez la balise existante par de nouvelles valeurs. Par conséquent, la meilleure façon de modifier une balise dépend de la modification d'une clé de balise, d'une valeur de balise ou des deux. Pour modifier une clé de balise, supprimez la balise actuelle et ajoutez-en une nouvelle.

Pour modifier ou supprimer uniquement la valeur de balise associée à une clé de balise, remplacez la valeur existante à l'aide TagResourcede l'API Security Lake. Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande tag-resource. Dans votre demande, spécifiez le Amazon Resource Name (ARN) de la ressource dont vous souhaitez modifier ou supprimer la valeur de balise.

Pour modifier la valeur d'une balise, utilisez le `tags` paramètre pour spécifier la clé de balise dont vous souhaitez modifier la valeur de balise. Spécifiez également la nouvelle valeur de balise pour la clé. Par exemple, la AWS CLI commande suivante modifie la valeur de balise de `Cloud` à `On-Premises` pour la clé de `Environment` balise attribuée à l'abonné spécifié. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ 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
```

Où :

- `resource-arn`spécifie l'ARN de l'abonné.
- *`Environment`*est la clé de balise associée à la valeur de balise à modifier.
- *`On-Premises`*est la nouvelle valeur de balise pour la clé de balise spécifiée (*`Environment`*).

Pour supprimer une valeur de balise d'une clé de balise, ne spécifiez pas de valeur pour l'`value`argument de la clé dans le `tags` paramètre. Par exemple :

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

Si l'opération réussit, Security Lake renvoie une réponse HTTP 200 vide. Sinon, Security Lake renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Supprimer les balises des ressources Amazon Security Lake

Pour supprimer des balises d'une ressource Amazon Security Lake, vous pouvez utiliser la console Security Lake ou l'API Security Lake.

> **Important**
>
> La suppression de balises d'une ressource peut affecter l'accès à cette ressource. Avant de supprimer un tag, passez en revue les politiques AWS Identity and Access Management (IAM) susceptibles d'utiliser le tag pour contrôler l'accès aux ressources.

Console

Procédez comme suit pour supprimer une ou plusieurs balises d'une ressource à l'aide de la console Security Lake.

Pour supprimer un tag d'une ressource

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.

2. Selon le type de ressource dont vous souhaitez supprimer une balise, effectuez l'une des opérations suivantes :

   - Pour une configuration de lac de données, choisissez Regions dans le volet de navigation. Ensuite, dans le tableau Régions, sélectionnez la Région.
   - Pour un abonné, choisissez Subscribers dans le volet de navigation. Ensuite, dans le tableau Mes abonnés, sélectionnez l'abonné.

     Si l'abonné n'apparaît pas dans le tableau, utilisez le Région AWS sélecteur dans le coin supérieur droit de la page pour sélectionner la région dans laquelle vous l'avez créé. Le tableau répertorie les abonnés existants uniquement pour la région actuelle.
3. Choisissez Modifier.
4. Développez la section identification. La section Balises répertorie toutes les balises actuellement attribuées à la ressource.
5. Effectuez l'une des actions suivantes :

   - Pour supprimer uniquement la valeur de balise d'une balise, choisissez X dans la zone Valeur qui contient la valeur à supprimer.
   - Pour supprimer à la fois la clé de balise et la valeur de balise (par paire) d'une balise, choisissez Supprimer à côté de la balise à supprimer.
6. Pour supprimer des balises supplémentaires de la ressource, répétez l'étape précédente pour chaque balise supplémentaire à supprimer.
7. Lorsque vous avez fini de supprimer les balises, choisissez Enregistrer.

API

Pour supprimer une ou plusieurs balises d'une ressource par programmation, utilisez le UntagResourcefonctionnement de l'API Security Lake. Dans votre demande, utilisez le `resourceArn` paramètre pour spécifier le nom de ressource Amazon (ARN) de la ressource dont vous souhaitez supprimer une balise. Utilisez le `tagKeys` paramètre pour spécifier la clé de balise de la balise à supprimer. Pour supprimer plusieurs balises, ajoutez le `tagKeys` paramètre et l'argument de chaque balise à supprimer, séparés par une esperluette (&), par exemple,. `tagKeys=key1&tagKeys=key2` Pour supprimer uniquement une valeur de balise spécifique (et non une clé de balise) d'une ressource, modifiez la balise au lieu de la supprimer.

Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande untag-resource pour supprimer une ou plusieurs balises d'une ressource. Pour le `resource-arn`

paramètre, spécifiez l'ARN de la ressource dont vous souhaitez supprimer une balise. Utilisez le `tag-keys` paramètre pour spécifier la clé de balise de la balise à supprimer. Par exemple, la commande suivante supprime le `Environment` tag (à la fois la clé du tag et la valeur du tag) de l'abonné spécifié :

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

Where `resource-arn` indique l'ARN de l'abonné dont le tag doit être supprimé, et *`Environment`* représente la clé du tag à supprimer.

Pour supprimer plusieurs balises d'une ressource, ajoutez chaque clé de balise supplémentaire en tant qu'argument pour le `tag-keys` paramètre. Par exemple :

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

Si l'opération réussit, Security Lake renvoie une réponse HTTP 200 vide. Sinon, Security Lake renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Résolution des problèmes liés à Amazon Security Lake

Consultez les rubriques suivantes si vous rencontrez des problèmes lors de l'utilisation de Security Lake.

Résolution des problèmes liés à l'état des lacs

La page Problèmes de la console Security Lake présente un résumé des problèmes affectant votre lac de données. Par exemple, Security Lake ne peut pas activer la collecte de journaux pour les événements de AWS CloudTrail gestion si vous n'avez pas créé CloudTrail de suivi pour votre organisation. La page Problèmes couvre les problèmes survenus au cours des 14 derniers jours. Vous pouvez consulter une description de chaque problème et les étapes de résolution suggérées.

Pour accéder par programmation à un résumé des problèmes, vous pouvez utiliser le ListDataLakeExceptionsfonctionnement du Security Lake. API Si vous utilisez le AWS CLI, exécutez la list-data-lake-exceptionscommande. Pour le `regions` paramètre, vous pouvez spécifier un ou plusieurs codes de région, par exemple pour la région de l'est des États-Unis (Virginie du Nord), `us-east-1` afin de connaître les problèmes affectant ces régions. Si vous n'incluez pas le `regions` paramètre, des problèmes affectant toutes les régions sont renvoyés. Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.

Par exemple, la AWS CLI commande suivante répertorie les problèmes qui affectent les `eu-west-3` régions `us-east-1` et. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securitylake list-data-lake-exceptions \
--regions "us-east-1" "eu-west-3"
```

Pour informer un utilisateur de Security Lake d'un problème ou d'une erreur, utilisez le CreateDataLakeExceptionSubscriptionfonctionnement du Security LakeAPI. L'utilisateur peut être averti par e-mail, par livraison vers une file d'attente Amazon Simple Queue Service (AmazonSQS), par livraison vers une AWS Lambda fonction ou par un autre protocole pris en charge.

Par exemple, la AWS CLI commande suivante envoie des notifications relatives aux exceptions de Security Lake au compte spécifié par SMS livraison. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securitylake create-data-lake-exception-subscription \
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

Pour afficher les détails d'un abonnement exceptionnel, vous pouvez utiliser l'GetDataLakeExceptionSubscriptionopération. Pour mettre à jour un abonnement exceptionnel, vous pouvez utiliser cette UpdateDataLakeExceptionSubscriptionopération. Pour supprimer un abonnement exceptionnel et arrêter les notifications, vous pouvez utiliser cette DeleteDataLakeExceptionSubscriptionopération.

Résolution des problèmes liés à Lake Formation

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Security Lake, de AWS Lake Formation bases de données ou de tables. Pour plus d'informations sur la résolution des problèmes liés à Lake Formation, consultez la section Dépannage du Guide du AWS Lake Formation développeur.

Table introuvable

Ce message d'erreur peut s'afficher lorsque vous tentez de créer un abonné.

Pour résoudre cette erreur, assurez-vous d'avoir déjà ajouté des sources dans la région. Si vous avez ajouté des sources alors que le service Security Lake était en version préliminaire, vous devez les ajouter à nouveau avant de créer un abonné. Pour plus d'informations sur l'ajout de sources, consultezgestion des sources dans Amazon Security Security Security Security Security Security Security Security.

400 AccessDenied

Cette erreur peut s'afficher lorsque vous ajoutez une source personnalisée et que vous appelez le `CreateCustomLogSource`API.

Pour résoudre l'erreur, vérifiez vos autorisations relatives à Lake Formation. Le IAM rôle qui appelle le API doit disposer des autorisations de création de table pour la base de données Security Lake. Pour plus d'informations, consultez la section Octroi d'autorisations de base de données à l'aide de la console Lake Formation et de la méthode de ressource nommée dans le Guide du AWS Lake Formation développeur.

SYNTAX_ ERROR : ligne 1:8 SELECT :* non autorisée à partir d'une relation qui n'a pas de colonnes

Cette erreur peut s'afficher lorsque vous interrogez une table source pour la première fois dans Lake Formation.

Pour résoudre l'erreur, accordez `SELECT` l'autorisation au IAM rôle que vous utilisez lorsque vous êtes connecté à votre Compte AWS. Pour savoir comment accorder une `SELECT` autorisation, consultez la section Octroi d'autorisations de table à l'aide de la console Lake Formation et de la méthode de ressource nommée dans le Guide du AWS Lake Formation développeur.

Security Lake n'a pas réussi à ajouter le principal de l'appelant ARN à l'administrateur du lac de données de Lake Formation. Les administrateurs actuels des lacs de données peuvent inclure des principes non valides qui n'existent plus.

Cette erreur peut s'afficher lors de l'activation de Security Lake ou de l'ajout AWS service d'une source de journal.

Pour résoudre l'erreur, procédez comme suit :

1. Ouvrez la console Lake Formation à l'adresse https://console.aws.amazon.com/lakeformation/.
2. Connectez-vous en tant qu'utilisateur administratif.
3. Dans le volet de navigation, sous Autorisations, sélectionnez Rôles et tâches administratifs.
4. Dans la section Administrateurs du lac de données, choisissez Choisir les administrateurs.
5. Effacez les principes marqués « Non trouvé dans »IAM, puis choisissez Enregistrer.
6. Réessayez l'opération Security Lake.

Security Lake CreateSubscriber with Lake Formation n'a pas créé de nouvelle invitation à partager RAM des ressources à accepter

Cette erreur peut s'afficher si vous avez partagé des ressources avec le partage de données entre comptes de Lake Formation version 2 ou 3 avant de créer un abonné Lake Formation dans Security Lake. Cela est dû au fait que le partage entre comptes des versions 2 et 3 de Lake Formation optimise le nombre de partages de AWS RAM ressources en mappant plusieurs autorisations entre comptes avec un seul AWS RAM partage de ressources.

Assurez-vous que le nom du partage de ressources possède l'ID externe que vous avez spécifié lors de la création de l'abonné et que le partage de ressources ARN correspond à celui indiqué ARN dans la `CreateSubscriber` réponse.

Résolution des problèmes liés aux requêtes dans Amazon Athena

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous utilisez Athena pour interroger des objets stockés dans votre compartiment Security Lake S3. Pour plus d'informations sur la résolution des problèmes liés à Athena, consultez la section Résolution des problèmes liés à Athena du Guide de l'utilisateur d'Amazon Athena.

L'interrogation ne renvoie pas de nouveaux objets dans le lac de données

Votre requête Athena peut ne pas renvoyer de nouveaux objets dans votre lac de données, même si le compartiment S3 pour Security Lake contient ces objets. Cela peut se produire si vous avez désactivé Security Lake puis l'avez réactivé. Par conséquent, les AWS Glue partitions risquent de ne pas enregistrer correctement les nouveaux objets.

Pour résoudre l'erreur, procédez comme suit :

1. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans la barre de navigation, dans le sélecteur de régions, choisissez la région dans laquelle Security Lake est activé mais où la requête Athena ne renvoie aucun résultat.
3. Dans le volet de navigation, choisissez Functions, puis sélectionnez la fonction dans la liste suivante en fonction de la version source :

   - `Source version 1 (OCSF 1.0.0-rc.2)` — SecurityLake _Glue_Partition_Updater_Lambda_***#region>***fonction.
   - `Source version 2 (OCSF 1.1.0)` – AmazonSecurityLakeMetastoreManager_***#region>***fonction.
4. Dans l'onglet Configurations, sélectionnez Déclencheurs.
5. Sélectionnez l'option située à côté de la fonction, puis choisissez Modifier.
6. Sélectionnez Activer le déclencheur, puis cliquez sur Enregistrer. Cela fera passer l'état de la fonction à Activé.

Impossible d'accéder aux AWS Glue tables

Un abonné ayant accès aux requêtes peut ne pas être en mesure d'accéder aux AWS Glue tables contenant les données de Security Lake.

Tout d'abord, assurez-vous d'avoir suivi les étapes décrites dansConfiguration du partage de tables entre comptes (étape réservée aux abonnés).

Si l'abonné n'y a toujours pas accès, procédez comme suit :

1. Ouvrez la AWS Glue console à l'adresse https://console.aws.amazon.com/glue/.
2. Dans le volet de navigation, choisissez le catalogue de données et les paramètres du catalogue.
3. Autorisez l'abonné à accéder aux AWS Glue tables avec une politique basée sur les ressources. Pour plus d'informations sur la création de politiques basées sur les ressources, consultez les exemples de politiques basées sur les ressources AWS Glue dans le Guide du développeur.AWS Glue

Résolution des problèmes liés aux Organisations

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Security Lake et AWS Organizations. Pour plus d'informations sur le dépannage des Organisations, consultez la section Dépannage du Guide de AWS Organizations l'utilisateur.

Une erreur de refus d'accès s'est produite lors de l'appel de l' CreateDataLake opération : votre compte doit être le compte d'administrateur délégué d'une organisation ou un compte autonome.

Cette erreur peut s'afficher si vous supprimez l'organisation à laquelle appartenait un compte d'administrateur délégué, puis si vous essayez d'utiliser ce compte pour configurer Security Lake à l'aide de la console Security Lake ou du CreateDataLakeAPI.

Pour résoudre l'erreur, utilisez un compte d'administrateur délégué d'une autre organisation ou un compte autonome.

Résolution des problèmes d'identité et d'accès à Amazon Security Lake

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Security Lake etIAM.

Je ne suis pas autorisé à effectuer une action dans Security Lake

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations d'identification.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour afficher les détails d'une fiction *`subscriber`* mais ne dispose pas `SecurityLake:`*`GetSubscriber`* des autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder aux *`subscriber`* informations à l'aide de l'`SecurityLake:`*`GetSubscriber`*action.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Security Lake.

Certains vous AWS services permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Security Lake. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources de Security Lake

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Security Lake prend en charge ces fonctionnalités, consultezComment fonctionne Amazon Security Lake avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Comment est déterminée la tarification de Security Lake

La tarification d'Amazon Security Lake repose sur deux dimensions : l'ingestion et la conversion des données. Security Lake travaille également avec d'autres acteurs AWS services pour stocker et partager vos données, et ces activités peuvent entraîner des frais distincts.

Lorsque vous activez la collecte de journaux pour la première fois Compte AWS dans un compte compatible avec Security Lake, ce compte est automatiquement inscrit à un essai gratuit de 15 jours de Security Lake. Région AWS Il se peut que vous deviez encore payer des frais liés à d'autres services pendant l'essai gratuit.

Pour comprendre la méthodologie qui sous-tend la tarification de Security Lake, regardez la vidéo suivante : Tarification d'Amazon Security Lake -->

Ingestion de données

Ces coûts découlent du volume de journaux ingérés et d'autres AWS CloudTrail AWS service journaux et événements (journaux de requêtes du résolveur Amazon Route 53, AWS Security Hub résultats et journaux Amazon VPC Flow).

Conversion des données

Ces coûts découlent du volume de AWS service journaux et d'événements que Security Lake normalise en Cadre de schéma de cybersécurité ouvert (OCSF) schéma et convertit au format Apache Parquet.

Coûts des services connexes

Voici certains des coûts que vous pourriez encourir AWS services pour stocker et partager les données dans votre lac de données de sécurité :

- Amazon S3 — Ces coûts sont liés à la gestion des compartiments Amazon S3 dans votre compte Security Lake, au stockage de vos données dans celui-ci, ainsi qu'à l'évaluation et à la surveillance de votre compartiment pour des raisons de sécurité et de contrôle d'accès. Pour plus d'informations, consultez Tarification Amazon S3.
- Amazon SQS — Ces coûts sont liés à la création d'une SQS file d'attente Amazon pour la livraison des messages. Pour plus d'informations, consultez les SQStarifs Amazon.

- Amazon EventBridge — Ces coûts découlent de l' EventBridge envoi par Amazon de notifications d'objets aux points de terminaison d'abonnement. Pour plus d'informations, consultez les EventBridgetarifs Amazon.

Les coûts encourus par un abonné en interrogeant des données auprès de Security Lake et en stockant les résultats des requêtes sont à la charge de l'abonné.

Pour une liste complète des services auxiliaires, consultez la section Tarification de Security Lake.

Examen de l'utilisation de Security Lake et des coûts estimés

La page Utilisation de la console Amazon Security Lake vous permet de consulter votre utilisation actuelle de Security Lake, ainsi que l'utilisation future et les estimations de coûts. Si vous participez actuellement à un essai gratuit de 15 jours, votre utilisation pendant la période d'essai peut vous aider à estimer les coûts liés à l'utilisation de Security Lake après la fin de votre essai gratuit. Pour un aperçu de la tarification de Security Lake, consultezComment est déterminée la tarification de Security Lake. Pour obtenir des informations détaillées et des exemples de coûts, consultez la section Tarification d'Amazon Security Lake.

Dans Security Lake, les coûts d'utilisation estimés sont indiqués en dollars américains et s'appliquent uniquement aux coûts actuels Région AWS. Les coûts couvrent l'utilisation de Security Lake par tous les comptes de votre organisation et incluent la conversion vers l'Open Cybersecurity Schema Framework (OCSF) et le format Apache Parquet. Toutefois, les coûts prévus n'incluent pas les coûts des autres services avec lesquels Security Lake travaille, tels qu'Amazon Simple Storage Service (Amazon S3 AWS Glue) et.

Sur la page Utilisation, vous choisissez une période pour laquelle vous souhaitez consulter les données d'utilisation et de coûts. La période par défaut est le dernier jour calendaire. Vous devez avoir utilisé Security Lake pendant au moins un jour pour voir les prévisions de coûts.

Le haut de la page indique le coût prévu pour tous les comptes. Il s'agit de votre estimation du coût actuel de Security Lake Région AWS pour les 30 prochains jours calendaires sur la base de votre utilisation réelle pendant la période sélectionnée. L'utilisation réelle et le coût prévu reflètent tous les comptes de votre organisation.

Dans le reste de la page, les données relatives à l'utilisation et aux coûts sont réparties dans les deux tableaux suivants :

- Utilisation et coût par source : il s'agit de votre utilisation actuelle de Security Lake ventilée par source de données, ainsi que de l'utilisation et des coûts estimés pour les 30 prochains jours calendaires sur la base de votre utilisation réelle pendant la période sélectionnée. L'utilisation réelle, l'utilisation prévue et le coût prévu reflètent tous les comptes de votre organisation. Si vous sélectionnez une source, un panneau séparé s'ouvre et indique quels comptes ont généré des journaux et des événements à partir de cette source. Pour chaque compte, le panneau divisé inclut à la fois l'utilisation réelle provenant de cette source et l'utilisation et les coûts prévus.
- Utilisation et coût par compte — Il s'agit de votre utilisation actuelle de Security Lake ventilée par compte, ainsi que de l'utilisation et des coûts estimés pour les 30 prochains jours calendaires sur la base de votre utilisation réelle pendant la période sélectionnée. Si vous sélectionnez un compte, un panneau séparé s'ouvre et affiche les sources ayant contribué à l'utilisation de ce compte. Pour chaque source contributive, le panneau divisé inclut à la fois l'utilisation réelle et l'utilisation et les coûts prévus.

Toutes les sources de AWS données prises en charge apparaissent dans les tableaux précédents, même si vous n'avez pas ajouté de source particulière dans Security Lake. Nous vous recommandons d'ajouter toutes les AWS sources si vous participez à l'essai gratuit afin d'obtenir une estimation des coûts pour l'ensemble complet de vos journaux et événements. Pour obtenir des instructions sur l'ajout d'une AWS source, consultezCollecte de données auprès de AWS services. Les sources personnalisées ne sont pas incluses dans le calcul de l'utilisation ou des coûts.

Suivez ces étapes pour consulter vos données d'utilisation et de coûts dans la console Security Lake.

Pour examiner l'utilisation de Security Lake et les coûts prévus (console)

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez consulter votre consommation et vos coûts.
3. Dans le volet de navigation, choisissez Paramètres, puis Utilisation.
4. Sélectionnez la période pour laquelle vous souhaitez consulter les données d'utilisation et de coûts. La valeur par défaut est le dernier jour.
5. Sélectionnez l'onglet Par source de données ou Par comptes pour examiner l'utilisation et les coûts en détail.

Amazon Security

Pour obtenir la liste des régions et des points de terminaison de service pris en charge pour Security Lake, consultez les points de terminaison Amazon Security Lake dans le Références générales AWS.

Nous vous recommandons d'activer Security Lake dans tous les cas compatiblesRégions AWS. Cela vous permet d'utiliser Security Lake pour détecter et enquêter sur les activités non autorisées ou inhabituelles, même dans les régions que vous n'utilisez pas activement.

Désactivation d'Amazon Security Lake

Lorsque vous désactivez Amazon Security Lake, Security Lake cesse de collecter les journaux et les événements provenant de vos AWS sources. Les paramètres de Security Lake existants et les ressources créées dans votre environnement Compte AWS sont conservés. En outre, les données que vous avez stockées ou que vous avez publiées pour d'autres AWS services, telles que les données sensibles contenues dans AWS Lake Formation des tables et AWS CloudTrail des journaux, restent disponibles. Les données stockées dans votre compartiment Amazon Simple Storage Service (Amazon S3) restent disponibles conformément à votre cycle de vie de stockage Amazon S3.

La désactivation de Security Lake depuis la page Paramètres de la console Security Lake arrête la collecte des AWS journaux et des événements Régions AWS dans toutes les régions où Security Lake est actuellement activé. Vous pouvez utiliser la page Régions de la console pour arrêter la collecte des journaux dans des régions spécifiques. L'API Security Lake permet AWS CLI également d'arrêter la collecte de journaux dans les régions que vous spécifiez dans votre demande.

Si vous utilisez l'intégration avec Security Lake AWS Organizations et que votre compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Security Lake, seul l'administrateur délégué de Security Lake peut désactiver Security Lake pour lui-même et pour les comptes des membres. Cependant, le fait de quitter une organisation arrête la collecte des journaux pour le compte d'un membre.

Lorsque vous désactivez Security Lake pour une organisation, la désignation d'administrateur délégué est conservée si vous suivez les instructions de désactivation fournies sur cette page. Il n'est pas nécessaire de désigner à nouveau l'administrateur délégué pour pouvoir réactiver Security Lake.

Pour les sources personnalisées, lorsque vous désactivez Security Lake, vous devez désactiver chaque source en dehors de la console Security Lake. Si vous ne désactivez pas une intégration, les intégrations source continueront à envoyer des journaux dans Amazon S3. En outre, vous devez désactiver l'intégration d'un abonné, sinon celui-ci pourra toujours utiliser les données de Security Lake. Pour plus de détails sur la suppression d'une source personnalisée ou d'une intégration d'abonnés, consultez la documentation du fournisseur concerné.

Nous vous recommandons de supprimer AWS Glue les tables avant de réactiver Security Lake afin de garantir le bon fonctionnement de l'accès aux requêtes des abonnés. Lorsque Security Lake est réactivé, un nouveau compartiment Amazon S3 du lac de données est créé et les données sont collectées dans ce nouveau compartiment S3. Si vous avez déjà supprimé AWS Glue des tables, un nouvel ensemble de AWS Glue tables est créé.

Toutes les données collectées avant la désactivation de Security Lake resteront dans l'ancien compartiment Amazon S3. Si vous souhaitez interroger d'anciennes données, vous devez les déplacer vers le nouveau compartiment à l'aide de la `Sync` commande Amazon S3. Pour plus de détails, consultez la commande Sync dans le manuel de référence des AWS CLI commandes.

Cette rubrique explique comment désactiver Security Lake à l'aide de la console Security Lake, de l'API Security Lake ou AWS CLI.

Console

1. Ouvrez la console Security Lake à l'adresse https://console.aws.amazon.com/securitylake/.
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Choisissez Désactiver Security Lake.
4. Lorsque vous êtes invité à confirmer, entrez**`Disable`**, puis choisissez Désactiver.

API

Pour désactiver Security Lake par programmation, utilisez le DeleteDataLakefonctionnement de l'API Security Lake. Si vous utilisez le AWS CLI, exécutez la delete-date-lakecommande. Dans votre demande, utilisez la `regions` liste pour spécifier le code de région pour chaque région dans laquelle vous souhaitez désactiver Security Lake. Pour obtenir la liste des codes de région, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.

Dans le cas d'un déploiement utilisant Security Lake AWS Organizations, seul l'administrateur délégué de Security Lake à l'organisation peut désactiver Security Lake pour les comptes de l'organisation.

Par exemple, la AWS CLI commande suivante désactive le lac de sécurité dans les `eu-central-1` régions `ap-northeast-1` et. Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

Questions fréquentes (FAQ)

Mise à jour de Security Lake vers la dernière version du parquet

Le 20/05/2024, Amazon Security Lake sera mis à jour vers la dernière version du parquet.

Pourquoi Security Lake effectue-t-il cette mise à jour ?

Dans le cadre des efforts continus déployés par Amazon pour fournir à ses clients des services sécurisés et efficaces, Security Lake met régulièrement à jour les dépendances, les bibliothèques tierces, les API et les outils. Security Lake veille également à ce que les clients utilisent les dernières extensions de toutes les normes, y compris les spécifications du parquet.

Dans de rares cas, cela peut entraîner des modifications mineures de la manière dont les données sont stockées et/ou traitées. Les modifications sont toujours rétrocompatibles avec les normes communautaires établies.

Security Lake normalise les fichiers journaux de sécurité des clients au format OCSF et les expose dans un format parquet efficace pour les requêtes. Security Lake apporte cette modification afin de garantir une adoption sans faille du dernier format de parquet. Pour plus de détails, voir Format du parquet.

Où puis-je en savoir plus sur la modification des spécifications du parquet ?

Pour plus d'informations, consultez la section Horodatage obsolète ConvertedType dans le référentiel du format parquet. GitHub

Cette mise à niveau a-t-elle un impact sur mes intégrations à Security Lake ?

Si vous utilisez uniquement les outils Amazon Athena ou Apache (Spark, Hive, Impala, Hadoop) pour accéder aux tables de Security Lake, il n'y a aucun changement. Les modifications liées à la mise à niveau seront automatiquement gérées par les outils clients et les API de manière transparente.

Si vous utilisez d'autres outils clients, Security Lake recommande de comprendre les nouvelles méthodes de stockage et de gestion des champs de date/heure. Le tableau suivant répertorie les différences mineures que vous pouvez observer entre les anciennes et les nouvelles données synthétiques.

Changements dans les données synthétiques

AWS Services	Type	Current	New
Amazon Athena	Date/heure	20-01-1970 03:04:05 .399 000	Pas de modification
Apache Spark	Date/heure	1970-01-20T 00:04:05 000-03:00	Pas de modification
PyArrow	Date/heure	20-01-1970 03:04:05	1970-01-20 03:04:05 + 00:00 L'introduction du marqueur de fuseau horaire UTC a changé.

Comment puis-je identifier les changements dans le traitement du format du parquet ?

Téléchargez le fichier zip parquet_format.zip. Le fichier zip est composé de deux fichiers.

- Données de test synthétiques générées par l'ancien framework — `parquet_format_old.parquet`

- Données de test synthétiques générées par le nouveau framework — `parquet_format_new.parquet`

Testez vos outils clients et comparez les données de test synthétiques générées par l'ancien framework avec les données générées par le nouveau framework.

Si vous observez des changements notables, utilisez les recommandations du `Changes in synthetic data` tableau. Si vous avez besoin d'une assistance supplémentaire, contactez AWS le support.

Historique du document pour le guide de l'utilisateur d'Amazon Security Lake

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version d'Amazon Security Lake. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Dernière mise à jour de la documentation : 10 juin 2024

Modification	Description	Date
Disponibilité par région	Security Lake est désormais disponible dans AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). Régions AWS Pour obtenir la liste complète des régions dans lesquelles Security Lake est actuellement disponible, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.	10 juin 2024
Mise à jour de la politique gérée existante	Security Lake a ajouté AWS WAF des actions à la politique AWS gérée pour la `SecurityLakeServiceLinkedRole` politique. Les actions supplémentaires permettent à Security Lake de collecter AWS WAF des journaux lorsqu'il est activé en tant que source de journaux dans Security Lake.	22 mai 2024

Nouvelle source de AWS journal	Security Lake a ajouté les journaux AWS WAF en tant AWS que source de journaux. AWS WAF vous permet de surveiller les requêtes Web que les utilisateurs finaux envoient aux applications.	22 mai 2024
Mise à jour de la politique gérée existante	Security Lake a ajouté des actions SID à la `AmazonSecurityLakePermissionsBoundary` politique.	13 mai 2024
Mise à jour de la politique gérée existante	Security Lake a mis à jour la politique du AmazonSecurityLakeMetastoregestionnaire pour ajouter une action de nettoyage des métadonnées qui vous permet de supprimer les métadonnées de votre lac de données.	27 mars 2024
Nouvelles versions sources	Mettez à jour les autorisations de votre rôle pour ingérer les données des nouvelles versions des sources de données.	29 février 2024
Nouvelle source de AWS journal	Security Lake a ajouté les journaux d'audit EKS en tant que source de AWS journaux. Les journaux d'audit EKS vous aident à détecter les activités potentiellement suspectes dans vos clusters EKS au sein d'Amazon Elastic Kubernetes Service.	29 février 2024

Mise à jour de la politique gérée existante	Security Lake a mis à jour la politique pour autoriser `iam:PassRole` le nouveau `AmazonSecurityLakeMetastoreManagerV2` rôle et permet à Security Lake de déployer ou de mettre à jour les composants du lac de données.	23 février 2024
Nouvelle politique gérée	Security Lake a ajouté une nouvelle politique AWS gérée , la `AmazonSecurityLakeMetastoreManager` politique. Cette politique autorise Security Lake à gérer les métadonnées de votre lac de données.	23 janvier 2024
Disponibilité par région	Security Lake est désormais disponible dans les pays suivants Régions AWS : Asie-Pacifique (Osaka), Canada (Centre), Europe (Paris) et Europe (Stockholm). Pour obtenir la liste complète des régions dans lesquelles Security Lake est actuellem ent disponible, consultez la section Points de terminaison Amazon Security Lake dans le Références générales AWS.	26 octobre 2023

Nouvelles fonctionnalités	Vous pouvez désormais modifier certains paramètres pour les abonnés ayant accès aux requêtes. Vous pouvez également attribuer des balises aux ressources de Security Lake pour votre Compte AWS.	20 juillet 2023
Nouvelle politique gérée	Security Lake a ajouté une nouvelle politique AWS gérée, la `AmazonSecurityLakeAdministrator` politique. Cette politique accorde des autorisations administratives qui permettent un accès complet principal à toutes les actions de Security Lake.	30 mai 2023
Disponibilité générale	Security Lake est désormais disponible pour tous.	30 mai 2023
Nouvelle fonction	Security Lake envoie désormais des métriques à Amazon CloudWatch.	4 mai 2023
Disponibilité par région	Security Lake est désormais disponible dans les pays suivants Régions AWS : Asie-Pacifique (Singapour), Europe (Londres) et Amérique du Sud (São Paulo).	22 mars 2023

Nouvelle fonction	Security Lake crée désormais des rôles AWS Identity and Access Management (IAM) en votre nom lorsque vous utilisez la console Security Lake pour activer et commencer à utiliser Security Lake.	15 février 2023
Première version	Il s'agit de la version initiale du guide de l'utilisateur d'Amazon Security Lake.	29 novembre 2022

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.