aws

用户指南

Amazon Security Lake

Amazon Security Lake: 用户指南

Table of Contents

什么是 Amazon Security Lake？

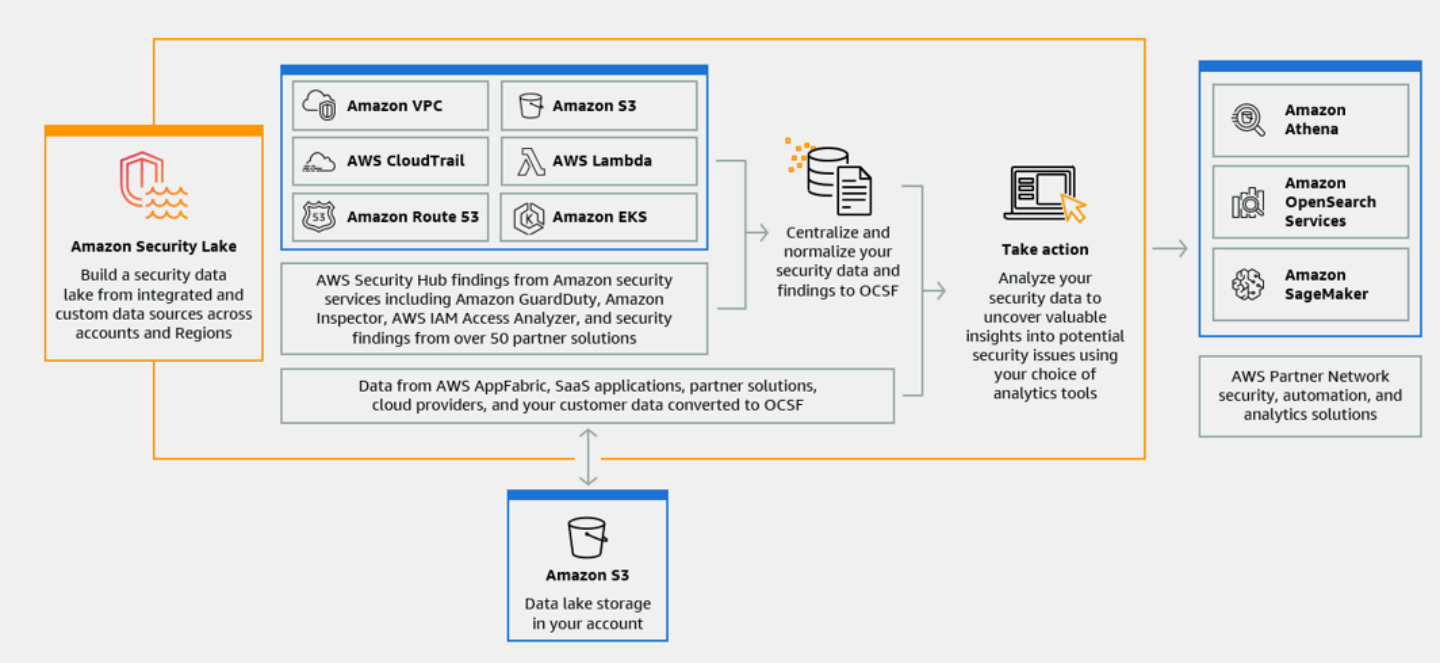
Amazon Security Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 将来自 AWS 环境、SaaS 提供商、本地、云端和第三方来源的安全数据自动集中到您的 AWS 账户 的专用数据湖中。Security Lake 可以帮助您分析安全数据，让您更全面地了解整个组织的安全状况。借助 Security Lake，您还可以改善对工作负载、应用程序和数据的保护。

数据湖由 Amazon Simple Storage Service (Amazon S3) 存储桶提供支持，您保留数据的所有权。

Security Lake 可以自动从集成的 AWS 服务和第三方服务中收集与安全相关的日志和事件数据。它还可以通过可自定义的保留和复制设置帮助您管理数据的生命周期。Security Lake 会将摄取的数据转换为 Apache Parquet 格式和名为开放网络安全架构框架 (OCSF) 的标准开源架构。在 OCSF 的支持下，Security Lake 可以对来自 AWS 和各种企业安全数据来源的安全数据进行标准化处理和合并。

其他 AWS 服务和第三方服务可以订阅存储在 Security Lake 中的数据，用于事件响应和安全数据分析。

Security Lake 概览



Security Lake 的功能

以下是 Security Lake 帮助您集中、管理和订阅与安全相关的日志和事件数据的一些关键方法。

将数据汇总到您的账户中

Security Lake 会在您的账户中创建专用的安全数据湖。Security Lake 可以从云端、本地以及不同账户和区域的自定义数据来源中收集日志和事件数据。数据湖由 Amazon Simple Storage Service (Amazon S3) 存储桶提供支持，您保留数据的所有权。

支持多种日志和事件来源

Security Lake 可以从包括本地、AWS 服务和第三方服务在内的多个来源中收集安全日志和事件。收集日志后，无论来源是什么，您都可以集中访问它们并管理其生命周期。有关 Security Lake 从中收集日志和事件的来源的详细信息，请参阅 Amazon Security Lake 中的来源管理

数据转换和标准化

Security Lake 会自动对来自原生支持的 AWS 服务的传入数据进行分区，并将其转换为适合高效存储和查询的 Parquet 格式。它还会将来自原生支持的 AWS 服务的数据转换为开放网络安全架构框架 (OCSF) 开源架构。这使得数据可以与其他 AWS 服务和第三方提供商兼容，无需进行后期处理。Security Lake 对数据进行了标准化，因此许多安全解决方案都可以并行使用这些数据。

为订阅用户提供多种级别的访问权限

订阅用户可以使用存储在 Security Lake 中的数据。您可以选择订阅用户对您的数据的访问权限级别。订阅用户只能使用来自您指定的来源和 AWS 区域中的数据。当新对象被写入数据湖时，订阅用户可能会自动收到有关这些对象的通知。订阅用户也可以从数据湖中查询数据。Security Lake 会自动在 Security Lake 和订阅用户之间创建和交换所需的凭证。

多账户和多区域数据管理

您可以在支持 Security Lake 的所有区域和多个 AWS 账户中集中启用 Security Lake。在 Security Lake 中，您还可以指定汇总区域，以便整合来自多个区域的安全日志和事件数据。这可以帮助您遵守数据驻留合规性要求。

可配置且可自定义

Security Lake 是一项可配置并且可自定义的服务。您可以指定要为哪些来源、账户和区域配置日志收集。您还可以指定订阅用户对数据湖的访问权限级别。

数据生命周期管理和优化

Security Lake 能够通过可自定义的留存设置来管理数据的生命周期，并通过自动存储分层来管理存储成本。Security Lake 会自动对传入的安全数据进行分区，并将其转换为适合高效存储和查询的 Parquet 格式。

访问 Security Lake

有关提供 Security Lake 的区域的列表，请参阅 Amazon Security Lake 区域和端点。要了解有关区域的更多信息，请参阅 AWS 一般参考中的 AWS服务端点。

在每个区域，您可以通过以下任何方式访问 Security Lake：

AWS Management Console

AWS Management Console 是一个基于浏览器的界面，可以用来创建和管理 AWS 资源。Security Lake 控制台可以提供对您的 Security Lake 账户和资源的访问权限。您可以使用 Security Lake 控制台执行大多数 Security Lake 任务。

Security Lake API

要以编程方式访问 Security Lake，您可以使用 Security Lake API，直接向服务发出 HTTPS 请求。有关更多信息，请参阅 Security Lake API 参考。

AWS Command Line Interface (AWS CLI)

使用 AWS CLI，您可以在系统的命令行中发出命令以执行 Security Lake 任务和 AWS 任务。与控制台相比，使用命令行更快捷、更方便。如果要构建执行任务的脚本，命令行工具也会十分有用。有关安装和使用 AWS CLI 的更多信息，请参阅 AWS Command Line Interface。

AWS 软件开发工具包

AWS 提供的软件开发工具包包含用于各种编程语言和平台的库和示例代码，例如 Java、Go、Python、C++ 和 .NET 等。这些软件开发工具包可以提供对 Security Lake 和其他 AWS 服务的编程式便捷访问。它们可以执行多种任务，例如以加密方式对请求进行签名、管理错误以及自动重试请求等。有关安装和使用 AWS 软件开发工具包的信息，请参阅在 AWS 上构建的工具。

相关服务

以下是 Security Lake 使用的其他 AWS 服务：

- Amazon EventBridge – 当对象被写入数据湖时，Security Lake 使用 EventBridge 通知订阅用户。
- AWS Glue – Security Lake 使用 AWS Glue 爬网程序来创建 AWS Glue Data Catalog 表并将新写入的数据发送到 Data Catalog。Security Lake 还会将 AWS Lake Formation 表的分区元数据存储在 Data Catalog 中。

- AWS Lake Formation – Security Lake 会为每个向 Security Lake 提供数据的来源创建一个单独的 Lake Formation 表。Lake Formation 表中包含来自每个来源的数据的相关信息，包括架构、分区和数据位置信息。订阅用户可以选择通过查询 Lake Formation 表来使用数据。
- AWS Lambda – Security Lake 使用 Lambda 函数来支持对原始数据进行提取、转换和加载 (ETL) 作业，并在 AWS Glue 中为源数据注册分区。
- Amazon S3 – Security Lake 将数据存储为 Amazon S3 对象。存储类和保留设置基于 Amazon S3 产品。Security Lake 不支持 Amazon S3 Select。

除以下 AWS 服务外，Security Lake 还从自定义来源收集数据：

- AWS CloudTrail 管理事件和数据事件（S3、Lambda）
- Amazon Route 53 resolver 查询日志
- AWS Security Hub 结果
- Amazon Virtual Private Cloud (Amazon VPC) 流日志

有关这些来源的更多信息，请参阅 从中收集数据 AWS 服务。您可以创建能够读取 OCSF 架构中的数据的订阅用户，从而使用安全数据湖中的 Amazon S3 对象。您还可以使用 Athena、Amazon Redshift 和与 AWS Glue 集成的第三方订阅服务来查询数据。

概念和术语

本部分介绍了可以帮助您使用 Amazon Security Lake 的关键概念和术语。

数据提供区域

一个或多个向汇总区域提供数据的 AWS 区域。

数据湖

存储在 Amazon Simple Storage Service (Amazon S3) 中并由 Security Lake 管理的永久数据。Security Lake 使用 AWS Glue 将新写入的数据发送到数据目录。Security Lake 还会为向数据湖提供数据的每个来源创建一个 AWS Lake Formation 表。数据湖中通常存储以下内容：

- 结构化数据和非结构化数据
- 原始数据和转换后的数据

Security Lake 是一项数据湖服务，旨在收集与安全相关的日志和事件。

开放式网络安全架构框架 (OCSF)

用于安全日志和事件的标准化开源架构。它由 AWS 和各种安全领域的其他安全行业领导者共同开发。Security Lake 会将其从 AWS 服务 收集的日志和事件自动转换为 OCSF 架构。自定义来源会将其日志和事件转换为 OCSF，然后再发送到 Security Lake。

汇总区域

用于整合来自一个或多个数据提供区域的安全日志和事件的 AWS 区域。指定一个或多个汇总区域可以帮助您遵守区域合规性要求。

来源

来源是单个系统中生成的与 OCSF 中的特定事件类相匹配的一系列日志和事件。Security Lake 可以从来源收集数据。来源可以是其他 AWS 服务，也可以是第三方服务。对于第三方来源，您必须先将数据转换为 OCSF 架构，然后再将其发送到 Security Lake。

订阅用户

使用来自 Security Lake 的日志和事件的一项服务。订阅用户可以是其他 AWS 服务，也可以是第三方服务。

Amazon Security Lake 入门

本部分介绍如何启用和开始使用 Security Lake。您将学习如何配置数据湖设置和设置日志收集。您可以通过 AWS Management Console 或以编程方式启用和使用 Security Lake。无论使用哪种方法，都必须先设置 AWS 账户 和管理员用户。之后的步骤因访问方法而异。Security Lake 控制台提供了简化的入门流程，并创建了创建数据湖所需的所有必需的 AWS Identity and Access Management (IAM) 角色。

初始 AWS 账户 设置

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实操，请为管理用户分配管理访问权限，并且只使用根用户执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择 My Account（我的账户）来查看当前的账户活动并管理您的账户。

创建管理用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。

2. 对您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建管理用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为管理用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

作为管理用户登录

- 要使用 IAM Identity Center 用户身份登录，请使用在创建 IAM Identity Center 用户时发送到电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

确定您用来启用 Security Lake 的账户

Security Lake 与 AWS Organizations 集成，可管理组织中多个账户的日志收集。如果您想在组织中使用 Security Lake，必须使用您的 Organizations 管理账户来指定一个委托的 Security Lake 管理员。然后，您必须使用委托管理员的凭证启用 Security Lake、添加成员账户并为他们启用 Security Lake。有关更多信息，请参阅使用管理多个账户 AWS Organizations。

另外，对于不属于组织的独立账户，您可以使用未与 Organizations 集成的 Security Lake。

启用 Amazon 安全湖时的注意事项

在启用 Security Lake 之前，请考虑以下事项：

- Security Lake 提供跨区域管理功能，这意味着您可以跨 AWS 区域创建数据湖并配置日志收集。要在所有受支持的区域中启用 Security Lake，您可以选择任意受支持的区域端点。您还可以添加汇总区域，以便将来自多个区域的数据聚合到一个区域。

- 我们建议在所有受支持的 AWS 区域中激活 Security Lake。如果这样做，Security Lake 可以收集与未经授权的活动或异常活动相关的数据，即使在您没有主动使用的区域也可以。如果不在所有受支持的区域中激活 Security Lake，则它从您在多个区域使用的其他服务收集数据的能力就会降低。
- 在任何区域首次启用 Security Lake 时，系统都会为您的账户创建一个名为 `AWSServiceRoleForSecurityLake` 的服务相关角色。此角色包括代表您呼叫他人 AWS 服务 以及操作安全数据湖的权限。要详细了解服务相关角色的工作原理，请参阅 IAM 用户指南中的使用服务相关角色。如果您以委托的 Security Lake 管理员身份启用 Security Lake，Security Lake 将在组织中的每个成员账户中创建服务相关角色。
- Security Lake 不支持 Amazon S3 对象锁定。创建数据湖存储桶时，S3 对象锁定默认处于禁用状态。如果在存储桶上启用对象锁定，则向数据湖传输标准化日志数据的过程将会中断。

主机入门

本教程介绍如何通过启用和配置 Security Lake AWS Management Console。作为其中的一部分 AWS Management Console，Security Lake 控制台提供了简化的入门流程，并创建了创建数据湖所需的所有必需的 AWS Identity and Access Management (IAM) 角色。

步骤 1：配置源

Security Lake 会从您的 AWS 账户 和 AWS 区域中的各种来源收集日志和事件数据。按照以下说明指定您希望 Security Lake 收集哪些数据。您只能使用这些说明将原生支持的 AWS 服务 添加为来源。有关添加自定义来源的更多信息，请参阅从自定义源收集数据。

配置日志源收集

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 使用页面右上角的 AWS 区域 选择器选择一个区域。您可以在服务启用过程中在当前区域和其他区域启用 Security Lake。
3. 选择开始。
4. 对于选择日志和事件来源，选择以下选项之一：

    a. 采集默认 AWS 来源 — 选择推荐的选项时， CloudTrail 不包括 S3 数据事件供摄取。这是因为摄取大量 CloudTrail -S3 数据事件可能会显著影响使用成本。要摄取此来源，请选择摄取特定 AWS 来源选项。

    b. 摄取特定 AWS 来源-使用此选项，您可以选择一个或多个要采集的日志和事件源。

> **Note**
>
> 首次在账户中启用 Security Lake 时，所有选定的日志和事件来源都将包含在 15 天免费试用期内。有关使用情况统计数据的信息，请参阅查看使用量和估算费用。

5. 对于版本，选择要从中提取日志和事件源的数据源的版本。

> **Important**
>
> 如果您没有在指定区域启用新版本 AWS 日志源所需的角色权限，请联系您的 Security Lake 管理员。有关更多信息，请参阅更新角色权限。

6. 对于选择区域，选择是从所有受支持的区域还是从特定的区域摄取日志和事件来源。如果选择特定区域，请选择要从哪些区域摄取数据。
7. 要服务访问权限，请创建一个新的 IAM 角色或使用现有的 IAM 角色来授予 Security Lake 从您的来源收集数据并将其添加到数据湖的权限。启用了 Security Lake 的所有区域中都使用一个角色。
8. 选择下一步。

步骤 2：定义存储设置和汇总区域（可选）

您可以指定 Security Lake 用来存储数据的 Amazon S3 存储类以及存储多长时间。您也可以指定一个汇总区域，以整合来自多个区域的数据。这些是可选步骤。有关更多信息，请参阅Security Lake 中的生命周期管理。

配置存储和汇总设置

1. 如果要将来自多个区域的数据整合到汇总区域，请在选择汇总区域中选择添加汇总区域。指定汇总区域以及向汇总区域提供数据的区域。您可以设置一个或多个汇总区域。
2. 在选择存储类中，选择 Amazon S3 存储类。默认的存储类是 S3 Standard。如果希望数据在留存期结束后转换到另一个存储类，请提供留存期（以天为单位），然后选择添加转换。留存期结束后，对象将过期，Amazon S3 会将其删除。有关 Amazon S3 存储类和留存的更多信息，请参阅留存管理。
3. 如果在第一步中选择了汇总区域，则对于服务访问权限，请创建一个新的 IAM 角色或使用现有 IAM 角色来向 Security Lake 授予跨多个区域复制数据的权限。
4. 选择下一步。

步骤 3：查看并创建数据湖

查看 Security Lake 将从中收集数据的来源、您的汇总区域和留存期设置。然后，创建您的数据湖。

查看和创建数据湖

1. 在启用 Security Lake 时，请查看日志和事件来源、区域、汇总区域和存储类。
2. 选择创建。

创建数据湖后，您将在 Security Lake 控制台上看到摘要页面。此页面概述了区域和汇总区域的数量、有关订阅者的信息以及问题。

“问题” 菜单显示了过去 14 天内影响安全湖服务或您的 Amazon S3 存储桶的问题摘要。有关每个问题的更多详细信息，您可以访问 Security Lake 控制台的 “问题” 页面。

第 4 步：查看和查询自己的数据

创建数据湖后，您可以使用 Amazon Athena 或类似服务查看和查询数据库和表 AWS Lake Formation 中的数据。当您使用控制台时，Security Lake 会自动向您用于启用 Security Lake 的角色授予数据库查看权限。该角色必须至少拥有数据分析师权限。有关权限级别的更多信息，请参阅 Lake Formation 角色和 IAM 权限参考。有关授予 SELECT 权限的说明，请参阅《AWS Lake Formation 开发人员指南》中的使用命名的资源方法授予数据目录权限。

步骤 5：创建订阅者

创建数据湖后，您可以添加订阅用户来使用您的数据。订阅用户可以通过直接访问您的 Amazon S3 存储桶中的对象或查询数据湖来使用数据。有关订阅用户的更多信息，请参阅 Amazon Security Lake 中的订阅用户管理。

以编程方式入门

本教程介绍如何以编程方式启用和开始使用 Security Lake。Amazon Security Lake API 让您能够以编程方式全面访问您的安全湖账户、数据和资源。或者，您可以使用 AWS 命令行工具（或用于的工具 PowerShell ）AWS Command Line Interface或软件开发AWS 工具包来访问 AWS Security Lak e。

步骤 1：创建 IAM 角色

如果您以编程方式访问 Security Lake，则需要创建一些 AWS Identity and Access Management (IAM) 角色才能配置您的数据湖。

> **Important**
>
> 如果您使用 Security Lake 控制台启用和配置 Security Lake，则无需创建这些 IAM 角色。

如果您要执行以下一项或多项操作，则必须在 IAM 中创建角色（选择链接以查看有关每个操作的 IAM 角色的更多信息）：

- 创建自定义来源：自定义来源是指除原生支持的 AWS 服务 之外的其他向安全湖发送数据的来源。
- 创建具有数据访问权限的订阅用户：拥有权限的订阅用户可以直接从您的数据湖访问 S3 对象。
- 创建具有查询权限的订阅用户：拥有权限的订阅用户可以使用诸如 Amazon Athena 之类的服务查询来自 Security Lake 的数据。
- 配置汇总区域：汇总区域合并来自多个 AWS 区域的数据。

创建前面提到的角色后，将AmazonSecurityLakeAdministrator AWS 托管策略附加到您用于启用 Security Lake 的角色。此策略授予管理权限，允许主体登录到 Security Lake 并访问所有 Security Lake 操作。

附加AmazonSecurityLakeMetaStoreManager AWS 托管策略以创建您的数据湖或从 Security Lake 查询数据。Security Lake 需要使用此策略来支持对从源收到的原始日志和事件数据进行提取、转换和加载 (ETL) 作业。

第 2 步：启用 Amazon 安全湖

要以编程方式启用安全湖，请使用安全湖 API 的CreateDataLake操作。如果您使用的是 AWS CLI，请运行create-data-lake命令。在您的请求中，使用 `configurations` 对象的 `region` 字段为要在其中启用 Security Lake 的区域指定区域代码。有关区域代码的列表，请参阅 AWS 一般参考 中的 Amazon Security Lake 端点。

示例 1

以下示例命令在`us-east-1`和`us-east-2`区域中启用安全湖。在这两个区域中，该数据湖均使用 Amazon S3 托管密钥进行加密。对象在 365 天后过期，对象在 60 天后过渡到 `ONEZONE_IA` S3 存储类别。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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"
```

示例 2

以下示例命令在us-east-2区域中启用安全湖。此数据湖使用在 AWS Key Management Service (AWS KMS) 中创建的客户托管密钥进行加密。对象在 500 天后过期，对象在 30 天后转换到 GLACIER S3 存储类别。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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**
>
> 如果您已经启用了 Security Lake，并且想要更新某个区域或来源的配置设置，请使用UpdateDataLake操作，或者如果使用 AWS CLI，则使用update-data-lake命令。不要使用该CreateDataLake操作。

步骤 3：配置源

Security Lake 会从您的 AWS 账户 和 AWS 区域中的各种来源收集日志和事件数据。按照以下说明指定您希望 Security Lake 收集哪些数据。您只能使用这些说明将原生支持的 AWS 服务 添加为来源。有关添加自定义来源的更多信息，请参阅从自定义源收集数据。

要以编程方式定义一个或多个集合源，请使用 Security Lake API 的CreateAwsLogSource操作。对于每个来源，请为 sourceName 参数指定区域唯一的值。（可选）使用其他参数将来源的范围限制为特定账户 (accounts) 或特定版本 (sourceVersion)。

> **Note**
>
> 如果您在请求中未包含可选参数，Security Lake 会根据您排除的参数，将请求应用到指定来源的所有账户或所有版本。例如，如果您是组织委托的 Security Lake 管理员，并且您排除 `accounts` 参数，则 Security Lake 会将请求应用于组织中的所有账户。同样，如果您排除 `sourceVersion` 参数，Security Lake 会将请求应用于指定来源的所有版本。

如果请求指定了您尚未启用 Security Lake 的区域，则会发生错误。要解决此错误，请确保 `regions` 数组仅指定您已启用 Security Lake 的区域。或者，您也可以在区域中启用 Security Lake，然后再次提交请求。

首次在账户中启用 Security Lake 时，所有选定的日志和事件来源都将包含在 15 天免费试用期内。有关使用情况统计数据的信息，请参阅查看使用量和估算费用。

步骤 4：配置存储设置和汇总区域（可选）

您可以指定 Security Lake 用来存储数据的 Amazon S3 存储类以及存储多长时间。您也可以指定一个汇总区域，以整合来自多个区域的数据。这些是可选步骤。有关更多信息，请参阅Security Lake 中的生命周期管理。

要在启用 Security Lake 时以编程方式定义目标目标，请使用 Security Lake API 的CreateDataLake操作。如果您已经启用 Security Lake 并想要定义目标目标，请使用UpdateDataLake操作而不是`CreateDataLake`操作。

对于任一操作，请使用受支持的参数来指定所需的配置设置：

- 要指定汇总区域，请使用该`region`字段指定要向汇总区域提供数据的区域。在`replicationConfiguration`对象的`regions`数组中，为每个汇总区域指定区域代码。有关区域代码的列表，请参阅 AWS 一般参考 中的 Amazon Security Lake 端点。
- 要为数据指定留存期设置，请使用 `lifecycleConfiguration` 参数：
  - 对于 `transitions`，请指定要在特定 Amazon S3 存储类 (`storageClass`) 中存储 S3 对象的总天数 (`days`)。
  - 对于 `expiration`，可以使用任意存储类指定对象创建后在 Amazon S3 中存储对象的总天数。此留存期结束后，对象将过期，Amazon S3 会将其删除。

  Security Lake 会将指定的留存期设置应用于您在 `configurations` 对象的 `region` 字段中指定的区域。

例如，以下命令使用ap-northeast-2汇总区域创建数据湖。该us-east-1地区将向该ap-northeast-2地区提供数据。此示例还为添加到数据湖中的对象设定了 10 天的过期期。

```
$ 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"
```

现在，您已经创建了数据湖。使用 Security Lake API 的ListDataLakes操作来验证每个区域中是否启用了安全湖和您的数据湖设置。

如果在创建数据湖时出现问题或错误，则可以使用该ListDataLakeExceptions操作查看异常列表，并将CreateDataLakeExceptionSubscription操作的异常通知用户。有关更多信息，请参阅对数据湖状态进行故障排除。

第 5 步：查看和查询自己的数据

创建数据湖后，您可以使用 Amazon Athena 或类似服务查看和查询数据库和表 AWS Lake Formation 中的数据。当您以编程方式启用 Security Lake 时，不会自动授予数据库查看权限。中的数据湖管理员账户 AWS Lake Formation 必须向要用于查询相关数据库和表的 IAM 角色授予SELECT权限。该角色必须至少拥有数据分析师权限。有关权限级别的更多信息，请参阅 Lake Formation 角色和 IAM 权限参考。有关授予 SELECT 权限的说明，请参阅《AWS Lake Formation 开发人员指南》中的使用命名的资源方法授予数据目录权限。

步骤 6：创建订阅者

创建数据湖后，您可以添加订阅用户来使用您的数据。订阅用户可以通过直接访问您的 Amazon S3 存储桶中的对象或查询数据湖来使用数据。有关订阅用户的更多信息，请参阅 Amazon Security Lake 中的订阅用户管理。

使用管理多个账户 AWS Organizations

您可以使用 Amazon Security Lake 从多个 AWS 账户收集安全日志和事件。为帮助您自动化和简化多个账户的管理，我们强烈建议您将 Security Lake 与 AWS Organizations 集成。

在 Organizations 中，用于创建组织的账户称为管理账户。要将 Security Lake 与 Organizations 集成，管理账户必须为组织指定一个委托的 Security Lake 管理员账户。

委托的 Security Lake 管理员可以启用 Security Lake，并为成员账户配置 Security Lake 设置。委派的管理员可以在所有启用了 Security Lake AWS 区域 的地方（无论他们当前使用的是哪个区域终端节点）收集整个组织的日志和事件。委托管理员还可以配置 Security Lake 来自动收集新组织账户的日志和事件数据。

委托的 Security Lake 管理员有权访问关联成员账户中的日志和事件数据。因此，他们可以配置 Security Lake 来收集关联成员账户拥有的数据。他们还可以向订阅用户授予使用关联成员账户所拥有的数据的权限。

要为组织中的多个账户启用 Security Lake，组织管理账户必须首先为组织指定一个委托的 Security Lake 管理员账户。然后，委托管理员可以为组织启用和配置 Security Lake。

有关设置 Organizations 的信息，请参阅《AWS Organizations 用户指南》中的创建和管理组织。

委托的 Security Lake 管理员的重要注意事项

请注意以下因素，它们定义了委托管理员在 Security Lake 中的行为方式：

委托管理员在所有区域都是相同的。

在您创建委托管理员后，它将成为您启用了 Security Lake 的每个区域的委托管理员。

我们建议将日志存档账户设置为 Security Lake 委托管理员。

日志存档账户专用于摄取和存档所有与安全相关的日志。 AWS 账户 通常只有少数用户拥有对该账户的访问权限，例如审计员和进行合规调查的安全团队。我们建议将日志存档账户设置为 Security Lake 委托管理员，这样您就可以查看与安全相关的日志和事件，且只需进行极少的上下文切换。

此外，我们建议仅允许极少数用户直接访问日志存档账户。除了这些用户外，如果其他用户需要访问 Security Lake 收集的数据，您可以将其添加为 Security Lake 订阅用户。有关添加订阅用户的信息，请参阅 Amazon Security Lake 中的订阅用户管理。

如果您不使用该 AWS Control Tower 服务，则可能没有日志存档帐户。有关日志存档账户的更多信息，请参阅《AWS 安全参考架构》中的安全 OU – 日志存档账户。

一个组织只能有一个委托管理员。

每个组织只能有一个委托的 Security Lake 管理员。

组织的管理账户不能成为委托管理员。

根据 AWS 安全最佳实践和最低权限原则，您的组织管理账户不能成为委托管理员。

委托管理员必须属于有效组织。

删除组织后，委托管理员账户将无法再管理 Security Lake。您必须从其他组织指定一个委托管理员，或通过不属于组织的独立账户来使用 Security Lake。

指定委托管理员所需的 IAM 权限

在指定委派的 Security Lake 管理员时，您必须拥有启用安全湖和使用以下政策声明中列出的某些 AWS Organizations API 操作的权限。

您可以在 AWS Identity and Access Management (IAM) 策略的末尾添加以下语句来授予这些权限。

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

指定委托的 Security Lake 管理员并添加成员账户

选择您的访问方式，为组织指定委托的 Security Lake 管理员账户。只有组织管理账户可以为其组织指定委托管理员账户。组织管理账户不能成为其组织的委托管理员账户。

> **Note**
>
> - 组织管理账户应使用 Security Lake `RegisterDataLakeDelegatedAdministrator` 操作来指定委派的 Security Lake 管理员账户。不支持通过 Organizations 指定委派的 Security Lake 管理员。
> - 如果要更改组织的委托管理员，您必须首先删除当前的委托管理员，然后再指定新的委托管理员。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   使用组织管理账户的凭据登录。

2. - 如果尚未启用 Security Lake，请选择开始，然后在启用 Security Lake 页面上指定委托的 Security Lake 管理员。
   - 如果已启用 Security Lake，请在设置页面上指定委托的 Security Lake 管理员。
3. 在 “将管理委托给其他账户” 下，选择已担任其他 AWS 安全服务委派管理员的账户（推荐）。或者，输入您要指定为 Security Lake 委派管理员的账户的 12 位 AWS 账户 ID。
4. 选择 Delegate（委派）。如果 Security Lake 尚未启用，指定委托管理员将在您的当前区域内为该账户启用 Security Lake。

API

要以编程方式指定委派管理员，请使用 Security Lake API 的RegisterDataLakeDelegatedAdministrator操作。您必须从组织管理账户调用该操作。如果您使用的是 AWS CLI，请从组织管理账户运行register-data-lake-delegated-administrator命令。在您的请求中，使用`accountId`参数指定的 12 位数账户 ID， AWS 账户 以指定为组织的委托管理员账户。

例如，以下 AWS CLI 命令指定委派的管理员。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

委托管理员还可以选择自动收集新组织账户的 AWS 日志和事件数据。使用此配置，在新账户中将账户添加到组织时，Security Lake 会自动启用 AWS Organizations。作为委托管理员，您可以使用 Security Lake API 的CreateDataLakeOrganizationConfiguration操作启用此配置，或者如果您使用的是 AWS CLI，则可以通过运行create-data-lake-organization-configuration命令来启用此配置。您还可以在请求中为新账户指定某些配置设置。

例如，以下 AWS CLI 命令会自动启用 Security Lake 以及在新的组织账户中收集 Amazon Route 53 解析器查询日志、 AWS Security Hub 调查结果和亚马逊虚拟私有云 (Amazon VPC) 流日志。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

组织的管理账户指定委托管理员后，管理员可以为组织启用和配置 Security Lake。这包括启用和配置 Security Lake 以收集组织中各个账户的 AWS 日志和事件数据。有关更多信息，请参阅从中收集数据 AWS 服务。

您可以使用该GetDataLakeOrganizationConfiguration操作来获取有关组织当前新成员账户配置的详细信息。

移除委托的 Security Lake 管理员

只有组织管理账户可以为其组织移除委托的 Security Lake 管理员。如果要更改组织的委托管理员，请移除当前的委托管理员，然后指定新的委托管理员。

> **Important**
>
> 移除委托的 Security Lake 管理员会删除数据湖，并针对组织中的账户禁用 Security Lake。

您无法使用 Security Lake 控制台更改或移除委托管理员。这些任务只能以编程方式执行。

要以编程方式移除委派的管理员，请使用 Security Lake API 的DeregisterDataLakeDelegatedAdministrator操作。您必须从组织管理账户调用该操作。如果您使用的是 AWS CLI，请从组织管理账户运行deregister-data-lake-delegated-administrator命令。

例如，以下 AWS CLI 命令删除委派的 Security Lake 管理员。

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

要保留委托管理员指定，但要更改新成员账户的自动配置设置，请使用 Security Lake API 的DeleteDataLakeOrganizationConfiguration操作，或者，如果你使用的是 AWS CLI，则使用delete-data-lake-organization-configuration命令。只有授权的管理员才能更改组织的这些设置。

例如，以下 AWS CLI 命令停止从加入组织的新成员账户自动收集 Security Hub 调查结果。在委托的管理员调用此操作后，新的成员账户将不会将 Security Hub 的发现结果贡献给数据湖。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

Security Lake 可信访问

为组织设置 Security Lake 后， AWS Organizations 管理账户可以通过 Security Lake 启用可信访问。可信访问允许 Security Lake 创建与 IAM 服务相关角色，并代表您在您的组织及其账户中执行任务。有关详细信息，请参阅《AWS Organizations 用户指南》中的结合使用 AWS Organizations 与其他 AWS 服务。

作为组织管理账户的用户，您可以在 AWS Organizations 中禁用对 Security Lake 的可信访问。有关禁用可信访问的说明，请参阅《AWS Organizations 用户指南》中的如何启用或禁用可信访问。

如果委派的管理员 AWS 账户 处于暂停状态、隔离状态或关闭状态，我们建议您禁用可信访问权限。

管理 区域

Amazon Security Lake AWS 区域 可以收集您启用该服务的安全日志和事件。对于每个区域，您的数据都存储在不同的 Amazon S3 存储桶中。您可以为不同的区域指定不同的数据湖配置（例如，不同的来源和留存设置）。您还可以定义一个或多个汇总区域来整合多个区域的数据。

检查区域状态

Security Lake 可以跨多个 AWS 区域收集数据。要跟踪数据湖的状态，了解每个区域的当前配置可能会有所帮助。选择您的首选访问方式，然后按照以下步骤获取区域的当前状态。

Console

查看地区状态

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中，选择区域。此时会显示区域页面，其中提供了当前已启用 Security Lake 的区域的概览。
3. 选择一个区域，然后选择编辑，查看该区域的详细信息。

API

要获取当前区域中日志收集的状态，请使用 Security Lake API 的GetDataLakeSources操作。如果您使用的是 AWS CLI，请运行该get-data-lake-sources命令。对于`accounts`参数，将一个或多个 AWS 账户 ID 指定为列表。如果您的请求成功，Security Lake 将返回当前区域中这些账户的快照，包括 Security Lake 正在从哪些 AWS 来源收集数据以及每个来源的状态。如果您不包含`accounts`参数，则响应将包含当前区域中配置了 Security Lake 的所有账户的日志收集状态。

例如，以下 AWS CLI 命令检索当前区域中指定账户的日志收集状态。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

以下 AWS CLI 命令列出指定区域中所有账户和已启用源的日志收集状态。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

要确定您是否为某个区域启用了安全湖，请使用ListDataLakes操作。如果您使用的是 AWS CLI，请运行该list-data-lakes命令。对于 `regions` 参数，请指定区域的区域代码。例如，`us-east-1` 表示美国东部（弗吉尼亚州北部）区域。有关区域代码的列表，请参阅《AWS 一般参考》中的 Amazon Security Lake 端点。`ListDataLakes` 操作会返回您在请求中指定的每个区域的数据湖配置设置。如果您未指定区域，Security Lake 会返回每个可用 Security Lake 的区域中您的数据湖的状态和配置设置。

例如，以下 AWS CLI 命令显示该`eu-central-1`区域中数据湖的状态和配置设置。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

更改区域设置

选择首选方式，然后按照以下说明更新一个或多个 AWS 区域中的数据湖的设置。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中，选择区域。
3. 选择一个区域，然后选择编辑。
4. 选择覆盖<区域>中所有账户的来源复选框，确认使用此处的选择覆盖该区域以前的选择。
5. 在选择存储类中，选择添加转换，为您的数据添加新的存储类。
6. 对于标签，您可以选择为区域指定或编辑标签。标签是您可以为某些类型的 AWS 资源定义和分配的标签，包括您在特定 AWS 账户 区域的数据湖配置。要了解更多信息，请参阅为 Amazon Security Lake 资源添加标签。
7. 要将某个区域变为汇总区域，请在导航窗格中选择汇总区域（在设置下）。然后选择 Modify (修改)。在选择汇总区域部分，选择添加汇总区域。选择数据提供区域，并向 Security Lake 提供跨多个区域复制数据的权限。完成后，选择保存以保存更改。

API

要以编程方式更新数据湖的区域设置，请使用 Security Lake API 的UpdateDataLake操作。如果您使用的是 AWS CLI，请运行该update-data-lake命令。对于 `region` 参数，请指定您要更改设置的区域的区域代码。例如，`us-east-1` 表示美国东部（弗吉尼亚州北部）区域。有关区域代码的列表，请参阅《AWS 一般参考》中的 Amazon Security Lake 端点。

使用其他参数为要更改的每个设置指定新值，例如，加密密钥 (`encryptionConfiguration`) 和留存设置 (`lifecycleConfiguration`)。

例如，以下 AWS CLI 命令更新该`us-east-1`区域的数据过期和存储类别转换设置。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

配置汇总区域

汇总区域整合了来自一个或多个数据提供区域的数据。指定汇总区域可以帮助您遵守区域合规性要求。

在添加汇总区域之前，您首先需要在 AWS Identity and Access Management (IAM) 中创建两个不同的角色：

- 用于数据复制的 IAM 角色
- 用于注册 AWS Glue 分区的 IAM 角色

> **Note**
>
> 当您使用 Security Lake 控制台时，Security Lake 会代您创建这些 IAM 角色或使用现有角色。但是，在使用 Security Lake API 时必须创建这些角色或 AWS CLI。

用于数据复制的 IAM 角色

此 IAM 角色授予 Amazon S3 跨多个区域复制源日志和事件的权限。

要授予这些权限，请创建一个带有前缀 SecurityLake 的 IAM 角色，并将以下示例策略附加到该角色。在 Security Lake 中创建汇总区域时，您需要该角色的 Amazon 资源名称 (ARN)。在此策略中，sourceRegions 是数据提供区域，destinationRegions 是汇总区域。

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

将以下信任策略附加到您的角色，以便允许 Amazon S3 代入该角色：

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

如果您使用 AWS Key Management Service (AWS KMS) 中的客户托管密钥来加密您的 Security Lake 数据湖，则除了数据复制策略中的权限外，还必须授予以下权限。

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

有关复制角色的更多信息，请参阅《Amazon 简单存储服务用户指南》中的设置权限。

用于注册 AWS Glue 分区的 IAM 角色

此 IAM 角色授予对 Security Lake 使用的分区更新程序 AWS Lambda 功能的权限，该功能用于为从其他区域复制的 S3 对象注册 AWS Glue 分区。如果不创建此角色，订阅用户就无法从这些对象中查询事件。

要授予这些权限，请创建一个名为 AmazonSecurityLakeMetaStoreManager 的角色（您可能已在启用 Security Lake 时创建了此角色）。有关此角色的更多信息，包括示例策略，请参阅步骤 1：创建 IAM 角色。

在 Lake Formation 控制台中，您还必须按照以下步骤向 `AmazonSecurityLakeMetaStoreManager` 授予数据湖管理员的权限：

1. 打开 Lake Formation 控制台：https://console.aws.amazon.com/lakeformation/。
2. 以管理用户的身份登录。
3. 如果显示欢迎使用 Lake Formation 窗口，请选择您在步骤 1 中创建或选择的用户，然后选择“开始”。
4. 如果没有看到欢迎使用 Lake Formation 窗口，请执行以下步骤来配置 Lake Formation 管理员。
    1. 在导航窗格的权限下，选择管理角色和任务。在数据湖管理员部分，选择选择管理员。
    2. 在管理数据湖管理员对话框中，对于 IAM 用户和角色，选择您创建AmazonSecurityLakeMetaStoreManager的 IAM 角色，然后选择保存。

有关更改数据湖管理员权限的更多信息，请参阅 AWS Lake Formation 开发人员指南中的创建数据湖管理员。

添加汇总区域

选择您的首选访问方式，然后按照以下步骤添加汇总区域。

> **Note**
>
> 一个区域可以向多个汇总区域提供数据。但是，一个汇总区域无法向其他汇总区域提供数据。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中的设置下，选择汇总区域。
3. 选择修改，然后选择添加汇总区域。
4. 指定汇总区域以及数据提供区域。如果要添加多个汇总区域，请重复此步骤。
5. 如果这是您首次添加汇总区域，对于服务访问权限，请创建一个新的 IAM 角色或使用现有 IAM 角色向 Security Lake 授予跨多个区域复制数据的权限。
6. 完成后，选择保存。

您也可以在启用 Security Lake 时添加汇总区域。有关更多信息，请参阅 Amazon Security Lake 入门。

API

要以编程方式添加汇总区域，请使用 Security Lake API 的UpdateDataLake操作。如果您使用的是 AWS CLI，请运行该update-data-lake命令。在您的请求中，使用 `region` 字段指定要向汇总区域提供数据的区域。在`replicationConfiguration`参数`regions`数组中，为每个汇总区域指定区域代码。有关区域代码的列表，请参阅 AWS 一般参考 中的 Amazon Security Lake 端点。

例如，以下命令设置`ap-northeast-2`为汇总区域。该`us-east-1`地区将向该`ap-northeast-2`地区提供数据。此示例还为添加到数据湖中的对象设定了 365 天的过期期。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

您也可以在启用 Security Lake 时添加汇总区域。为此，请使用CreateDataLake操作（或者，如果使用 AWS CLI，则使用create-data-lake命令）。有关在入职期间配置汇总区域的更多信息，请参阅。Amazon Security Lake 入门

更新或移除汇总区域

选择您的首选访问方式，然后按照以下步骤更新或移除 Security Lake 中的汇总区域。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中的设置下，选择汇总区域。
3. 选择 Modify(修改)。
4. 要更改汇总区域的数据提供区域，请在汇总区域行中指定更新后的数据提供区域。
5. 要移除汇总区域，请在汇总区域行中选择移除。
6. 完成后，选择保存。

API

要以编程方式配置汇总区域，请使用 Security Lake API 的UpdateDataLake操作。如果您使用的是 AWS CLI，请运行该update-data-lake命令。在您的请求中，使用支持的参数指定汇总区域设置：

- 要添加数据提供区域，请使用 `region` 字段为要添加的区域指定区域代码。在 `replicationConfiguration` 对象的 `regions` 阵列中，为每个要向其提供数据的汇总区域指定区域代码。有关区域代码的列表，请参阅 AWS 一般参考 中的 Amazon Security Lake 端点。
- 要移除数据提供区域，请使用 `region` 字段为要移除的区域指定区域代码。对于 `replicationConfiguration` 参数，请勿指定任何值。

例如，以下命令将`us-east-1`和配置`us-east-2`为贡献区域。两个区域都将向`ap-northeast-3`汇总区域提供数据。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

Amazon Security Lake 中的来源管理

来源是单个系统中生成的与 开放式网络安全架构框架 (OCSF) 架构中的特定事件类相匹配的日志和事件。Amazon Security Lake 可以从各种来源收集日志和事件，包括原生支持的 AWS 服务 和第三方自定义来源。

Security Lake 可以对原始来源数据执行提取、转换和加载 (ETL) 任务，并将数据转换为 Apache Parquet 格式和 OCSF 架构。处理之后，Security Lake 会将来源数据存储在生成数据的 AWS 区域 内的 AWS 账户中的 Amazon Simple Storage Service (Amazon S3) 存储桶内。Security Lake 会为启用 Amazon S3 服务的每个区域创建一个不同的 Amazon S3 存储桶。每个来源在 S3 存储桶中都有一个单独的前缀，而 Security Lake 会将来自每个来源的数据整理到一组单独的 AWS Lake Formation 表中。

主题

从中收集数据 AWS 服务

Amazon Security Lake 可以从以下原生支持的 AWS 服务中收集日志和事件：

- AWS CloudTrail 管理和数据事件（S3、Lambda）
- 亚马逊 Elastic Kubernetes Service（亚马逊 EKS）审核日志
- Amazon Route 53 resolver 查询日志
- AWS Security Hub 调查结果
- Amazon Virtual Private Cloud (Amazon VPC) 流日志

Security Lake 会自动将这些数据转换为开放式网络安全架构框架 (OCSF) 和 Apache Parquet 格式。

> **Tip**
>
> 要将上述一项或多项服务添加为 Security Lake 中的日志源，除了 CloudTrail 管理事件外，无需在这些服务中单独配置日志记录。如果您在这些服务中配置了日志记录，那么您无需更改日志记录配置即可将其添加为 Security Lake 中的日志源。Security Lake 会通过独立且重复的事件流直接从这些服务中拉取数据。

先决条件：验证权限

要将 AWS 服务 作为来源添加到 Security Lake 中，您必须拥有必要的权限。验证附加到您用于添加源的角色的 AWS Identity and Access Management (IAM) 策略是否有权执行以下操作：

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

建议该角色具有以下条件和资源范围，且s3:PutObject具有S3:getObject和权限。

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

这些操作允许您从收集日志和事件，并将它们发送到正确的 AWS Glue 数据库和表。 AWS 服务

如果您使用 AWS KMS 密钥对数据湖进行服务器端加密，则还需要获得权限。`kms:DescribeKey`

CloudTrail 事件日志

AWS CloudTrail 为您提供账户的 AWS API 调用历史记录，包括使用、 AWS 软件开发工具包 AWS Management Console、命令行工具和某些 AWS 服务进行的 API 调用。 CloudTrail 还允许您识别哪些用户和账户为支持的服务调用了 AWS API CloudTrail、发出呼叫的源 IP 地址以及调用的发生时间。有关更多信息，请参阅《AWS CloudTrail 用户指南》。

Security Lake 可以收集与 S3 和 Lambda 的 CloudTrail 管理事件和 CloudTrail 数据事件相关的日志。CloudTrail 管理事件、S3 数据事件和 Lambda 数据事件是安全湖中的三个独立来源。因此，当您将其中一个添加为摄取日志源时，它们的 `sourceName` 会显示不同的值。管理事件（也称为控制平面事件）可让您深入了解对中的资源执行的管理操作 AWS 账户。 CloudTrail 数据事件，也称为数据平面操作，显示对您的资源或资源内部执行的资源操作 AWS 账户。这些操作通常是大规模活动。

要在 Security Lake 中收集 CloudTrail 管理事件，您必须至少有一个用于收集读取和写入 CloudTrail 管理事件的 CloudTrail多区域组织跟踪。您必须为该跟踪启用日志记录。如果您在其他服务中配置了日志记录，那么您无需更改日志记录配置即可将其添加为 Security Lake 中的日志源。Security Lake 会通过独立且重复的事件流直接从这些服务中拉取数据。

多区域跟踪可将多个区域的日志文件传输到单个 AWS 账户的单个 Amazon Simple Storage Service (Amazon S3) 桶中。如果您已经通过 CloudTrail 控制台或管理了多区域跟踪 AWS Control Tower，则无需采取进一步的操作。

- 有关创建和管理通过跟踪的信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》中的为组织创建跟踪。
- 有关创建和管理通过跟踪的信息 AWS Control Tower，请参阅《AWS Control Tower 用户指南》AWS CloudTrail中的使用记录 AWS Control Tower 操作。

当您将 CloudTrail 事件添加为来源时，Security Lake 会立即开始收集您的 CloudTrail 事件日志。它 CloudTrail 通过独立且重复的事件流直接使用 CloudTrail 管理和数据事件。

Security Lake 不会管理您的 CloudTrail 事件，也不会影响您的现有 CloudTrail 配置。要直接管理 CloudTrail 事件的访问和保留，必须使用 CloudTrail 服务控制台或 API。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的使用 CloudTrail 事件历史记录查看事件。

以下列表提供了指向映射参考的 GitHub 存储库链接，以了解 Security Lake 如何将 CloudTrail 事件标准化为 OCSF。

GitHub OCSF 事件存储库 CloudTrail

- 源版本 1 (v1.0.0-rc.2)
- 源代码版本 2 (v1.1.0)

亚马逊 EKS 审核日志

当您将 Amazon EKS 审计日志添加为来源时，Security Lake 会开始收集有关在弹性 Kubernetes 服务 (EKS) 集群中运行的 Kubernetes 资源上执行的活动的深入信息。EKS 审核日志可帮助您在 Amazon Elastic Kubernetes Service 中检测您的 EKS 集群中可能存在的可疑活动。

Security Lake 通过独立且重复的审计日志流直接使用 Amazon EKS 控制平面日志记录功能中的 EKS 审核日志事件。此过程不需要任何其他设置，也不影响您可能拥有的任何现有 Amazon EKS 控制面板日志配置。有关更多信息，请参阅《Amazon EKS 用户指南》中的 Amazon EKS 控制面板日志。

有关 Security Lake 如何将 EKS 审核日志事件标准化为 OCSF 的信息，请参阅 GitHub OCSF 存储库中有关 Amazon EKS 审核日志事件的映射参考。

Route 53 Resolver 查询日志

Route 53 Resolver 查询日志可以跟踪由 Amazon Virtual Private Cloud (Amazon VPC) 中的资源进行的 DNS 查询。这可以帮助您了解应用程序的运行情况并发现安全威胁。

在 Security Lake 中添加 Route 53 Resolver 查询日志作为来源时，Security Lake 会立即开始通过独立且重复的事件流直接从 Route 53 收集 Resolver 查询日志。

Security Lake 不会管理您的 Route 53 日志，也不会影响现有的 Resolver 查询日志配置。要管理 Resolver 查询日志，您必须使用 Route 53 服务控制台。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的管理 Resolver 查询日志记录配置。

以下列表提供了指向映射参考的 GitHub 存储库链接，以了解 Security Lake 如何将 Route 53 日志标准化为 OCSF。

GitHub 存放 Route 53 日志的 OCSF 存储库

- 源版本 1 (v1.0.0-rc.2)
- 源代码版本 2 (v1.1.0)

Security Hub 调查发现

Security Hub 的调查结果可帮助您了解自己的安全状况， AWS 并允许您根据安全行业标准和最佳实践检查您的环境。Security Hub 从各种来源收集调查结果，包括与其他第三方产品集成的集成 AWS 服务，以及对照 Security Hub 控制措施进行检查。Security Hub 以一种名为 AWS 安全调查结果格式 (ASFF) 的标准格式处理调查结果。

当您在 Security Lake 中添加 Security Hub 调查发现作为来源时，Security Lake 会立即开始通过独立且重复的事件流直接从 Security Hub 收集您的调查发现。Security Lake 还会将调查发现从 ASFF 转换为开放式网络安全架构框架 (OCSF) (OCSF)。

Security Lake 不会管理您的 Security Hub 调查发现，也不会影响您的 Security Hub 设置。要管理 Security Hub 的调查结果，必须使用 Security Hub 服务控制台、API 或 AWS CLI。有关更多信息，请参阅《AWS Security Hub 用户指南》中的 AWS Security Hub中的调查发现。

以下列表提供了指向映射参考的 GitHub 存储库链接，以了解 Security Lake 如何将 Security Hub 的调查结果标准化为 OCSF。

GitHub OCSF 存储库，用于存放 Security Hub 调查结果

- 源版本 1 (v1.0.0-rc.2)
- 源代码版本 2 (v1.1.0)

Amazon VPC 流日志

Amazon VPC 的 VPC 流日志功能可以捕获环境中进出网络接口的 IP 流量信息。

当您在 Security Lake 中添加 VPC 流日志作为来源时，Security Lake 会立即开始收集 VPC 流日志。它通过独立且重复的流日志流直接从 Amazon VPC 获取 VPC 流日志。

Security Lake 不会管理您的 VPC 流日志，也不会影响您的 Amazon VPC 配置。要管理流日志，您必须使用 Amazon VPC 服务控制台。有关更多信息，请参阅《Amazon VPC 开发人员指南》中的使用流日志。

以下列表提供了指向映射参考的 GitHub 存储库链接，以了解 Security Lake 如何将 VPC 流日志标准化为 OCSF。

GitHub 用于 VPC 流日志的 OCSF 存储库

- 源版本 1 (v1.0.0-rc.2)

- 源代码版本 2 (v1.1.0)

将添加 AWS 服务 为来源

添加 AWS 服务 为源后，Security Lake 会自动开始从中收集安全日志和事件。这些说明告诉你如何在 Security Lake 中添加原生支持的 AWS 服务 源代码。有关添加自定义源的说明，请参阅从自定义源收集数据。

Console

添加 AWS 日志源（控制台）

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 从导航窗格中选择来源。
3. 选择 AWS 服务 要从中收集数据的，然后选择配置。
4. 在源设置部分，启用源并选择要用于数据摄取的数据源的版本。默认情况下，最新版本的数据源由 Security Lake 摄取。

   > **Important**
   >
   > 如果您没有在指定区域启用新版本 AWS 日志源所需的角色权限，请联系您的 Security Lake 管理员。有关更多信息，请参阅更新角色权限。

   要让订阅者获取所选版本的数据源，您还必须更新订阅者设置。有关如何编辑订阅者的详细信息，请参阅 Amazon Security Lake 中的订阅者管理。

   或者，您可以选择仅采集最新版本，并禁用所有以前用于数据摄取的源版本。
5. 在 “区域” 部分中，选择要为源收集数据的区域。Security Lake 将从所选区域中的所有账户的来源收集数据。
6. 选择启用。

API

添加 AWS 日志源 (API)

要以编程方式将添加 AWS 服务 为源，请使用 Security Lake API 的CreateAwsLogSource操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该create-aws-log-

source命令。sourceName 和 regions 参数是必需的。或者，您可以将来源的范围限制为特定accounts或特定sourceVersion。

> **Important**
>
> 当你没有在命令中提供参数时，Security Lake 会假设缺少的参数指的是整个参数集。例如，如果您未提供accounts参数，则该命令将应用于组织中的整组账户。

以下示例将 VPC 流日志添加为指定账户和区域中的来源。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

> **Note**
>
> 如果您将此请求应用于尚未启用 Security Lake 的区域，则会收到一条错误消息。您可以通过在该区域启用 Security Lake 或使用regions参数仅指定已启用 Security Lake 的区域来解决此错误。

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

更新角色权限

如果您没有所需的角色权限或资源（新 AWS Lambda 函数和 Amazon Simple Queue Service (Amazon SQS) Simple Queue Service 队列），无法从新版本的数据源摄取数据，则必须更新角色权限并创建一组新的资源来处理来自AmazonSecurityLakeMetaStoreManagerV2您的源的数据。

选择您的首选方法，然后按照说明更新您的角色权限并创建新资源来处理来自指定区域中新版本 AWS 日志源的数据。这是一次性操作，因为权限和资源会自动应用于 future 的数据源版本。

Console

更新角色权限（控制台）

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

使用委派 Security Lake 管理员的凭证进行登录。

2. 在导航窗格中的设置下，选择常规。
3. 选择 “更新角色权限”。
4. 在 “服务访问权限” 部分，执行以下任一操作：
   - 创建和使用新的服务角色-您可以使用由 Security Lake 创建的 AmazonSecurityLakeMetaStoreManagerV2 角色。
   - 使用现有的服务角色-您可以从服务角色名称列表中选择现有的服务角色。
5. 选择 应用。

API

更新角色权限 (API)

要以编程方式更新权限，请使用 Security Lake API 的UpdateDataLake操作。要使用更新权限 AWS CLI，请运行update-data-lake命令。

要更新您的角色权限，您必须将AmazonSecurityLakeMetastoreManager策略附加到该角色。

删除 AmazonSecurityLakeMetaStoreManager 角色

> **Important**
>
> 将角色权限更新为后AmazonSecurityLakeMetaStoreManagerV2，请先确认数据湖是否正常运行，然后再移除旧AmazonSecurityLakeMetaStoreManager角色。建议至少等待 4 小时后再移除该角色。

如果您决定移除该角色，则必须先从中删除该AmazonSecurityLakeMetaStoreManager角色 AWS Lake Formation。

按照以下步骤从 Lake Formation 控制台中移除该AmazonSecurityLakeMetaStoreManager角色。

1. 登录并打开 Lake AWS Management Console Formation 控制台，网址为 https://console.aws.amazon.com/lakeformation/。
2. 在 Lake Formation 控制台的导航窗格中，选择管理角色和任务。

3. AmazonSecurityLakeMetaStoreManager从每个区域中移除。

移除 AWS 服务 作为来源的

选择您的访问方法，然后按照以下步骤删除原生支持的 Security L AWS 服务 ake 源。您可以移除一个或多个区域的来源。移除来源后，Security Lake 将停止从指定区域和账户中的来源收集数据，订阅用户也无法再从来源获取新数据。但是，订阅用户仍然可以获取 Security Lake 在该来源被移除之前从中收集的数据。您只能使用这些说明删除原生支持的源代码 AWS 服务 。有关移除自定义来源的更多信息，请参阅从自定义源收集数据。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 从导航窗格中选择来源。
3. 选择一个来源，然后选择禁用。
4. 选择要停止从该来源收集数据的一个或多个区域。Security Lake 将停止从所选区域中的所有账户的来源收集数据。

API

要以编程方式将 AWS 服务 作为来源删除，请使用 Security Lake API 的DeleteAwsLogSource操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该delete-aws-log-source命令。sourceName 和 regions 参数是必需的。或者，您可以将移除范围限制为特定accounts或特定sourceVersion。

> **Important**
>
> 当你没有在命令中提供参数时，Security Lake 会假设缺少的参数指的是整个参数集。例如，如果您未提供accounts参数，则该命令将应用于组织中的整组账户。

以下示例删除了指定账户和区域中的 VPC 流日志作为来源。

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

以下示例删除了指定账户和区域中作为来源的 Route 53。

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

前面的示例是针对 Linux、macOS 或 Unix 进行格式化的，它们使用反斜杠 (\) 行继续符来提高可读性。

获取来源集合的状态

选择您的访问方式，然后按照步骤获取当前区域中启用日志收集的账户和来源的快照。

Console

获取当前区域中日志收集的状态

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格上，选择 “帐户”。
3. 将光标悬停在 “来源” 列中的数字上，查看为所选账户启用了哪些日志。

API

要获取当前区域中日志收集的状态，请使用 Security Lake API 的GetDataLakeSources操作。如果您使用的是 AWS CLI，请运行该get-data-lake-sources命令。对于`accounts`参数，您可以将一个或多个 AWS 账户 ID 指定为列表。如果您的请求成功，Security Lake 将返回当前区域中这些账户的快照，包括 Security Lake 正在从哪些 AWS 来源收集数据以及每个来源的状态。如果您不包含`accounts`参数，则响应将包含当前区域中配置了 Security Lake 的所有账户的日志收集状态。

例如，以下 AWS CLI 命令检索当前区域中指定账户的日志收集状态。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

从自定义源收集数据

Amazon Security Lake 可以从自定义的第三方源收集安全日志和事件。对于每个自定义源，Security Lake 会进行以下处理：

- 为 Amazon S3 存储桶中的源提供一个唯一前缀。
- 在 AWS Identity and Access Management (IAM) 中创建允许自定义源向数据湖写入数据的角色。此角色的权限边界由名为的 AWS 托管策略设置AmazonSecurityLakePermissionsBoundary。
- 创建一个 AWS Lake Formation 表来整理源写入 Security Lake 的对象。
- 设置 AWS Glue 搜寻器来对源数据进行分区。爬虫 AWS Glue Data Catalog 用表格填充。它还会自动发现新的源数据并提取架构定义。

要向 Security Lake 添加自定义源，必须满足以下要求：

1. 目标 – 自定义源必须能够将数据作为一组 S3 对象写入 Security Lake，这些对象位于分配给该源的前缀之下。对于包含多个类别数据的源，您应将每个唯一的开放网络安全架构框架（OCSF）事件类作为单独的源提供。Security Lake 会创建一个 IAM 角色，该角色允许自定义源向您的 S3 存储桶中的指定位置进行写入。

   > **Note**
   >
   > 使用 OCSF 验证工具验证自定义源是否与OCSF Schema 1.1兼容。

2. 格式 – 从自定义源收集的每个 S3 对象都应格式化为 Apache Parquet 文件。
3. 架构 – 相同的 OCSF 事件类应该应用于 Parquet 格式的对象中的每条记录。

摄取自定义源的最佳实践

为提高数据处理和查询效率，建议在向 Security Lake 添加自定义源时遵循以下最佳实践：

分区

对象应按源位置、 AWS 区域 AWS 账户、和日期进行分区。分区数据路径的格式为 *bucket-name*/*source-location*/region=*region*/accountId=*accountID*/eventDay=*YYYYMMDD*。

一个分区示例是 aws-security-data-lake-*us-west-2-lake-uid*/*source-location*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/。

- bucket-name – Security Lake 用来存储自定义源数据的 Amazon S3 存储桶的名称。
- source-location – S3 存储桶中自定义源的前缀。Security Lake 将给定源的所有 S3 对象存储在该前缀下，并且该前缀对于给定源是唯一的。
- region— AWS 区域 向其中写入数据。
- accountId— 源分区中记录所属的 AWS 账户 ID。
- eventDay – 事件发生的日期，格式为八个字符的字符串 (YYYYMMDD)。

对象大小和速率

写入到 Security Lake 的对象应将记录缓冲 5 分钟。如果缓冲期内的数据过多，导致无法有效查询，则自定义源可以在 5 分钟时限内写入多条记录，前提是这些文件的平均大小保持在 256MB 以下。吞吐量较低的自定义源可以每 5 分钟写入一次较小的对象，以保持 5 分钟的摄取延迟，并可以将记录缓冲更长时间。

Parquet 设置

Security Lake 支持 Parquet 版本 1.x 和 2.x。数据页大小应限制为 1MB（未压缩）。行组大小不应超过 256MB（已压缩）。要在 Parquet 对象内进行压缩，首选 zstandard。

排序

在每个 Parquet 格式的对象中，记录应按时间排序，以降低查询数据的成本。

添加自定义源的先决条件

添加自定义源时，Security Lake 会创建一个 IAM 角色，该角色允许该源将数据写入到数据湖中的正确位置。角色的名称遵循格式AmazonSecurityLake-Provider-{name of the custom source}-{region}，其中region是 AWS 区域 您添加自定义源的格式。Security Lake 将向该角色附加允许访问数据湖的策略。如果您使用客户管理的 AWS KMS 密钥对数据湖进行了加密，Security Lake 还会为该角色附加策略kms:Decrypt和kms:GenerateDataKey权限。此角色的权限边界由名为的 AWS 托管策略设置AmazonSecurityLakePermissionsBoundary。

主题

- 验证权限
- 创建 IAM 角色以允许对 Security Lake 存储桶位置进行写入访问（ AWS CLI仅限 API 和步骤）

验证权限

在添加自定义源之前，请验证您是否具有执行以下操作的权限。

要验证您的权限，请使用 IAM 查看附加到 IAM 身份的 IAM 策略。然后，将这些策略中的信息与以下操作列表（您必须被允许执行这些操作才能添加自定义源）进行比较。

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

这些操作允许您从自定义来源收集日志和事件，将其发送到正确的 AWS Glue 数据库和表，并将其存储在 Amazon S3 中。

如果您使用 AWS KMS 密钥对数据湖进行服务器端加密，则还需要获得`kms:CreateGrant`、`kms:DescribeKey`和`kms:GenerateDataKey`的权限。

> **Important**
>
> 如果您打算使用 Security Lake 控制台添加订阅用户，可以跳过下一步，继续执行添加自定义源。Security Lake 控制台提供了简化的入门流程，可以为您创建所有必要的 IAM 角色或使用现有角色。
>
> 如果您计划使用 Security Lake API 或 AWS CLI 添加订阅者，请继续执行下一步创建 IAM 角色以允许对 Security Lake 存储桶位置进行写入访问。

创建 IAM 角色以允许对 Security Lake 存储桶位置进行写入访问（ AWS CLI仅限 API 和步骤）

如果您正在使用 Security Lake API 或 AWS CLI 添加自定义源，请添加此 IAM 角色以授予对您的自定义源数据进行爬网和识别数据分区的 AWS Glue 权限。这些分区是整理数据以及在 Data Catalog 中创建和更新表所必需的。

创建此 IAM 角色后，您需要该角色的 Amazon 资源名称（ARN）才能添加自定义源。

您必须附加`arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS 托管策略。

要授予必要的权限，您还必须在角色中创建并嵌入以下内联策略， AWS Glue 爬网程序 以允许从自定义源读取数据文件并在 AWS Glue 数据目录中创建/更新表。

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

附上以下信任策略 AWS 账户 以允许使用该策略根据外部 ID 代入角色：

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

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

如果您要添加自定义源的区域中的 S3 存储桶是使用客户管理的加密的 AWS KMS key，则还必须将以下策略附加到该角色和您的 KMS 密钥策略：

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

添加自定义源

创建用于调用 AWS Glue 爬虫的 IAM 角色后，请按照以下步骤在 Security Lake 中添加自定义源。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中创建自定义源的区域。
3. 在导航窗格中选择自定义来源，然后选择创建自定义来源。
4. 在自定义来源详细信息部分，为自定义源输入一个全局唯一名称。然后，选择一个 OCSF 事件类，它描述了自定义源将发送到 Security Lake 的数据类型。
5. 对于拥有写入数据权限的AWS 账户 ，输入将把日志和事件写入到数据湖的自定义源的 AWS 账户 ID 和外部 ID。

6. 对于服务访问权限，创建并使用新的服务角色，或使用向 Security Lake 授予调用 AWS Glue 的权限的现有服务角色。
7. 选择 创建。

API

要以编程方式添加自定义源，请使用 Security Lake API 的CreateCustomLogSource操作。使用要创建自定义源代码的 AWS 区域 位置中的操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该create-custom-log-source命令。

在您的请求中，使用受支持的参数为自定义源指定配置设置：

- `sourceName`— 为源指定名称。该名称必须是区域中唯一的值。
- `eventClasses`— 指定一个或多个 OCSF 事件类来描述源将发送到 Security Lake 的数据类型。有关 Security Lake 中支持作为源的 OCSF 事件类的列表，请参阅开放网络安全架构框架 (OCSF)。
- `sourceVersion`— （可选）指定一个值，将日志收集限制为特定版本的自定义源数据。
- `crawlerConfiguration`— 指定您为调用爬网程序而创建的 IAM 角色的 Amazon 资源名称 (ARN)。 AWS Glue 有关创建 IAM 角色的详细步骤，请参阅添加自定义源的先决条件
- `providerIdentity`— 指定源将用于向数据湖写入日志和事件的 AWS 身份和外部 ID。

以下示例在指定区域的指定日志提供者账户中添加自定义源作为日志源。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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”]
```

更新自定义源数据 AWS Glue

在 Security Lake 中添加自定义来源后，Security Lake 会创建一个 AWS Glue 爬虫。该爬网程序将连接到您的自定义源，确定数据结构，然后用表填充 AWS Glue Data Catalog。

我们建议您手动运行该爬网程序，以确保自定义源的架构保持最新，并维护 Athena 和其他查询服务中的查询功能。具体来说，如果自定义源的输入数据集中发生以下任一变化，您就应该运行该爬网程序：

- 数据集有一个或多个新的顶级列。
- 数据集在具有 `struct` 数据类型的列中有一个或多个新字段。

有关运行爬虫的说明，请参阅《AWS Glue 开发者指南》中的安排 AWS Glue 爬网程序。

Security Lake 无法删除或更新您账户中的现有爬网程序。如果您删除一个自定义源并计划在将来创建同名的自定义源，我们建议您删除关联的爬网程序。

删除自定义源

删除自定义源可以停止将数据从该源发送到 Security Lake。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 使用页面右上角的 AWS 区域 选择器，选择要从中移除自定义来源的区域。
3. 在导航窗格中，选择自定义来源。
4. 选择要删除的自定义源。
5. 选择取消注册自定义来源，然后选择删除以确认操作。

API

要以编程方式删除自定义源，请使用 Security Lake API 的DeleteCustomLogSource操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该delete-custom-log-source命令。在要删除自定义源的 AWS 区域 中使用该操作。

在您的请求中，使用 `sourceName` 参数指定要删除的自定义源的名称。也可以指定自定义源的名称，然后使用 `sourceVersion` 参数将删除范围限制为自定义源中特定版本的数据。

以下示例从 Security Lake 中删除自定义日志源。

此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

Amazon Security Lake 中的订阅用户管理

Amazon Security Lake 订阅用户可以使用来自 Security Lake 的日志和事件。为了控制成本并遵循最低权限访问最佳实践，您可以按来源为订阅用户提供对数据的访问权限。更多有关来源的信息，请参阅 Amazon Security Lake 中的来源管理。

Security Lake 支持两种类型的订阅用户访问：

- 数据访问：当某个来源的新 Amazon S3 对象被写入 Security Lake 数据湖时，订阅用户会收到有关这些对象的通知。订阅用户可以通过订阅端点或通过轮询某个 Amazon Simple Queue Service (Amazon SQS) 队列来直接访问 S3 对象并接收有关新对象的通知。此订阅类型`S3`在 CreateSubscriberAPI 的`accessTypes`参数中标识。
- 查询访问权限 — 订阅者使用诸如 Amazon Athena 之类的服务来查询 S3 存储桶中 AWS Lake Formation 表中的源数据。此订阅类型`LAKEFORMATION`在 CreateSubscriberAPI 的`accessTypes`参数中标识。

订阅者只能访问您在创建订阅者时选择的中的源数据。 AWS 区域 要允许订阅用户访问多个区域中的数据，您可以将创建订阅用户时所在的区域指定为汇总区域，并让其他区域向其提供数据。有关汇总区域和数据提供区域的更多信息，请参阅管理 区域。

> **Important**
>
> Security Lake 允许每位订阅者添加的最大来源数为 10。这可能是 AWS 来源和自定义来源的组合。

主题

管理 Security Lake 订阅用户的数据访问权限

当数据写入 S3 存储桶时，有权访问 Amazon Security Lake 中的源数据的订阅用户会收到有关该源的新对象的通知。默认情况下，订阅用户会通过他们提供的 HTTPS 端点收到有关新对象的通知。订阅用户还可以通过轮询 Amazon Simple Queue Service (Amazon SQS) 队列收到有关新对象的通知。

创建具有数据访问权限的订阅用户的先决条件

您必须实现以下先决条件才能在 Security Lake 中创建具有数据访问权限的订阅用户。

主题

验证权限

要验证您的权限，请使用 IAM 查看附加到 IAM 身份的 IAM 策略。然后，将这些策略中的信息与以下（权限）操作列表进行比较。在新数据被写入数据湖时，您必须执行这些操作才能通知订阅用户。

您需要获得执行以下操作的权限：

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

除了上表之外，您还需要获得执行以下操作的权限：

- `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

获取订阅用户的外部 ID

要创建订阅者，除了订阅者的 AWS 账户 ID 之外，您还需要获取他们的外部 ID。外部 ID 是订阅用户提供给您的唯一标识符。Security Lake 会将外部 ID 添加到其创建的订阅用户 IAM 角色中。在 Security Lake 控制台中通过 API 或 AWS CLI 创建订阅用户时，您需要使用外部 ID。

有关外部 ID 的更多信息，请参阅 IAM 用户指南中的如何在向第三方授予 AWS 资源访问权限时使用外部 ID。

> **Important**
>
> 如果您打算使用 Security Lake 控制台添加订阅用户，可以跳过下一步，继续执行创建具有数据访问权限的订阅用户。Security Lake 控制台提供了简化的入门流程，可以为您创建所有必要的 IAM 角色或使用现有角色。
>
> 如果您计划使用 Security Lake API 或 AWS CLI 添加订阅者，请继续执行下一步创建用于调用 EventBridge API 目标的 IAM 角色。

创建 IAM 角色以调用 EventBridge API 目标（ AWS CLI仅限 API 和步骤）

如果您通过 API 或使用 Security Lake AWS CLI，请在 AWS Identity and Access Management (IAM) 中创建一个角色，授予亚马逊调用 API 目标和向正确的 HTTPS 终端节点发送对象通知的 EventBridge 权限。

此 IAM 角色创建完成后，您需要提供角色的 Amazon 资源名称 (ARN) 才能创建订阅用户。如果订阅用户轮询某个 Amazon Simple Queue Service (Amazon SQS) 队列中的数据或直接从 AWS Lake Formation 中查询数据，则不需要使用这一 IAM 角色。有关此类型的数据访问方法（访问类型）的更多信息，请参阅管理 Security Lake 订阅用户的查询访问权限。

将以下策略附加到您的 IAM 角色：

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

将以下信任策略附加到您的 IAM 角色 EventBridge 以允许代入该角色：

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

Security Lake 会自动创建一个 IAM 角色，允许订阅用户从数据湖读取数据（或者从 Amazon SQS 队列中轮询事件，如果这是首选的通知方式）。此角色受名为的 AWS 托管策略保护AmazonSecurityLakePermissionsBoundary。

创建具有数据访问权限的订阅用户

选择以下访问方法之一来创建可以访问当前数据的订阅者 AWS 区域。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中创建订阅者的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，选择创建订阅用户。
5. 对于订阅用户详细信息，输入订阅用户名称和可选的描述。

   该区域将自动填充为您当前选择的区域 AWS 区域 ，并且无法修改。
6. 对于日志源和事件来源，选择订阅用户有权使用的来源。
7. 对于数据访问方法，选择 S3，以便为订阅用户设置数据访问权限。
8. 对于订阅者凭证，请提供订阅者的 AWS 账户 ID 和外部 ID。
9. （可选）对于通知详情，如果您想让 Security Lake 创建一个 Amazon SQS 队列供订阅用户轮询以便获得对象通知，请选择 SQS 队列。如果您希望 Security Lake 向 HTTPS 终端节点发送通知，请选择订阅终端节点。 EventBridge

   如果选择订阅端点，您还要执行以下操作：

   a. 输入订阅端点。有效端点格式的示例为 **`http://example.com`**。您也可以选择提供 HTTPS 密钥名称和 HTTPS 密钥值。

   b. 对于服务访问权限，请创建新的 IAM 角色或使用现有 IAM 角色来 EventBridge授予调用 API 目的地和向正确的终端节点发送对象通知的权限。

      有关创建新 IAM 角色的信息，请参阅创建 IAM 角色以调用 EventBridge API 目标。
10. （可选）对于标签，最多输入 50 个要分配给订阅用户的标签。

    标签是您可以为某些类型的 AWS 资源定义和分配的标签。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理各种资源。要了解更多信息，请参阅为 Amazon Security Lake 资源添加标签。

11. 选择创建。

API

要以编程方式创建具有数据访问权限的订阅者，请使用 Security Lake API 的CreateSubscriber操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 create-subscriber 命令。

在您的请求中，使用这些参数为订阅者指定以下设置：

- 对于 `sources`，请指定您希望订阅用户访问的每个来源。
- 对于`subscriberIdentity`，请指定订阅者用于访问源数据的 AWS 帐户 ID 和外部 ID。
- 对于`subscriber-name`，请指定订阅者的名称。
- 对于 `accessTypes`，请指定 S3。

示例 1

以下示例创建了一个订阅者，该订阅者可以访问当前 AWS 区域中针对某个 AWS 源的指定订阅者身份的数据。

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

示例 2

以下示例创建了一个订阅者，该订阅者可以访问当前 AWS 区域中自定义源的指定订阅者身份。

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

前面的示例是针对 Linux、macOS 或 Unix 进行格式化的，它们使用反斜杠 (\) 行继续符来提高可读性。

（可选）创建订阅者后，使用CreateSubscriberNotification操作来指定当您希望订阅者访问的源有新数据写入数据湖时，如何通知订阅者。如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该create-subscriber-notification命令。

- 要覆盖默认通知方式（HTTPS 端点）并创建 Amazon SQS 队列，请指定 `sqsNotificationConfiguration` 参数的值。
- 如果您更喜欢使用 HTTPS 端点发送通知，请指定 `httpsNotificationConfiguration` 参数的值。
- `targetRoleArn`在该字段中，指定您为调用 EventBridge API 目标而创建的 IAM 角色的 ARN。

```
$ 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"}
```

要获取`subscriberID`，请使用 Security Lake API 的ListSubscribers操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 list-subscriber 命令。

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

要随后更改订阅者的通知方式（Amazon SQS 队列或 HTTPS 终端节点），请使用UpdateSubscriberNotification操作，或者，如果您使用的是 AWS CLI，则运行命令。update-subscriber-notification您也可以使用 Security Lake 控制台更改通知方式：在订阅用户页面上选择订阅用户，然后选择编辑。

对象通知消息示例

```
{
  "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"
  }
}
```

更新数据订阅用户

您可以通过更改订阅用户的访问来源来更新订阅用户。您也可以为订阅用户分配或编辑标签。标签是您可以定义并分配给某些类型的 AWS 资源（包括订阅者）的标签。要了解更多信息，请参阅为 Amazon Security Lake 资源添加标签。

请选择一种访问方式，然后按照以下步骤为现有订阅定义新的来源。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中选择订阅用户。
3. 选择订阅用户。
4. 选择编辑，然后执行以下任一操作：
   - 要更新订阅用户的来源，请在日志和事件来源部分输入新设置。
   - 要为订阅用户分配或编辑标签，请在标签部分根据需要更改标签。
5. 完成后，选择保存。

API

要以编程方式更新订阅者的数据访问源，请使用 Security Lake API 的UpdateSubscriber操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 update- subscriber 命令。在您的请求中，使用 `sources` 参数指定您希望订阅用户访问的每个来源。

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

要查看与特定 AWS 账户 或组织关联的订阅者列表，请使用ListSubscribers操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行列表订阅者命令。

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

要查看特定订阅者的当前设置，请使用GetSubscriber操作。运行 get- subscriber 命令。然后，Security Lake 会返回订阅用户的名称和描述、外部 ID 以及其他信息。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 get-subscriber 命令。

要更新订阅者的通知方法，请使用UpdateSubscriberNotification操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行该update-subscriber-notification命令。例如，您可以为订阅用户指定新的 HTTPS 端点，也可以从 HTTPS 端点切换到 Amazon SQS 队列。

移除数据订阅用户

如果您不再希望某个订阅用户访问 Security Lake 中的数据，可以按照以下步骤删除该订阅用户。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中选择订阅用户。
3. 选择想要移除的订阅用户。
4. 选择删除，然后确认操作。这将删除订阅用户和所有关联的通知设置。

API

根据您的场景，执行以下操作之一：

- 要删除订阅者和所有相关的通知设置，请使用 Security Lake API 的DeleteSubscriber操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行删除订阅者命令。
- 要保留订阅者但停止将来向订阅者发送通知，请使用 Security Lake API 的DeleteSubscriberNotification操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 run delete-subscriber-notification命令。

管理 Security Lake 订阅用户的查询访问权限

具有查询权限的订阅用户可以查询 Security Lake 收集的数据。这些订阅者使用诸如 Amazon Athena 之类的服务直接查询您的 S3 存储桶中的 AWS Lake Formation 表。尽管 Security Lake 的主要查询引擎是 Athena，但您也可以使用与 AWS Glue Data Catalog 集成的其他服务，例如 Amazon Redshift Spectrum 和 Spark SQL。

> **Note**
>
> 本部分介绍了如何向第三方订阅用户授予查询访问权限。有关针对自己的数据湖运行查询的信息，请参阅第 4 步：查看和查询自己的数据。

创建具有查询访问权限的订阅用户的先决条件

您必须实现以下先决条件才能在 Security Lake 中创建具有数据访问权限的订阅用户。

主题

- 验证权限
- 创建 IAM 角色以查询 Security Lake 数据（ AWS CLI仅限 API 和步骤）
- 授予 Lake Formation 管理员权限

验证权限

在创建具有查询访问权限的订阅用户之前，请确认您有权执行下列操作。

要验证您的权限，请使用 IAM 查看附加到 IAM 身份的 IAM 策略。然后，将这些策略中的信息与以下操作列表（您必须有权执行这些操作才能创建具有查询访问权限的订阅用户）进行比较。

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

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

> **Important**
>
> 验证权限后：
>
> - 如果您打算使用 Security Lake 控制台添加订阅用户，可以跳过下一步，继续执行授予 Lake Formation 管理员权限。Security Lake 会为您创建所有必要的 IAM 角色或使用现有角色。
> - 如果您准备使用 Security Lake API 或 CLI 添加具有查询访问权限的订阅用户，请继续执行下一步，创建 IAM 角色来查询 Security Lake 数据。

创建 IAM 角色以查询 Security Lake 数据（ AWS CLI仅限 API 和步骤 ）

在使用 Security Lake API 或 AWS CLI 向订阅者授予查询访问权限时，您需要创建一个名为的角色`AmazonSecurityLakeMetaStoreManager`。Security Lake 使用此角色注册 AWS Glue 分区和更新 AWS Glue 表。您可能已经在创建必要的 IAM 角色时创建了此角色。

授予 Lake Formation 管理员权限

您还需要向用于访问 Security Lake 控制台和添加订阅用户的 IAM 角色添加 Lake Formation 管理员权限。

您可以按照以下步骤为您的角色授予 Lake Formation 管理员权限：

1. 打开 Lake Formation 控制台：https://console.aws.amazon.com/lakeformation/。
2. 以管理用户的身份登录。
3. 如果显示欢迎使用 Lake Formation 窗口，请选择您在步骤 1 中创建或选择的用户，然后选择“开始”。
4. 如果没有看到欢迎使用 Lake Formation 窗口，请执行以下步骤来配置 Lake Formation 管理员。

    1. 在导航窗格的权限下，选择管理角色和任务。在数据湖管理员部分，选择选择管理员。

2. 在管理数据湖管理员对话框中，对于 IAM 用户和角色，选择访问 Security Lake 控制台时使用的管理员角色，然后选择保存。

有关更改数据湖管理员权限的更多信息，请参阅 AWS Lake Formation 开发人员指南中的创建数据湖管理员。

IAM 角色必须拥有对您想要向订阅用户授予访问权限的数据库和表的 SELECT 权限。有关如何执行此操作的说明，请参阅 AWS Lake Formation 开发人员指南中的使用命名资源方法授予数据目录权限。

创建具有查询访问权限的订阅用户

选择您的首选方法来创建当前具有查询访问权限的订阅者 AWS 区域。订阅者只能从中 AWS 区域 创建的数据中查询数据。要创建订阅者，您需要拥有订阅者的 AWS 账户 ID 和外部 ID。外部 ID 是订阅用户提供给您的唯一标识符。有关外部 ID 的更多信息，请参阅 IAM 用户指南中的如何在向第三方授予 AWS 资源访问权限时使用外部 ID。

> **Note**
>
> Security Lake 不支持 Lake Formation 跨账户数据共享版本 1。您必须将 Lake Formation 跨账户数据共享更新到版本 2 或版本 3。有关通过 AWS Lake Formation 控制台或 AWS CLI 更新跨账户版本设置的步骤，请参阅AWS Lake Formation 开发者指南中的启用新版本。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   登录委托管理员账户。
2. 使用页面右上角的 AWS 区域 选择器，选择要在其中创建订阅者的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，选择创建订阅用户。
5. 对于订阅用户详细信息，请输入订阅用户名称和可选描述。

   该区域将自动填充为您当前选择的区域 AWS 区域 ，并且无法修改。
6. 对于日志和事件源，请选择您希望 Security Lake 在返回查询结果时包含哪些来源。
7. 对于数据访问方法，请选择 Lake Formation，以便为订阅用户创建查询访问权限。
8. 对于订阅者凭证，请提供订阅者的 AWS 账户 ID 和外部 ID。

9. （可选）对于标签，最多输入 50 个要分配给订阅用户的标签。

   标签是您可以为某些类型的 AWS 资源定义和分配的标签。每个标签都包含一个必需的标签键和一个可选的标签值。标签可以帮助您以不同的方式识别、分类和管理各种资源。要了解更多信息，请参阅为 Amazon Security Lake 资源添加标签。

10. 选择创建。

API

要以编程方式创建具有查询访问权限的订阅者，请使用 Security Lake API 的CreateSubscriber操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 create-subscriber 命令。

在您的请求中，使用这些参数为订阅者指定以下设置：

- 对于 `accessTypes`，请指定 `LAKEFORMATION`。
- 对于 `sources`，请指定您希望 Security Lake 在返回查询结果时包含的每个来源。
- 对于`subscriberIdentity`，请指定订阅者用于查询源数据的 AWS 身份和外部 ID。

以下示例为指定的订阅者身份创建了在当前 AWS 区域具有查询访问权限的订阅者。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

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

设置跨账户表共享（订阅用户步骤）

Security Lake 使用 Lake Formation 跨账户表共享来支持订阅用户的查询访问权限。当您在 Security Lake 控制台、API 或 AWS CLI中创建具有查询权限的订阅者时，Security Lake 会通过在 AWS Resource Access Manager (AWS RAM) 中创建资源共享来与订阅者共享有关相关 Lake Formation 表的信息。

当您对具有查询访问权限的订阅用户进行某些类型的编辑时，Security Lake 会创建一个新的资源共享。有关更多信息，请参阅编辑具有查询访问权限的订阅用户。

订阅用户应按照以下步骤使用您的 Lake Formation 表中的数据：

1. 接受资源共享 – 订阅用户必须接受在您创建或编辑订阅用户时生成的 `resourceShareArn` 和 `resourceShareName` 资源共享。选择以下访问方法之一：
   - 有关控制台和 AWS CLI，请参阅接受来自的资源共享邀请 AWS RAM。
   - 对于 API，请调用 GetResourceShareInvitationsAPI。按 `resourceShareArn` 和 `resourceShareName` 进行筛选，以找到正确的资源共享。AcceptResourceShareInvitation通过 API 接受邀请。

   资源共享邀请会在 12 小时后过期，因此您必须在 12 小时内验证并接受邀请。如果邀请过期，您会看到它处于 `PENDING` 状态，但此时即使您接受邀请也无法访问共享资源。超过 12 小时后，请删除 Lake Formation 订阅用户并重新创建订阅用户，以获得新的资源共享邀请。
2. 创建指向共享表的资源链接 – 订阅用户必须在 AWS Lake Formation （如果使用控制台）或 AWS Glue （如果使用 API/AWS CLI）中创建指向共享 Lake Formation 表的资源链接。此资源链接将订阅用户的账户指向共享表。选择以下访问方法之一：
   - 对于控制台和 AWS CLI，请参阅《AWS Lake Formation 开发人员指南》中的创建指向共享数据目录表的资源链接。
   - 对于 API，请调用 AWS Glue CreateTableAPI。我们建议订阅者还使用 CreateDatabaseAPI 创建唯一的数据库，用于存储资源链接表。
3. 查询共享表 – Amazon Athena 等服务可以直接引用这些表，而 Security Lake 收集的新数据将自动可供查询。查询在订阅者处运行 AWS 账户，查询产生的费用由订阅者计费。您可以在自己的 Security Lake 账户中控制对资源的读取权限。

有关授予跨账户权限的更多信息，请参阅 AWS Lake Formation 开发人员指南中的 Lake Formation 中的跨账户数据共享。

编辑具有查询访问权限的订阅用户

Security Lake 支持对具有查询访问权限的订阅用户进行编辑。您可以编辑订阅者的姓名、描述、外部 ID、主AWS 账户 体 (ID) 以及订阅者能够使用的日志源。请选择您的首选方法，然后按照步骤编辑在当前 AWS 区域中具有查询访问权限的订阅用户。

> **Note**
>
> Security Lake 不支持 Lake Formation 跨账户数据共享版本 1。您必须将 Lake Formation 跨账户数据共享更新到版本 2 或版本 3。有关通过 AWS Lake Formation 控制台或 AWS CLI 更新跨账户版本设置的步骤，请参阅AWS Lake Formation 开发者指南中的启用新版本。

Console

根据您要编辑的详细信息，请仅按照为该操作提供的步骤进行操作。

编辑订阅用户名称

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   登录委托管理员账户。
2. 使用页面右上角的 AWS 区域 选择器，选择要编辑订阅者详细信息的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，使用单选按钮选择要编辑的订阅用户。所选订阅用户的数据访问方式必须为 LAKEFORMATION。
5. 选择编辑。
6. 输入新的订阅用户名称，然后选择保存。

编辑订阅用户描述

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   登录委托管理员账户。
2. 使用页面右上角的 AWS 区域 选择器，选择要编辑订阅者的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，使用单选按钮选择要编辑的订阅用户。所选订阅用户的数据访问方式必须为 LAKEFORMATION。
5. 选择编辑。
6. 为订阅用户输入新描述，然后选择保存。

编辑外部 ID

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   登录委托管理员账户。
2. 使用页面右上角的 AWS 区域 选择器，选择要编辑订阅者详细信息的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，使用单选按钮选择要编辑的订阅用户。所选订阅用户的数据访问方式必须为 LAKEFORMATION。
5. 选择编辑。
6. 输入订阅用户提供的新外部 ID，然后选择保存。

   保存新的外部 ID 会自动删除以前的 AWS RAM 资源共享，并为订阅者创建新的资源共享。
7. 订阅用户必须按照设置跨账户表共享（订阅用户步骤）中的步骤 1 接受新的资源共享。确保订阅用户详细信息中显示的 Amazon 资源名称 (ARN) 与 Lake Formation 控制台中的名称相同。指向共享表的资源链接保持不变，因此订阅用户不必创建新的资源链接。

编辑委托人 (AWS 账户 ID)

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   登录委托管理员账户。
2. 使用页面右上角的 AWS 区域 选择器，选择要编辑订阅者详细信息的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，使用单选按钮选择要编辑的订阅用户。所选订阅用户的数据访问方式必须为 LAKEFORMATION。
5. 选择编辑。
6. 输入订阅用户的新 AWS 账户 ID，然后选择保存。

   保存新的账户 ID 会自动删除之前的 AWS RAM 资源共享，这样以前的委托人就无法使用日志和事件源。Security Lake 会创建新的资源共享。
7. 订阅用户必须使用新主体的凭证接受新的资源共享，并创建指向共享表的资源链接。这可以为新主体提供访问共享资源的权限。有关说明，请参阅设置跨账户表共享（订阅用户步骤）中的步骤 1 和 2。确保订阅用户详细信息中显示的 ARN 与 Lake Formation 控制台中显示的 ARN 相同。

编辑日志和事件源

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

   登录委托管理员账户。
2. 使用页面右上角的 AWS 区域 选择器，选择要编辑订阅者详细信息的区域。
3. 在导航窗格中选择订阅用户。
4. 在订阅用户页面上，使用单选按钮选择要编辑的订阅用户。所选订阅用户的数据访问方式必须为 LAKEFORMATION。
5. 选择编辑。
6. 取消选择现有来源或选择要添加的来源。如果您取消选择来源，则无需执行进一步操作。如果您选择添加来源，则不会创建新的资源共享邀请。但是，Security Lake 会根据添加的来源更新共享的 Lake Formation 表。订阅用户必须创建指向更新的共享表的资源链接，这样他们才能查询源数据。有关说明，请参阅设置跨账户表共享（订阅用户步骤）中的步骤 2。
7. 选择保存。

API

要以编程方式编辑具有查询权限的订阅者，请使用 Security Lake API 的UpdateSubscriber操作。如果你使用的是 AWS Command Line Interface (AWS CLI)，请运行 update- subscriber 命令。在您的请求中，使用支持的参数为订阅用户指定以下设置：

- 对于 `subscriberName`，请指定新的订阅用户名称。
- 对于 `subscriberDescription`，请指定新的描述。
- 对于`subscriberIdentity`，请指定订阅者用于查询源数据的委托人 (AWS 账户 ID) 和外部 ID。您必须同时提供主体和外部 ID。如果想让其中一个值保持不变，请输入当前值。
  - 仅更新外部 ID：此操作会删除以前的 AWS RAM 资源共享，并为订阅用户创建新的资源共享。订阅用户必须按照设置跨账户表共享（订阅用户步骤）中的步骤 1 接受新的资源共享。指向共享表的资源链接保持不变，因此订阅用户不必创建新的资源链接。
  - 仅更新主体-此操作会删除以前的 AWS RAM 资源共享，因此以前的委托人无法使用日志和事件源。Security Lake 会创建新的资源共享。订阅用户必须使用新主体的凭证接受新的资源共享，并创建指向共享表的资源链接。这可以为新主体提供访问共享资源的权限。有关说明，请参阅设置跨账户表共享（订阅用户步骤）中的步骤 1 和 2。

要更新外部 ID 和主体，请按照设置跨账户表共享（订阅用户步骤）中的步骤 1 和 2 进行操作。

- 对于 `sources`，请移除现有来源或指定要添加的来源。如果您移除来源，则无需执行进一步的操作。如果您添加来源，则不会创建新的资源共享邀请。但是，Security Lake 会根据添加的来源更新共享的 Lake Formation 表。订阅用户必须创建指向更新的共享表的资源链接，这样他们才能查询源数据。有关说明，请参阅设置跨账户表共享（订阅用户步骤）中的步骤 2。

Security Lake 查询

您可以查询 Security Lake 存储在 AWS Lake Formation 数据库和表中的数据。您还可以在 Security Lake 控制台、API 或 AWS CLI 中创建第三方订阅用户。第三方订阅用户还可以从您指定的来源查询 Lake Formation 数据。

Lake Formation 数据湖管理员必须向查询数据的 IAM 身份授予相关数据库和表的 SELECT 权限。订阅用户也必须是在 Security Lake 中创建的，然后才能查询数据。有关如何创建具有查询权限的订阅用户的更多信息，请参阅管理 Security Lake 订阅用户的查询访问权限。

主题

Security Lake 查询 AWS 源版本 1 (OCSF 1.0.0-rc.2)

以下部分提供有关从 Security Lake 查询数据的指导，并包括一些原生 AWS 支持的来源的查询示例。这些查询旨在检索特定数据 AWS 区域。示例使用的是 us-east-1，即美国东部（弗吉尼亚州北部）。此外，示例查询使用 LIMIT 25 参数，最多返回 25 条记录。您可以省略该参数或根据自己的偏好进行调整。有关更多示例，请参阅 Amazon Security Lake OCSF 查询 GitHub 目录。

日志源表

查询 Security Lake 数据时，您必须将数据所在的 Lake Formation 表的名称包含在内。

```
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
```

日志源表的常见值包括以下内容：

- cloud_trail_mgmt_1_0— AWS CloudTrail 管理活动

- `lambda_execution_1_0`— Lambda CloudTrail 的数据事件
- `s3_data_1_0`— S3 CloudTrail 的数据事件
- `route53_1_0` – Amazon Route 53 Resolver 查询日志
- `sh_findings_1_0`— AWS Security Hub 调查结果
- `vpc_flow_1_0` – Amazon Virtual Private Cloud (Amazon VPC) 流日志

示例：表 **`sh_findings_1_0`** 中来自 us-east-1 区域的所有 Security Hub 调查发现

```
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
```

数据库区域

查询 Security Lake 数据时，您必须将要从中查询数据的数据库区域名称包含在内。有关当前提供 Security Lake 的数据库区域的完整列表，请参阅 Amazon Security Lake 端点。

示例：列出来自源 IP AWS CloudTrail 的活动

us-east-1 # cloud_trail_mgmt_1_0 ####### 202 30301#2023 # 3 # 1 ##### ####### IP 192.0.2. 1 CloudTrail #### 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
```

分区日期

通过对数据进行分区，您可以限制每次查询所扫描的数据量，从而提高性能并降低成本。Security Lake 通过 eventDay、region 和 accountid 参数实施分区。eventDay 分区采用格式 YYYYMMDD。

以下是使用 eventDay 分区的查询示例：

```
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
```

eventDay 的常见值包括以下内容：

过去 1 年内发生的事件

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

过去 1 个月内发生的事件

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

过去 30 天内发生的事件

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

过去 12 个小时内发生的事件

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

过去 5 分钟内发生的事件

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

7-14 天前发生的事件

```
  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)
```

在特定日期当天或之后发生的事件

```
  >= '20230301'
```

示例：表中列出了 2023 年 3 月 1 日当天或之后来自源 IP **192.0.2.1** 的所有 CloudTrail 活动 **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
```

示例：表中列出了过去 30 天内来自源 IP **192.0.2.1** 的所有 CloudTrail 活动 **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
```

CloudTrail 数据查询示例

AWS CloudTrail 跟踪中的用户活动和 API 使用情况 AWS 服务。订阅者可以查询 CloudTrail 数据以了解以下类型的信息：

以下是一些 CloudTrail 数据查询示例：

过去 7 天 AWS 服务 内未经授权的企图

```
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
```

过去 7 天**192.0.2.1**内来自源 IP 的所有 CloudTrail 活动清单

```
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
```

过去 7 天内所有 IAM 活动的列表

```
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
```

过去 7 天内使用过凭证 **AIDACKCEVSQ6C2EXAMPLE** 的实例

```
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
```

过去 7 天内失败的 CloudTrail 记录列表

```
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
```

Route 53 Resolver 查询日志的查询示例

Amazon Route 53 Resolver 查询日志可以跟踪由 Amazon VPC 中的资源进行的 DNS 查询。订阅用户可以查询 Route 53 Resolver 查询日志，以了解以下类型的信息：

以下是 Route 53 Resolver 查询日志的一些查询示例：

过去 7 天 CloudTrail 内的 DNS 查询列表

```
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
```

过去 7 天内与 **s3.amazonaws.com** 匹配的 DNS 查询的列表

```
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
```

过去 7 天内未解析的 DNS 查询的列表

```
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
```

过去 7 天内解析到 **192.0.2.1** 的 DNS 查询的列表

```
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
```

Security Hub 调查发现查询示例

Security Hub 为您提供安全状态的全面视图， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。Security Hub 会为安全检查生成调查发现，并接收来自第三方服务的调查发现。

以下是 Security Hub 调查发现的一些查询示例：

过去 7 天内严重性等级大于或等于 **MEDIUM** 的新调查发现

```
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
```

过去 7 天内的重复调查发现

```
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
```

过去 7 天内的所有非信息性调查发现

```
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
```

资源为 Amazon S3 存储桶的调查发现（无时间限制）

```
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
```

通用漏洞评分系统 (CVSS) 得分大于 **1** 的调查发现（无时间限制）

```
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
```

符合通用漏洞披露 (CVE) **CVE-0000-0000** 的调查发现（无时间限制）

```
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
```

过去 7 天内从 Security Hub 发送调查发现的产品数量

```
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
```

过去 7 天内调查发现中的资源类型数量

```
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
```

过去 7 天内调查发现中的易受攻击软件包

```
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
```

过去 7 天内发生更改的调查发现

```
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
```

Amazon VPC 流日志的查询示例

Amazon Virtual Private Cloud (Amazon VPC) 提供有关进出 VPC 网络接口的 IP 流量的详细信息。

以下是 Amazon VPC 流日志的一些查询示例：

最近 7 天的具体 AWS 区域 流量

```
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
```

过去 7 天内来自源 IP **192.0.2.1** 和源端口 **22** 的活动的列表

```
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
```

过去 7 天内不同目标 IP 地址的数量

```
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
```

过去 7 天内源自 198.51.100.0/24 的流量

```
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
```

过去 7 天内的所有 HTTPS 流量

```
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
```

按过去 7 天内发送到端口 **443** 的连接的数据包数量排序

```
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
```

过去 7 天内 IP **192.0.2.1** 和 **192.0.2.2** 之间的所有流量

```
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
```

过去 7 天内的所有入站流量

```
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
```

过去 7 天的所有出站流量

```
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
```

过去 7 天内所有被拒绝的流量

```
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
```

AWS 源版本 2 的 Security Lake 查询 (OCSF 1.1.0)

您可以查询 Security Lake 存储在 AWS Lake Formation 数据库和表中的数据。您还可以在 Security Lake 控制台、API 或 AWS CLI中创建第三方订阅用户。第三方订阅用户还可以从您指定的来源查询 Lake Formation 数据。

Lake Formation 数据湖管理员必须向查询数据的 IAM 身份授予相关数据库和表的 SELECT 权限。订阅用户也必须是在 Security Lake 中创建的，然后才能查询数据。有关如何创建具有查询权限的订阅用户的更多信息，请参阅管理 Security Lake 订阅用户的查询访问权限。

以下部分提供有关从 Security Lake 查询数据的指导，并包括一些原生 AWS 支持的来源的查询示例。这些查询旨在检索特定数据 AWS 区域。示例使用的是 us-east-1，即美国东部（弗吉尼亚州北部）。此外，示例查询使用 `LIMIT 25` 参数，最多返回 25 条记录。您可以省略该参数或根据自己的偏好进行调整。有关更多示例，请参阅 Amazon Security Lake OCSF 查询 GitHub 目录。

日志源表

查询 Security Lake 数据时，您必须将数据所在的 Lake Formation 表的名称包含在内。

```
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
```

日志源表的常见值包括以下内容：

- `cloud_trail_mgmt_2_0`— AWS CloudTrail 管理活动
- `lambda_execution_2_0`— Lambda CloudTrail 的数据事件
- `s3_data_2_0`— S3 CloudTrail 的数据事件
- `route53_2_0` – Amazon Route 53 Resolver 查询日志
- `sh_findings_2_0`— AWS Security Hub 调查结果
- `vpc_flow_2_0` – Amazon Virtual Private Cloud (Amazon VPC) 流日志
- `eks_audit_2_0`— 亚马逊 Elastic Kubernetes Service（亚马逊 EKS）审计日志

示例：表 **`sh_findings_2_0`** 中来自 us-east-1 区域的所有 Security Hub 调查发现

```
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
```

数据库区域

查询 Security Lake 数据时，您必须将要从中查询数据的数据库区域名称包含在内。有关当前提供 Security Lake 的数据库区域的完整列表，请参阅 Amazon Security Lake 端点。

示例：列出来自来源 IP 的亚马逊 Virtual Private Cloud 活动

us-west-2 # vpc_flow_ 2_0 ###### 2023030 1#2023 # 3 # 1 ############ IP 192.0.2. 1 #### VPC ### 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
```

分区日期

通过对数据进行分区，您可以限制每次查询所扫描的数据量，从而提高性能并降低成本。与 Security Lake 1.0 相比，Security Lake 2.0 中的分区工作 Security Lake 现在通过`time_dt`、`region`和`accountid`实现分区。而 Security Lake 1.0 通过`eventDay`、`region`和`accountid`参数实现了分区。

查询`time_dt`将自动生成来自 S3 的日期分区，并且可以像 Athena 中任何基于时间的字段一样进行查询。

以下是使用 `time_dt`分区查询 2023 年 3 月 1 日之后的日志的查询示例：

```
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
```

`time_dt` 的常见值包括以下内容：

过去 1 年内发生的事件

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

过去 1 个月内发生的事件

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

过去 30 天内发生的事件

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

过去 12 个小时内发生的事件

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

过去 5 分钟内发生的事件

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

7-14 天前发生的事件

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

在特定日期当天或之后发生的事件

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

示例：表中列出了 2023 年 3 月 1 日当天或之后来自源 IP **192.0.2.1** 的所有 CloudTrail 活动 **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
```

示例：表中列出了过去 30 天内来自源 IP **192.0.2.1** 的所有 CloudTrail 活动 **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
```

查询安全湖观测数据

Observables 是 Security Lake 2.0 现已推出的一项新功能。observable 对象是一个枢轴元素，其中包含在事件中许多地方发现的相关信息。通过查询可观察数据，用户可以从其数据集中获得高级安全见解。

通过查询可观察对象中的特定元素，您可以将数据集限制为诸如特定用户名、资源 UID、IP、哈希值和其他 IOC 类型信息之类的内容

这是一个使用 observables 数组查询包含 IP 值 “172.01.02.03” 的 VPC Flow 和 Route53 表中的日志的示例查询

```
WITH a AS
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip'),
b as
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip')
SELECT * FROM a
LEFT JOIN b ON a.value=b.value and a.name=b.name
LIMIT 25
```

CloudTrail 数据查询示例

AWS CloudTrail 跟踪中的用户活动和 API 使用情况 AWS 服务。订阅者可以查询 CloudTrail 数据以了解以下类型的信息：

以下是一些 CloudTrail 数据查询示例：

过去 7 天 AWS 服务 内未经授权的企图

```
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
```

过去 7 天**192.0.2.1**内来自源 IP 的所有 CloudTrail 活动清单

```
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
```

过去 7 天内所有 IAM 活动的列表

```
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
```

过去 7 天内使用过凭证 **AIDACKCEVSQ6C2EXAMPLE** 的实例

```
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
```

过去 7 天内失败的 CloudTrail 记录列表

```
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
```

Route 53 Resolver 查询日志的查询示例

Amazon Route 53 Resolver 查询日志可以跟踪由 Amazon VPC 中的资源进行的 DNS 查询。订阅用户可以查询 Route 53 Resolver 查询日志，以了解以下类型的信息：

过去 7 天 CloudTrail 内的 DNS 查询列表

```
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
```

过去 7 天内与 **s3.amazonaws.com** 匹配的 DNS 查询的列表

```
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
```

过去 7 天内未解析的 DNS 查询的列表

```
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
```

过去 7 天内解析到 **192.0.2.1** 的 DNS 查询的列表

```
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
```

Security Hub 调查发现查询示例

Security Hub 为您提供安全状态的全面视图， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。Security Hub 会为安全检查生成调查发现，并接收来自第三方服务的调查发现。

以下是 Security Hub 调查发现的一些查询示例：

过去 7 天内严重性等级大于或等于 **MEDIUM** 的新调查发现

```
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
```

过去 7 天内的重复调查发现

```
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
```

过去 7 天内的所有非信息性调查发现

```
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
```

资源为 Amazon S3 存储桶的调查发现（无时间限制）

```
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
```

通用漏洞评分系统 (CVSS) 得分大于 **1** 的调查发现（无时间限制）

```
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
```

符合通用漏洞披露 (CVE) **CVE-0000-0000** 的调查发现（无时间限制）

```
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
```

过去 7 天内从 Security Hub 发送调查发现的产品数量

```
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
```

过去 7 天内调查发现中的资源类型数量

```
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
```

过去 7 天内调查发现中的易受攻击软件包

```
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
```

过去 7 天内发生更改的调查发现

```
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
```

Amazon VPC 流日志的查询示例

Amazon Virtual Private Cloud (Amazon VPC) 提供有关进出 VPC 网络接口的 IP 流量的详细信息。

以下是 Amazon VPC 流日志的一些查询示例：

最近 7 天的具体 AWS 区域 流量

```
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
```

过去 7 天内来自源 IP **192.0.2.1** 和源端口 **22** 的活动的列表

```
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
```

过去 7 天内不同目标 IP 地址的数量

```
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
```

过去 7 天内源自 198.51.100.0/24 的流量

```
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
```

过去 7 天内的所有 HTTPS 流量

```
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
```

按过去 7 天内发送到端口 **443** 的连接的数据包数量排序

```
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
```

过去 7 天内 IP **192.0.2.1** 和 **192.0.2.2** 之间的所有流量

```
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
```

过去 7 天内的所有入站流量

```
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
```

过去 7 天的所有出站流量

```
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
```

过去 7 天内所有被拒绝的流量

```
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
```

亚马逊 EKS 的查询示例

Amazon EKS 日志跟踪控制平面活动可直接从 Amazon EKS 控制平面向您的账户提供审计和诊断 CloudWatch 日志。这些日志使您可以轻松保护和运行集群。订阅者可以查询 EKS 日志以了解以下类型的信息：

以下是 EKS 日志的一些查询示例：

过去 7 天内向特定 URL 发出的请求

```
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
```

更新过去 7 天来自 “10.0.97.167” 的请求

```
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
```

过去 7 天内与资源 “kube-controller-manager” 关联的请求和响应

```
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
```

Security Lake 中的生命周期管理

您可以自定义 Security Lake，将数据存储在您首 AWS 区域 选的时间段内。生命周期管理可以帮助您遵守不同的合规性要求。

留存管理

要管理您的数据，以便采用经济高效的方式存储，您可以为数据配置留存设置。Security Lake 将数据存储为 Amazon Simple Storage Service (Amazon S3) 桶中的对象，因此留存设置与 Amazon S3 生命周期配置是相对应的。通过配置这些设置，您可以指定首选 Amazon S3 存储类，以及 S3 对象在转换为其他存储类或过期之前在该存储类中留存的时间段。有关 Amazon S3 生命周期配置的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的管理您的存储生命周期。

在 Security Lake 中，您可以在区域级别指定留存设置。例如，您可以选择在特定的 S3 对象写入数据湖 30 天后， AWS 区域 将其转换为 S3 标准-IA 存储类别。默认的 Amazon S3 存储类是 S3 Standard。

> **Important**
>
> Security Lake 不支持 Amazon S3 对象锁定。创建数据湖存储桶时，S3 对象锁定默认处于禁用状态。在默认保留模式下启用 S3 对象锁定会中断向数据湖传输标准化日志数据。

启用 Security Lake 时配置留存设置

在开始使用 Security Lake 时，请按照以下说明为一个或多个区域配置留存设置。如果您未配置留存设置，Security Lake 会使用 Amazon S3 生命周期配置的默认设置，即使用 S3 Standard 存储类无限期存储数据。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 到达入门流程的第 2 步：定义目标后，在选择存储类下选择添加转换。然后选择要将 S3 对象转换为哪个 Amazon S3 存储类。（未列出的默认存储类是 S3 Standard。）您还要为该存储类指定留存期（以天为单位）。要在该时段后将对象转换为其他存储类，请选择添加转换，然后输入后续存储类和留存期的设置。

3. 要指定 S3 对象的过期时间，请选择添加转换。然后，对于存储类，选择过期。对于留存期，输入您想在对象创建后使用任意存储类将其存储在 Amazon S3 中的总天数。该时间段结束后，对象将过期，Amazon S3 会将其删除。
4. 完成后，选择 Next (下一步)。

您的更改将适用于您在之前的入门步骤中启用了 Security Lake 的所有区域。

API

要在登录 Security Lake 时以编程方式配置保留设置，请使用 Security Lake API 的CreateDataLake操作。如果您使用的是 AWS CLI，请运行该create-data-lake命令。在`lifecycleConfiguration`参数中指定所需的保留设置，如下所示：

- 对于 `transitions`，请指定要在特定 Amazon S3 存储类 (`storageClass`) 中存储 S3 对象的总天数 (`days`)。
- 对于 `expiration`，可以使用任意存储类指定对象创建后在 Amazon S3 中存储对象的总天数。该时间段结束后，对象将过期，Amazon S3 会将其删除。

Security Lake 会将设置应用到您在 `configurations` 对象的 `region` 字段中指定的区域。

例如，以下命令在`us-east-1`区域中启用安全湖。在该区域中，对象在 365 天后过期，对象在 60 天后转换到 `ONEZONE_IA` S3 存储类别。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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"
```

更新留存设置

启用 Security Lake 后，请按照以下说明更新一个或多个区域的留存设置。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。

2. 在导航窗格中，选择区域
3. 选择一个区域，然后选择编辑。
4. 在选择存储类部分，输入所需设置。对于存储类，选择要将 S3 对象转换为哪个 Amazon S3 存储类。（未列出的默认存储类是 S3 Standard。）对于留存期，请输入要将对象存储在该存储类中的天数。您可以指定多个转换。

   要指定 S3 对象的过期时间，请为存储类选择过期。对于留存期，输入您想在对象创建后使用任意存储类将其存储在 Amazon S3 中的总天数。该时间段结束后，对象将过期，Amazon S3 会将其删除。
5. 完成后，选择保存。

API

要以编程方式更新保留设置，请使用 Security Lake API 的UpdateDataLake操作。如果您使用的是 AWS CLI，请运行命令。update-data-lake在您的请求中，使用`lifecycleConfiguration`参数指定新设置：

- 要更改转换设置，请使用 `transitions` 参数指定要在特定 Amazon S3 存储类 (`days`) 中存储 S3 对象的每个新时间段 (`storageClass`)。
- 要更改总体留存期，请使用 `expiration` 参数指定在创建对象后使用任意存储类存储 S3 对象的总天数。此留存期结束后，对象将过期，Amazon S3 会将其删除。

Security Lake 会将设置应用到您在 `configurations` 对象的 `region` 字段中指定的区域。

例如，以下 AWS CLI 命令更新该`us-east-1`区域的数据过期设置和存储过渡设置。在该区域中，对象在 500 天后过期，对象在 30 天后转换到 `ONEZONE_IA` S3 存储类别。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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"
```

汇总区域

汇总区域整合了来自一个或多个数据提供区域的数据。这可以帮助您遵守区域数据合规性要求。

有关配置汇总区域的说明，请参阅配置汇总区域。

开放式网络安全架构框架 (OCSF)

什么是 OCSF？

开放网络安全架构框架 (OCSF) 是由 AWS 网络安全行业的领先合作伙伴共同开发的开源项目。OCSF 可为常见的安全事件提供标准架构，定义版本控制标准以推动架构发展，并包括安全日志生产者和使用者的自我管理流程。OCSF 的公共源代码托管在。GitHub

Security Lake 会自动将来自原生支持的日志和事件转换为 OCSF AWS 服务 架构。转换为 OCSF 后，Security Lake 会将数据存储在您的亚马逊简单存储服务 (Amazon S3) 存储桶（ AWS 区域每个存储桶一个存储桶）中。 AWS 账户从自定义来源写入 Security Lake 的日志和事件必须遵守 OCSF 架构和 Apache Parquet 格式。订阅用户可以将日志和事件视为通用 Parquet 记录，也可以应用 OCSF 架构事件类来更准确地解读记录中包含的信息。

OCSF 事件类

来自特定 Security Lake 来源的日志和事件与 OCSF 中定义的特定事件类相匹配。DNS 活动、SSH 活动和身份验证是 OCSF 中的事件类的示例。您可以指定特定来源所匹配的事件类。

OCSF 来源识别

OCSF 使用各种字段来帮助您确定特定日志或事件的来源。这些是 Security Lake AWS 服务 中原生支持作为来源的相关字段的值。

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

来源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	类名	元数据版本
CloudTrail Lambda 数据事件	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2

来源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	类名	元数据版本
CloudTrail 管理活动	CloudTrail	AWS	Management	API Activity、Authentication 或 Account Change	1.0.0-rc.2
CloudTrail S3 数据事件	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	匹配 Security Hub ProductName 值	Security Finding	1.0.0-rc.2
Amazon VPC 流日志	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.

来源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	类名	元数据版本
CloudTrail Lambda 数据事件	CloudTrail	AWS	Data	API Activity	1.1.0
CloudTrail 管理活动	CloudTrail	AWS	Management	API Activity、Au	1.1.0

来源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	类名	元数据版本
				ation 或 Account Change	
CloudTrail S3 数据事件	CloudTrail	AWS	Data	API Activity	1.1.0
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
Security Hub	匹配 AWS 安全调查结果格式 (ASFF) 值 ProductName	匹配 AWS 安全调查结果格式 (ASFF) 值 CompanyName	匹配来自 ASFF 的featureName 值 ProductFields	Vulnerability Finding, Compliance Finding, or Detection Finding	1.1.0
Amazon VPC 流日志	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0
EKS 审核日志	Amazon EKS	AWS	Elastic Kubernetes Service	API Activity	1.1.0

与 Security Lake 的集成

Amazon Security Lake 与其他产品 AWS 服务 和第三方产品集成。集成之后，可以作为来源将数据发送到 Security Lake，也可以作为订阅用户使用 Security Lake 中的数据。以下主题说明了哪些产品 AWS 服务 和第三方产品与 Security Lake 集成。

主题

AWS 服务 与安全湖集成

Amazon 安全湖与其他安全湖集成 AWS 服务。服务可以作为源集成和/或订阅用户集成运行。

源集成具有以下属性：

- 将数据发送到 Security Lake
- 数据以开放式网络安全架构框架 (OCSF) 架构到达
- 数据以 Apache Parquet 格式到达

订阅者集成具有以下属性：可以通过 HTTPS 终端节点或亚马逊简单队列服务 (Amazon SQS) 队列从 Security Lake 读取源数据，也可以直接从中查询源数据 AWS Lake Formation

以下部分说明了与哪个 Sec AWS 服务 urity Lake 集成的以及每个集成的工作原理。

与集成 AWS AppFabric

集成类型：源

AWS AppFabric是一项无代码服务，可连接组织中的软件即服务 (SaaS) 应用程序，因此 IT 和安全团队可以使用标准架构和中央存储库来管理和保护应用程序。

安全湖如何收到 AppFabric 调查结果

您可以将 AppFabric 审核日志数据发送到安全湖，方法是选择 Amazon Kinesis Data Firehose 作为目的地，然后将 Kinesis Data Firehose 配置为以 OCSF 架构和 Apache Parquet 格式向安全湖传输数据。

先决条件

在将 AppFabric 审核日志发送到 Security Lake 之前，必须将 OCSF 标准化审计日志输出到 Kinesis Data Firehose 流。然后，您可以配置 Kinesis Data Firehose，将输出发送到 Security Lake Amazon S3 存储桶。有关更多信息，请参阅《Amazon Kinesis 开发人员指南》中的选择 Amazon S3 作为目标。

将你的 AppFabric 调查结果发送到安全湖

要在完成上述先决条件后将 AppFabric 审计日志发送到 Security Lake，您必须启用这两项服务并在 Security Lake 中添加 AppFabric 为自定义来源。有关添加自定义源的说明，请参阅从自定义源收集数据。

停止在安全湖中接收 AppFabric 日志

要停止接收 AppFabric 审核日志，您可以使用 Security Lake 控制台、Security Lake API，也可以 AWS CLI 将其 AppFabric 作为自定义来源删除。有关说明，请参阅删除自定义源。

与 Amazon Detective 集成

集成类型：订阅用户

Amazon Detective 可帮助您分析、调查和快速识别安全结果或可疑活动的根本原因。Detective 会自动从您的 AWS 资源中收集日志数据。然后，它使用机器学习、统计分析和图形理论生成可视化效果，帮助更快、更高效地进行安全调查。Detective 的预构建数据聚合、摘要和上下文可有助于分析和确定潜在安全问题的性质和程度。

当你集成 Security Lake 和 Detective 时，你可以从 Detective 中查询 Security Lake 存储的原始日志数据。有关更多信息，请参阅与 Amazon Security Lake 集成。

与亚马逊 OpenSearch 服务集成

集成类型：订阅用户

Amazon OpenSearch Service 是一项托管服务，可让您在中轻松部署、操作和扩展 OpenSearch 服务集群 AWS Cloud。使用 S OpenSearch ervice Ingestion 将数据摄取到您的 OpenSearch 服务集群中，您可以更快地获得对时间敏感的安全调查的见解。您可以快速响应安全事件，从而保护您的关键业务数据和系统。

OpenSearch 服务控制面板

将 OpenSearch 服务与 Security Lake 集成后，您可以将 Security Lake 配置为通过无服务器 OpenSearch 服务接入将来自不同来源的安全数据发送到 OpenSearch 服务服务。有关如何配置 OpenSearch 服务摄取以处理安全数据的更多信息，请参阅使用 Amazon Service Ingestion 从 Amazon Security Lake 数据生成安全见解。 OpenSearch

在 OpenSearch 服务摄取开始将您的数据写入 OpenSearch 服务域之后。要使用预先构建的仪表板可视化数据，请导航到仪表板并选择任何一个已安装的仪表板。

与亚马逊集成 QuickSight

集成类型：订阅用户

Amazon QuickSight 是一项云规模的商业智能 (BI) 服务，无论您身在何处，都可以使用它向与之共事的人提供 easy-to-understand 见解。Amazon 会 QuickSight 连接到您在云中的数据，并合并来自许多不同来源的数据。Amazon QuickSight 让决策者有机会在交互式视觉环境中探索和解释信息。决策者可以从网络上的任何设备和移动设备安全地访问控制面板。

亚马逊 QuickSight 控制面板

在亚马逊中可视化您的 Amazon QuickSight Security Lake 数据，创建所需的 AWS 对象，并将 QuickSight 与安全湖相关的基本数据源、数据集、分析、控制面板和用户组部署到亚马逊。有关详细说明，请参阅与 Amazon 集成 QuickSight。

与亚马逊集成 SageMaker

集成类型：订阅用户

Amazon SageMaker 是一项完全托管的机器学习 (ML) 服务。借助 Security Lake，数据科学家和开发人员可以快速、自信地构建、训练机器学习模型，并将其部署到生产就绪的托管环境中。它为运行机器学习工作流程提供了用户界面体验，使 SageMaker 机器学习工具可在多个集成开发环境 (IDE) 中使用。

SageMaker 见解

您可以使用 SageMaker Studio 为 Security Lake 生成机器学习见解。 SageMaker Studio 是一个用于机器学习的 Web 集成开发环境 (IDE)，它为数据科学家提供了准备、构建、训练和部署机器学习模型的工具。使用此解决方案，您可以快速部署一组基本 Python 笔记本，重点关注 Security Lake 中的 AWS Security Hub 发现，还可以扩展这些笔记本以在 Security Lake 中纳入其他 AWS 来源或自定义数据源。有关更多详细信息，请参阅使用亚马逊为亚马逊安全湖数据生成机器学习见解 SageMaker。

与 Amazon Bedrock 集成

Amazon Bedrock 是一项完全托管的服务，它通过统一的 API 提供来自领先人工智能初创公司和亚马逊的高性能基础模型 (FM) 供您使用。借助 Amazon Bedrock 的无服务器体验，您可以快速入门，使用自己的数据私下自定义基础模型，并使用 AWS 工具轻松安全地将其集成和部署到您的应用程序中，而无需管理任何基础架构。

生成式人工智能

您可以使用 Amazon Bedrock 的生成人工智能功能和 SageMaker Studio 中的自然语言输入来分析安全湖中的数据，努力降低组织的风险并提高安全状况。您可以通过自动识别相应的数据源、生成和调用 SQL 查询以及可视化调查数据来缩短进行调查所需的时间。有关更多详细信息，请参阅使用 Amazon SageMaker Studio 和 Amazon Bedrock 为亚马逊安全湖生成人工智能驱动的见解。

与集成 AWS Security Hub

集成类型：源

AWS Security Hub为您提供安全状态的全面视图， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。Security Hub 从各种 AWS 账户服务和支持的第三方合作伙伴产品中收集安全数据，并帮助您分析安全趋势并确定优先级最高的安全问题。

当您启用 Security Hub 并将 Security Hub 调查发现添加为 Security Lake 中的源时，Security Hub 将开始向 Security Lake 发送新调查发现以及对现有调查发现的更新。

Security Lake 如何接收 Security Hub 调查发现

在 Security Hub 中，安全问题按调查结果进行跟踪。一些发现来自其他 AWS 服务或第三方合作伙伴检测到的问题。Security Hub 还可以根据规则运行自动和持续的安全检查，从而生成自己的调查发现。这些规则由安全控件来表示。

Security Hub 中的所有调查结果都使用名为 AWS 安全检测结果格式（ASFF）的标准 JSON 格式。

Security Lake 会接收 Security Hub 调查发现并将其转换为开放式网络安全架构框架 (OCSF)。

将 Security Hub 调查发现发送到 Security Lake

要将 Security Hub 调查发现发送到 Security Lake，您必须启用这两项服务，并将 Security Hub 调查发现添加为 Security Lake 中的源。有关添加 AWS 源的说明，请参阅将添加 AWS 服务 为来源。

如果您希望 Security Hub 生成控件调查发现并将其发送到 Security Lake，则必须在 AWS Config中启用相关安全标准并按区域启用资源记录。有关更多信息，请参阅《AWS Security Hub 用户指南》中的启用和配置 AWS Config。

停止在 Security Lake 中接收 Security Hub 调查发现

要停止接收 Security Hub 的调查结果，你可以使用 Security Hub 控制台、Security Hub API 或 AWS CLI。

请参阅《AWS Security Hub 用户指南》中的禁用和启用来自集成的调查发现流（控制台）或禁用来自集成的调查发现流（Security Hub API、AWS CLI）。

与 Security Lake 的第三方集成

Amazon Security Lake 与多个第三方提供商集成。提供商可以提供源集成、订阅用户集成或服务集成。提供商可以提供一个或多个集成类型。

源集成具有以下属性：

- 将数据发送到 Security Lake
- 数据以 Apache Parquet 格式到达
- 数据以开放式网络安全架构框架 (OCSF) 架构到达

订阅用户集成具有以下属性：

- 通过 HTTPS 终端节点或亚马逊简单队列服务 (Amazon SQS) 队列读取源数据，或者直接从中查询源数据 AWS Lake Formation
- 能够读取 Apache Parquet 格式的数据
- 能够读取采用 OCSF 架构的数据

服务集成可以帮助您在组织 AWS 服务 中实施 Security Lake 和其他内容。它们还能在报告、分析和其他使用案例方面提供帮助。

要搜索特定的合作伙伴提供商，请参阅合作伙伴解决方案查找器。要购买第三方产品，请参阅 AWS Marketplace。

要申请添加为合作伙伴集成或成为 Security Lake 合作伙伴，请发送电子邮件至 <securitylake-partners@amazon.com>。

如果您使用第三方集成将调查结果发送到，则如果启用了 Security Lake 的 Security Hub 集成，则还可以在安全湖中查看这些发现。 AWS Security Hub有关启用集成的说明，请参阅与集成 AWS Security Hub。要查看向 Security Hub 发送调查发现的第三方集成列表，请参阅《AWS Security Hub 用户指南》中的可用第三方合作伙伴产品集成。

在设置订阅者之前，请先验证订阅者的 OCSF 日志支持。有关最新详情，请查看您的订阅者文档。

查询集成

您可以查询 Security Lake 存储在 AWS Lake Formation 数据库和表中的数据。您还可以在 Security Lake 控制台、API 或中创建第三方订阅者 AWS Command Line Interface。

Lake Formation 数据湖管理员必须向查询数据的 IAM 身份授予相关数据库和表的 SELECT 权限。查询数据之前，您必须在安全湖中创建订阅者。有关如何创建具有查询权限的订阅用户的更多信息，请参阅管理 Security Lake 订阅用户的查询访问权限。

您可以为以下第三方合作伙伴配置与 Security Lake 的查询集成。

- Palo Alto Networks – XSOAR
- IBM – QRadar
- SOC Prime
- Tego Cyber
- Cribl – Search

Accenture – MxDR

集成类型：订阅用户、服务

Accenture's MxDR 与 Security Lake 的集成可提供日志和事件实时数据摄取、托管式异常检测、威胁搜寻和安全操作。这有助于分析和托管式检测和响应（MDR）。

作为服务集成，Accenture 还可帮助您在组织中实施 Security Lake。

集成文档

Aqua Security

集成类型：源

可以将 Aqua Security 添加为自定义源，以将审计事件发送到 Security Lake。审计事件将被转换为 OCSF 架构和 Parquet 格式。

集成文档

Barracuda – Email Protection

集成类型：源

Barracuda Email Protection 可以在检测到新的网络钓鱼电子邮件攻击时向 Security Lake 发送事件。您可以在数据湖中与其他安全数据一起接收这些事件。

集成文档

Booz Allen Hamilton

集成类型：服务

作为一项服务集成，Booz Allen Hamilton 通过将数据和分析与 Security Lake 服务相结合，使用数据驱动的方法来实现网络安全。

合作伙伴链接

ChaosSearch

集成类型：订阅用户

ChaosSearch 利用开放 API（如 Elasticsearch 和 SQL）或利用原生包含的 Kibana 和 Superset UI，为用户提供多模型数据访问权限。您可以在 ChaosSearch 中使用自己的 Security Lake 数据（没有留存限制）进行监控、警报和威胁搜寻。这可以帮助您应对当今复杂的安全环境和持续存在的威胁。

集成文档

Cisco Security – Secure Firewall

集成类型：源

通过将 Cisco Secure Firewall 与 Security Lake 集成，您可以采用结构化和可扩展的方式存储防火墙日志。Cisco 的 eNCore 客户端从 Firewall Management Center 流式传输防火墙日志，将架构转换为 OCSF 架构，并将其存储在 Security Lake 中。

集成文档

Claroty – xDome

集成类型：源

Claroty xDome 只需最少的配置即可将网络中检测到的警报发送到 Security Lake。灵活而快速的部署选项可帮助 xDome 保护您网络中的扩展物联网（XIoT）资产（包括 IoT、IIoT 和 BMS 资产），同时自动检测威胁的早期迹象。

集成文档

CMD Solutions

集成类型：服务

CMD Solutions 通过设计、自动化和持续保障流程尽早、持续地集成安全性，帮助企业提高敏捷性。作为服务集成，CMD Solutions 可帮助您在组织中实施 Security Lake。

合作伙伴链接

Confluent – Amazon S3 Sink Connector

集成类型：源

Confluent 使用完全托管式的预构建连接器自动连接、配置和编排数据集成。借助 Confluent S3 Sink Connector，您可以获取原始数据，并以原生 parquet 格式将其大规模接收到 Security Lake 中。

集成文档

Contrast Security

集成类型：源

用于集成的合作伙伴产品：Contrast Assess

Contrast Security Assess 是一款 IAST 工具，可在 Web 应用程序、API 和微服务中提供实时漏洞检测。Assess 与 Security Lake 集成，有助于为您的所有工作负载提供集中的可见性。

集成文档

Cribl – Search

集成类型：订阅用户

您可以使用 Cribl Search 来搜索 Security Lake 数据。

集成文档

Cribl – Stream

集成类型：源

您可以使用 Cribl Stream 以 OCSF 架构从 Cribl 支持的任何第三方源向 Security Lake 发送数据。

集成文档

CrowdStrike – Falcon Data Replicator

集成类型：源

此集成以连续流的方式从 CrowdStrike Falcon Data Replicator 中拉取数据，将数据转换为 OCSF 架构，然后将其发送到 Security Lake。

集成文档

CyberArk – Unified Identify Security Platform

集成类型：源

CyberArk Audit Adapter，一个 AWS Lambda 函数，它从 OCSF 架构中收集安全事件CyberArk Identity Security Platform并将数据发送到 Security Lake。

集成文档

Darktrace – Cyber AI Loop

集成类型：源

Darktrace 与 Security Lake 的集成将 Darktrace 自学习的强大功能引入 Security Lake。来自 Cyber AI Loop 的见解可以与组织的安全堆栈中的其他数据流和元素关联。该集成将 Darktrace 模型违规记录为安全调查发现。

集成文档（登录 Darktrace 门户查看文档）

Datadog

集成类型：订阅用户

Datadog Cloud SIEM检测您的云环境面临的实时威胁，包括 Security Lake 中的数据， DevOps 并在一个平台上统一安全团队。

集成文档

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

集成类型：订阅用户、服务

Deloitte MXDR CAE 可帮助您快速存储、分析和可视化标准化安全数据。CAE 套件包含自定义分析、AI 和 ML 功能，可根据针对 Security Lake 中 OCSF 格式数据运行的模型自动提供可操作的见解。

作为服务集成，Deloitte 还可帮助您在组织中实施 Security Lake。

集成文档

Devo

集成类型：订阅用户

的Devo收集器 AWS 支持从 Security Lake 摄取。此集成可帮助您分析和处理各种安全使用案例，例如威胁检测、调查和事件响应。

集成文档

DXC – SecMon

集成类型：订阅用户、服务

DXC SecMon 从 Security Lake 收集安全事件并监控这些事件，以检测潜在的安全威胁并发出警报。这有助于组织更好地了解其安全状况，并主动识别和响应威胁。

作为服务集成，DXC 还可帮助您在组织中实施 Security Lake。

集成文档

Eviden – AIsaac（以前称为 Atos）

集成类型：订阅用户

AIsaac MDR 平台使用 Security Lake 中以 OCSF 架构摄取的 VPC 流日志，并利用 AI 模型来检测威胁。

集成文档

ExtraHop – Reveal(x) 360

集成类型：源

通过以 OCSF 架构将来自 ExtraHop Reveal(x) 360 的网络数据（包括对 IOC 的检测）整合到 Security Lake，您可以增强工作负载和应用程序的安全性。

集成文档

Falcosidekick

集成类型：源

Falcosidekick 会收集 Falco 事件并将其发送到 Security Lake。此集成使用 OCSF 架构导出安全事件。

集成文档

Gigamon – Application Metadata Intelligence

集成类型：源

Gigamon Application Metadata Intelligence (AMI) 为您的可观测性、SIEM 和网络性能监控工具提供了关键元数据属性。这有助于您更深入地了解应用程序，从而找出性能瓶颈、质量问题和潜在的网络安全风险。

集成文档

Hoop Cyber

集成类型：服务

Hoop Cyber FastStart 包含数据来源评估、优先级排序、数据来源载入，并能帮助客户使用 Security Lake 提供的现有工具和集成来查询数据。

合作伙伴链接

IBM – QRadar

集成类型：订阅用户

IBM Security QRadar SIEM with UAX 将 Security Lake 与一个分析平台集成，可识别和防范混合云中的威胁。此集成支持数据访问和查询访问。

关于使用 AWS CloudTrail 日志的集成文档

关于使用 Amazon Athena 进行查询的集成文档

Infosys

集成类型：服务

Infosys 可帮助您根据组织需求自定义 Security Lake 实施方案，并提供自定义见解。

合作伙伴链接

Insbuilt

集成类型：服务

Insbuilt 专注于云咨询服务，可帮助您了解如何在组织中实施 Security Lake。

合作伙伴链接

Kyndryl – AIOps

集成类型：订阅用户、服务

Kyndryl 与 Security Lake 集成，以提供网络数据、威胁情报和基于 AI 的分析的互操作性。作为数据访问订阅者，从 Secur Kyndryl ity Lake 中提取 AWS CloudTrail 管理事件以进行分析。

作为服务集成，Kyndryl 还可帮助您在组织中实施 Security Lake。

集成文档

Lacework – Polygraph

集成类型：源

Lacework Polygraph® Data Platform作为数据源与 Security Lake 集成，并提供有关 AWS 环境中漏洞、配置错误以及已知和未知威胁的安全发现。

集成文档

Laminar

集成类型：源

Laminar 会以 OCSF 架构将数据安全事件发送到 Security Lake，使其可用于其他分析使用案例，例如事件响应和调查。

集成文档

MegazoneCloud

集成类型：服务

MegazoneCloud 专注于云咨询服务，可帮助您了解如何在组织中实施 Security Lake。我们将 Security Lake 与集成式 ISV 解决方案相关联，以构建自定义任务，并生成与客户需求相关的自定义见解。

集成文档

Monad

集成类型：源

Monad 会自动将您的数据转换为 OCSF 架构，并将其发送到您的 Security Lake 数据湖。

集成文档

NETSCOUT – Omnis Cyber Intelligence

集成类型：源

通过与 Security Lake 集成，NETSCOUT 成为安全调查发现和详细安全见解的自定义源，帮助您了解企业中正在发生的状况（如网络威胁、安全风险和攻击面变化）。这些调查发现由 NETSCOUT CyberStreams 和 Omnis Cyber Intelligence 在客户账户中生成，然后以 OCSF 架构被发送到 Security Lake。摄取的数据还符合 Security Lake 源的其他要求和最佳实践，包括格式、架构、分区和性能相关方面。

集成文档

Netskope – CloudExchange

集成类型：源

Netskope通过与 Security Lake 共享与安全相关的日志和威胁信息，帮助您加强安全态势。 Netskope 调查结果通过插件发送到 Security Lake，该CloudExchange插件可以在本地数据中心内 AWS 或本地数据中心内作为基于 docker 的环境启动。

集成文档

New Relic ONE

集成类型：订阅用户

New Relic ONE 是一个基于 Lambda 的订阅用户应用程序。它部署在您的账户中，由 Amazon SQS 触发，并使用 New Relic 许可证密钥将数据发送到 New Relic

集成文档

Okta – Workforce Identity Cloud

集成类型：源

Okta通过 Amazon EventBridge 集成向 OCSF 架构中的安全湖发送身份日志。 Okta System Logs 在 OCSF 架构中，将帮助安全和数据科学家团队按照开源标准查询安全事件。从 Okta 生成标准化的 OCSF 日志可帮助您执行审计活动，并在一致的架构下生成与身份验证、授权、账户更改和实体更改相关的报告。

集成文档

AWS CloudFormation 要在 Secur Okta ity Lake 中添加为自定义源的模板

Orca – Cloud Security Platform

集成类型：源

的Orca无代理云安全平台通过在 OCSF 架构中发送云检测和响应 (CDR) 事件 AWS 与 Security Lake 集成。

集成文档（登录 Orca 门户查看文档）

Palo Alto Networks – Prisma Cloud

集成类型：源

Palo Alto Networks Prisma Cloud 会聚合云原生环境中 VM 的漏洞检测数据，并将其发送到 Security Lake。

集成文档

Palo Alto Networks – XSOAR

集成类型：源

Palo Alto Networks XSOAR已与 XSOAR 和 Security Lake 建立了订阅者集成。

集成文档

Ping Identity – PingOne

集成类型：源

PingOne 会向 Security Lake 发送采用 OCSF 架构和 Parquet 格式的账户修改警报，让您可以发现账户变更并相应地采取行动。

集成文档

PwC – Fusion center

集成类型：订阅用户、服务

PwC 凭借知识和专业技能来帮助客户实施融合中心，满足他们的个性化需求。融合中心基于 Amazon Security Lake 而构建，能够组合来自各种来源的数据，以创建近乎实时的集中式视图。

集成文档

Rapid7 – InsightIDR

集成类型：订阅用户

InsightIDR 是 Rapid7 SIEM/XDR 解决方案，可以在 Security Lake 中摄取日志以用于检测威胁和可疑活动调查。

集成文档

RipJar – Labyrinth for Threat Investigations

集成类型：订阅用户

Labyrinth for Threat Investigations 提供了一种基于数据融合的企业级大规模威胁探查方法，具有精细的安全性、适应性强的工作流程以及报告功能。

集成文档

Sailpoint

集成类型：源

用于集成的合作伙伴产品：SailPoint IdentityNow

此集成使客户能够转换来自 SailPoint IdentityNow 的事件数据。此集成旨在提供一个自动化流程来将 IdentityNow 用户活动和监管事件载入 Security Lake，从而改善来自安全事件和事件监控产品的见解。

集成文档

Securonix

集成类型：订阅用户

Securonix Next-Gen SIEM 与 Security Lake 集成，使安全团队能够更快地摄取数据并提升其检测和响应能力。

集成文档

SentinelOne

集成类型：订阅用户

SentinelOne Singularity™ XDR 平台将实时检测和响应扩展到在本地和公有云基础设施上运行的端点、身份和云工作负载，包括 Amazon Elastic Compute Cloud（Amazon EC2）、Amazon Elastic Container Service（Amazon ECS）和 Amazon Elastic Kubernetes Service（Amazon EKS）。

集成文档（登录 SentinelOne 门户查看文档）

Sentra – Data Lifecyle Security Platform

集成类型：源

在您的账户中部署 Sentra 扫描基础设施后，Sentra 将获取调查发现并将其摄取到您的 SaaS。这些调查发现是元数据，Sentra 会存储它们，然后以 OCSF 架构将它们流式传输到 Security Lake 以用于查询。

集成文档

SOC Prime

集成类型：订阅用户

SOC Prime通过 Amazon S OpenSearch ervice 和 Amazon Athena 与 Security Lake 集成，以促进基于零信任里程碑的智能数据编排和威胁搜寻。 SOC Prime使安全团队能够在不发出大量警报的情况下提高威胁可见性并调查事件。您可以通过可重复使用的规则和查询来节省开发时间，这些规则和查询可自动转换为 OCSF 架构中的 Athena OpenSearch 和 Service。

集成文档

Splunk

集成类型：订阅用户

Amazon Web Services 的Splunk AWS 附加组件 (AWS) 支持从 Security Lake 进行提取。通过订阅来自 Security Lake 的采用 OCSF 架构的数据，此集成帮助您加快威胁检测、调查和响应。

集成文档

Stellar Cyber

集成类型：订阅用户

Stellar Cyber 使用来自 Security Lake 的日志，并将记录添加到 Stellar Cyber 数据湖。此连接器使用 OCSF 架构。

集成文档

Sumo Logic

集成类型：订阅用户

Sumo Logic使用来自 Security Lake 的数据 AWS，并提供跨本地和混合云环境的广泛可见性。Sumo Logic 为安全团队提供了跨所有安全工具的全面可见性、自动化和威胁监控。

集成文档

Swimlane – Turbine

集成类型：订阅用户

Swimlane 以 OCSF 架构从 Security Lake 摄取数据，并通过低代码 Playbook 和案例管理发送数据，以加快威胁检测、调查和事件响应。

集成文档（登录 Swimlane 门户查看文档）

Sysdig Secure

集成类型：源

Sysdig Secure's云原生应用程序保护平台 (CNAPP) 将安全事件发送到 Security Lake，以最大限度地进行监督、简化调查并简化合规性。

集成文档

Talon

集成类型：源

用于集成的合作伙伴产品：Talon Enterprise Browser

Talon's Enterprise Browser 是一个基于浏览器的安全、隔离的端点环境，可将 Talon 访问权限、数据保护、SaaS 操作和安全事件发送到 Security Lake，为检测、取证和调查提供可见性和用来交叉关联事件的选项。

集成文档（登录 Talon 门户查看文档）

Tanium

集成类型：源

Tanium Unified Cloud Endpoint Detection, Management, and Security 平台以 OCSF 架构向 Security Lake 提供清单数据。

集成文档

TCS

集成类型：服务

TCS AWS Business Unit 提供创新、经验和人才。此集成得益于十年的联合价值创造、深厚的行业知识、技术专长和交付智慧。作为服务集成，TCS 可帮助您在组织中实施 Security Lake。

集成文档

Tego Cyber

集成类型：订阅用户

Tego Cyber 与 Security Lake 集成，可帮助您快速检测和调查潜在的安全威胁。通过关联不同时间段和日志来源的不同威胁指标，Tego Cyber 可发现隐藏的威胁。该平台包含大量高度情境化的威胁情报，为威胁检测和调查提供精确性和洞察力。

集成文档

Tines – No-code security automation

集成类型：订阅用户

Tines No-code security automation 利用集中于 Security Lake 中的安全数据来帮助您做出更准确的决策。

集成文档

Torq – Enterprise Security Automation Platform

集成类型：源、订阅用户

Torq 作为自定义源和订阅用户与 Security Lake 无缝集成。Torq 利用一个简单的无代码平台帮助您实施企业级自动化和编排。

集成文档

Trellix – XDR

集成类型：源、订阅用户

作为一个开放 XDR 平台，Trellix XDR 支持 Security Lake 集成。Trellix XDR 可以利用 OCSF 架构的数据处理安全分析使用案例。您还可以利用 Trellix XDR 中的 1,000 多个安全事件源来扩充 Security Lake 数据湖。这可以帮助您扩展 AWS 环境的检测和响应能力。摄取的数据与其他安全风险关联，为您提供了及时应对风险所需的行动手册。

集成文档

Trend Micro – CloudOne

集成类型：源

Trend Micro CloudOne Workload Security 会将以下信息从 Amazon Elastic Compute Cloud（EC2）实例发送到 Security Lake：

- DNS 查询活动
- 文件活动
- 网络活动
- 流程活动
- 注册表值活动
- 用户账户活动

集成文档

Uptycs – Uptycs XDR

集成类型：源

Uptycs 以 OCSF 架构将大量数据从本地和云资产发送到 Security Lake。这些数据包括来自端点和云工作负载的行为威胁检测、异常检测、策略违反情况、风险策略、配置错误和漏洞。

集成文档

Vectra AI – Vectra Detect for AWS

集成类型：源

通过使用Vectra Detect for AWS，您可以使用专用 AWS CloudFormation 模板将高保真警报作为自定义来源发送到 Security Lake。

集成文档

VMware Aria Automation for Secure Clouds

集成类型：源

利用此集成，您可以检测云配置错误，然后将其发送到 Security Lake 进行高级分析。

集成文档

Wazuh

集成类型：订阅用户

Wazuh 旨在安全地处理用户数据、为每个来源提供查询访问权限和优化查询成本。

集成文档

Wipro

集成类型：源、服务

此集成使您能够从 Wipro Cloud Application Risk Governance (CARG) 平台收集数据，以统一视图展示您的云应用程序和整个企业的合规状况。

作为服务集成，Wipro 还可帮助您在组织中实施 Security Lake。

集成文档

Wiz – CNAPP

集成类型：源

Wiz 和 Security Lake 之间的集成通过使用 OCSF 架构（一种专为可扩展和标准化的安全数据交换而设计的开源标准）推动了单个安全数据湖中的云安全数据收集。

集成文档（登录 Wiz 门户查看文档）

Zscaler – Zscaler Posture Control

集成类型：源

Zscaler Posture Control™ 是一个云原生应用程序保护平台，可以将采用 OCSF 架构的安全调查发现发送到 Security Lake。

集成文档

Amazon Security Lake 中的安全性

AWS 十分重视云安全性。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 客户，您也将从这些数据中心和网络架构受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS负责保护在 AWS Cloud 中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS Compliance Programs 的一部分。要了解适用于 Amazon Security Lake 的合规性计划，请参阅按合规性计划提供的范围内 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Security Lake 时应用责任共担模型。以下主题说明如何配置 Security Lake 以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务来帮助您监控和保护 Security Lake 资源。

主题

适用于 Amazon Security Lake 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制哪些人可以通过身份验证（登录）和授权（具有权限）使用 Security Lake 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Security Lake 中所做的工作。

服务用户 – 如果您使用 Security Lake 服务来完成任务，您的管理员会为您提供所需的凭证和权限。如果需要使用更多 Security Lake 功能来完成工作，您可能需要额外的权限。了解访问权限是如何管理的，可以帮助您向管理员请求适合的权限。如果您无法访问 Security Lake 中的某项功能，请参阅Amazon Security Lake 身份和访问故障排除。

服务管理员 – 如果您在公司负责管理 Security Lake 资源，则您可能具有 Security Lake 的完全访问权限。您有责任确定您的服务用户应访问哪些 Security Lake 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何将 IAM 与 Security Lake 结合使用，请参阅Amazon Security Lake 如何与 IAM 一起使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能需要详细了解如何编写策略以管理对 Security Lake 的访问。要查看您可以在 IAM 中使用的 Security Lake 基于身份的策略示例，请参阅 Amazon Security Lake 基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您都可能需要提供其它安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS 中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个用于指定一组 IAM 用户的身份。您不能使用组的身份登录。可以使用群组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，可能具有一个名为 IAMAdmins 的群组，并为该群组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人担任。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户或角色可代入 IAM 角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户存取的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 创建向 AWS 服务 委派权限的角色。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以担任代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》 中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表（ACL）

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型所授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 字段中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。

- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Amazon Security Lake 如何与 IAM 一起使用

在使用 IAM 管理对 Security Lake 的访问之前，您应该了解哪些 IAM 功能可用于 Security Lake。

将 IAM 功能与 Amazon Security Lake 一起使用

IAM 特征	Security Lake 支持
基于身份的策略	是
基于资源的策略	是
策略操作	是
策略资源	是
策略条件键	是
ACL	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	否
服务相关角色	是

要全面了解 Security Lake 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

Security Lake 基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Security Lake 支持基于身份的策略。有关更多信息，请参阅Amazon Security Lake 基于身份的策略示例。

Security Lake 内基于资源的策略

支持基于资源的策略	是

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

Security Lake 服务会为存储数据的 Amazon S3 桶创建基于资源的策略。您无需将这些基于资源的策略附加到 S3 桶。Security Lake 会代表您自动创建这些策略。

示例资源是一个 S3 桶，其 Amazon 资源名称 (ARN) 为 `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`。在此示例中，`region`是您启用 Security Lake 的具体 AWS 区域 位置，并且`bucket-identifier`是 Security Lake 分配给存储桶的区域唯一字母数字字符串。Security Lake 创建了 S3 桶以存储来自该区域的数据。资源策略定义了哪些主体可以对该桶执行操作。以下是 Security Lake 附加到桶的基于资源的策略（桶策略）示例：

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

```
                }
            }
        }
    ]
}
```

要详细了解基于资源的策略，请参阅《IAM 用户指南》中的基于身份的策略和基于资源的策略。

Security Lake 的策略操作

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

有关 Security Lake 操作的列表，请参阅“服务授权参考”中的 Amazon Security Lake 定义的操作。

Security Lake 中的策略操作在操作前使用以下前缀：

```
securitylake
```

例如，要向用户授予访问特定订阅用户的信息的权限，请在分配给该用户的策略中包含 `securitylake:GetSubscriber` 操作。策略语句必须包含 `Action` 或 `NotAction` 元素。Security Lake 定义了一组自己的操作，以描述您可以使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Security Lake 基于身份的策略示例，请参阅 Amazon Security Lake 基于身份的策略示例。

Security Lake 的策略资源

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource`JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

Security Lake 定义了以下资源类型：订阅者和特定资源的数据湖配置 AWS 区域。 AWS 账户 您可以使用 ARN 在策略中指定这些类型的资源。

有关 Security Lake 资源类型的列表以及每种类型的 ARN 语法，请参阅“服务授权参考”中的 Amazon Security Lake 定义的资源类型。要了解可以为每种类型的资源指定哪些操作，请参阅“服务授权参考”中的 Amazon Security Lake 定义的操作。

要查看 Security Lake 基于身份的策略示例，请参阅 Amazon Security Lake 基于身份的策略示例。

Security Lake 的策略条件键

支持特定于服务的策略条件键	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评测它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

有关 Security Lake 条件键的列表，请参阅“服务授权参考”中的 Amazon Security Lake 的条件键。要了解可以为哪些操作和资源使用条件键，请参阅“服务授权参考”中的 Amazon Security Lake 定义的操作。有关使用条件键的策略示例，请参阅 Amazon Security Lake 基于身份的策略示例。

Security Lake 中的访问控制列表 (ACL)

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Security Lake 不支持 ACL，这意味着您无法将 ACL 附加到 Security Lake 资源。

用于 Security Lake 的基于属性的访问权限控制 (ABAC)

支持 ABAC（策略中的标签）	是

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

您可以将标签附加到 Security Lake 资源（订阅者），以及个人的数据湖配置。 AWS 账户 AWS 区域 您还可以通过在策略的 `Condition` 元素中提供标签信息来控制对这些资源的访问。有关标记 Security Lake 资源的更多信息，请参阅为 Amazon Security Lake 资源添加标签。有关基于身份的策略（用于根据资源的标签控制对该资源的访问）示例，请参阅 Amazon Security Lake 基于身份的策略示例。

为 Security Lake 使用临时凭证

支持临时凭证	是

当你使用临时凭证登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Security Lake 支持使用临时凭证。

安全湖的转发访问会话

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

某些 Security Lake 操作需要其他 AWS 服务 中的其他相关操作的权限。有关这些操作的列表，请参阅“服务授权参考”中的 Amazon Security Lake 定义的操作。

Security Lake 的服务角色

支持服务角色	否

服务角色是由一项服务代入、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 创建向 AWS 服务 委派权限的角色。

Security Lake 不代入或使用服务角色。但是，当您使用安全湖时 EventBridge AWS Lambda，诸如Amazon和Amazon S3之类的相关服务将扮演服务角色。要代表您执行操作，Security Lake 会使用服务相关角色。

> **Warning**
>
> 更改服务角色的权限可能会在您使用 Security Lake 时导致操作问题。仅当 Security Lake 提供相应指导时才编辑服务角色。

Security Lake 的服务相关角色

支持服务相关角色	是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以担任代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Security Lake 使用名为 `AWSServiceRoleForAmazonSecurityLake` 的 IAM 服务相关角色。Security Lake 服务相关角色授予代表客户操作安全数据湖服务的权限。服务相关角色是一种与 Security Lake 直接关联的 IAM 角色。它是由 Security Lake 预定义的，它包括 Security Lake AWS 服务 代表你呼叫他人所需的所有权限。Security Lake 在所有可用 Security Lake AWS 区域 的地方都使用此服务相关角色。

有关创建或管理 Security Lake 服务相关角色的详细信息，请参阅 Amazon Security Lake 的服务相关角色。

Amazon Security Lake 基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Security Lake 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 创建 IAM 策略。

有关 Security Lake 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅“服务授权参考”https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazonsecuritylake.html中的 Amazon Security Lake 的操作、资源和条件键。

主题

策略最佳实践

基于身份的策略用于确定某个人是否可以创建、访问或删除您账户中的 Security Lake 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略 或 工作职能的 AWS 托管策略。
- 应用最低权限：在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实操。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 Security Lake 控制台

要访问 Amazon Security Lake 控制台，您必须具有一组最低权限。这些权限必须允许您列出和查看有关您的 Security Lake 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色可以使用 Security Lake 控制台，请创建 IAM 策略并为其提供控制台访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 标识符。

如果您创建了允许用户或角色使用 Security Lake 控制台的策略，请确保该策略包含这些用户或角色需要在控制台上访问的资源的相应操作。否则，他们将无法在控制台上导航到或显示这些资源的详细信息。

例如，要使用控制台添加自定义来源，用户必须能够执行以下操作：

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

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

示例：允许用户查看自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

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

示例：允许组织管理账户指定和移除委托的管理员

此示例展示了如何创建一项策略来允许 AWS Organizations 组织管理账户的用户为其组织指定和移除委托的 Security Lake 管理员。

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

示例：允许用户根据标签查看订阅用户

在基于身份的策略中，您可以使用条件基于标签来控制对 Security Lake 资源的访问。本示例展示了如何创建允许用户使用 Security Lake 控制台或 Security Lake API 查看订阅用户的策略。但是，只有当订阅用户的 Owner 标签的值是用户的用户名时，系统才会授予权限。

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

在本示例中，如果用户名为 richard-roe 的用户试图查看某个订阅用户的详细信息，则该订阅用户必须标记为 Owner=richard-roe 或 owner=richard-roe。否则，该用户将被拒绝访问。条件标签键 Owner 匹配 Owner 和 owner，因为条件键名称不区分大小写。有关条件键的更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html中的 IAM JSON 策略元素：条件。有关标记 Security Lake 资源的更多信息，请参阅为 Amazon Security Lake 资源添加标签。

AWS Amazon 安全湖的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略： AmazonSecurityLakeMetastoreManager

Amazon Security Lake 使用一项 AWS Lambda 功能来管理您的数据湖中的元数据。通过使用此功能，Security Lake 可以将包含您的数据和数据文件的亚马逊简单存储服务 (Amazon S3) Service 分区索引到数据目录 AWS Glue 表中。此托管策略包含 Lambda 函数将 S3 分区和数据文件索引到表中的 AWS Glue 所有权限。

权限详细信息

该策略包含以下权限：

- logs— 允许委托人将 Lambda 函数的输出记录到 Amazon CloudWatch 日志。
- glue— 允许委托人对 AWS Glue 数据目录表执行特定的写入操作。这也允许 AWS Glue 抓取工具识别您的数据中的分区。
- sqs— 允许委托人对在数据湖中添加或更新对象时发送事件通知的 Amazon SQS 队列执行特定的读写操作。
- s3— 允许委托人对包含您的数据的 Amazon S3 存储桶执行特定的读取和写入操作。

```
{
  "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 托管策略： AmazonSecurityLakePermissionsBoundary

Amazon Security Lake 会为第三方自定义源创建 IAM 角色以将数据写入数据湖，为第三方自定义订阅用户创建 IAM 角色以使用数据湖中的数据，并在创建这些角色时使用此策略来定义其权限边界。您无需执行任何操作即可使用此策略。如果使用客户管理的 AWS KMS 密钥对数据湖进行加密`kms:Decrypt`，则添加了`kms:GenerateDataKey`权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
```

```
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
```

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

```
    {
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:sqs:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:sqs:arn": [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

AWS 托管策略： AmazonSecurityLakeAdministrator

您可以在某个主体为其账户启用 Amazon Security Lake 之前为该主体附加 `AmazonSecurityLakeAdministrator` 策略。此策略授予管理权限，允许主体拥有对所有 Security Lake 操作的完全访问权限。之后，该主体便可注册到 Security Lake 中，并在 Security Lake 中配置来源和订阅用户。

该策略包括 Security Lake 管理员可通过 Security Lake 对其他 AWS 服务执行的操作。

该`AmazonSecurityLakeAdministrator`政策不支持创建 Security Lake 所需的实用程序角色来管理 Amazon S3 跨区域复制、在中注册新的数据分区 AWS Glue、对添加到自定义源的数据运行 Glue 爬虫或通知 HTTPS 终端节点订阅者新数据。您可以按照 Amazon Security Lake 入门中的说明提前创建这些角色。

除 `AmazonSecurityLakeAdministrator` 托管式策略外，Security Lake 还需要 `lakeformation:PutDataLakeSettings` 权限来执行注册和配置功能。`PutDataLakeSettings` 允许将某个 IAM 主体设置为账户中所有区域 Lake Formation 资源的管理员。该角色必须同时附加有 `iam:CreateRole permission` 权限和 `AmazonSecurityLakeAdministrator` 策略。

Lake Formation 管理员拥有对 Lake Formation 控制台的完全访问权限，并且可以控制初始数据配置和访问权限。Security Lake 会将启用 Security Lake 的主体和

AmazonSecurityLakeMetaStoreManager 角色（或其他指定角色）指定为 Lake Formation 管理员，以便他们可以创建表、更新表架构、注册新分区以及配置表的权限。您必须在 Security Lake 管理员用户或角色的策略中包含以下权限：

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

权限详细信息

该策略包含以下权限。

- securitylake – 允许主体对所有 Security Lake 操作拥有完全访问权限。
- organizations – 允许主体通过 AWS Organizations 检索有关组织中的账户的信息。如果账户属于某个组织，则这些权限允许 Security Lake 控制台显示账户名称和账号。
- iam— 允许委托人在 Security Lake、 AWS Lake Formation、和中创建服务相关角色 Amazon EventBridge，这是启用这些服务时的必需步骤。同时，还允许为订阅用户和自定义来源角色创建和编辑策略，这些角色中的权限仅限于 AmazonSecurityLakePermissionsBoundary 策略允许的权限。
- ram— 允许委托人配置订阅者对 Security Lake 源的 Lake Formation基于查询的访问权限。
- s3– 允许主体创建和管理 Security Lake 桶并读取这些桶的内容。
- lambda— 允许委托人管理 Lambda 用于在 AWS 源数据传输和跨区域复制之后更新 AWS Glue 表分区。

- glue – 允许主体创建和管理 Security Lake 数据库和表。
- lakeformation— 允许委托人管理 Security Lake 表的 Lake Formation 权限。
- events – 允许主体管理用于在新数据写入 Security Lake 来源时通知订阅用户的规则。
- sqs— 允许委托人创建和管理 Amazon SQS 队列，用于向订阅者通知 Security Lake 源中的新数据。
- kms – 允许主体向 Security Lake 授予使用客户托管密钥写入数据的访问权限。
- secretsmanager – 允许主体管理用于在新数据通过 HTTPS 端点写入 Security Lake 来源时通知订阅用户的密钥。

```
{
"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 托管策略： SecurityLakeServiceLinkedRole

您不能将 `SecurityLakeServiceLinkedRole` 托管式策略附加到您的 IAM 实体。此策略附加到服务相关角色，允许 Security Lake 代表您执行操作。有关更多信息，请参阅 Amazon Security Lake 的服务相关角色。

AWS 托管策略： AWS GlueServiceRole

`AWS GlueServiceRole`托管策略调用 AWS Glue 爬虫并允许 AWS Glue 抓取自定义源数据和识别分区元数据。在数据目录中创建和更新表需要这些元数据。

有关更多信息，请参阅 从自定义源收集数据。

安全湖对 AWS 托管策略的更新

查看自该服务开始跟踪这些更改以来 Security Lake AWS 托管策略更新的详细信息。有关此页面更改的自动提示，请订阅“Security Lake 文档”历史记录页面上的 RSS 源。

更改	描述	日期
AmazonSecurityLakeMetastoreManager – 对现有策略的更新	Security Lake 更新了政策，添加了元数据清理操作，允许您删除数据湖中的元数据。	2024 年 3 月 27 日
AmazonSecurityLakeAdministrator – 更新了现有策略	Security Lake 更新了政策，允许使用`iam:PassR`	2024 年 2 月 23 日

更改	描述	日期
	ole 新AmazonSecurityLakeMetastoreManagerV2 角色，并允许 Security Lake 部署或更新数据湖组件。	
AmazonSecurityLakeMetastoreManager：新策略	Security Lake 添加了一个新的托管策略，该策略向 Security Lake 授予管理数据湖中元数据的权限。	2024 年 1 月 23 日
AmazonSecurityLakeAdministrator：新策略	Security Lake 添加了一项新的托管策略，允许委托人完全访问所有 Security Lake 操作。	2023 年 5 月 30 日
Security Lake 开始跟踪更改	Security Lake 开始跟踪其 AWS 托管策略的变更。	2022 年 11 月 29 日

Amazon Security Lake 的服务相关角色

Security Lake 使用名为 AWSServiceRoleForSecurityLake 的 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Security Lake 直接关联的 IAM 角色。这一角色由 Security Lake 预定义，包含 Security Lake 为您调用其他 AWS 服务 并运行安全数据胡服务所需的所有权限。Security Lake 在提供 Security Lake 的所有 AWS 区域都使用这一服务相关角色。

利用服务相关角色，您在设置 Security Lake 时不需要手动添加必要的权限。Security Lake 会定义这一服务相关角色的权限，而且除非另有定义，否则只有 Security Lake 可以担任该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的服务相关角色权限。只有在删除服务相关角色的相关资源后，您才能删除该角色。这可以保护您的资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 AWS 服务，并查找 Service-linked roles（服务相关角色）列中显示为 Yes（是）的服务。选择带有链接的是可以查看该服务的服务相关角色文档。

主题

Security Lake 的服务相关角色权限

Security Lake 使用名为 `AWSServiceRoleForSecurityLake` 的服务相关角色。该服务相关角色信任 `securitylake.amazonaws.com` 服务担任该角色。

该角色的权限策略是一项名为 `SecurityLakeServiceLinkedRole` 的 AWS 托管式策略，允许 Security Lake 创建和运行安全数据湖。该策略还允许 Security Lake 对指定资源执行以下操作：

- 使用 AWS Organizations 操作来检索有关关联账户的信息
- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 检索有关 Amazon VPC 流日志的信息
- 使用 AWS CloudTrail 操作来检索有关服务相关角色的信息

该角色使用以下权限策略进行配置：

```
{
    "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"
```

```
                }
            }
        }
    ]
}
```

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

创建 Security Lake 服务相关角色

您不需要为 Security Lake 手动创建 AWSServiceRoleForSecurityLake 服务相关角色。当您为自己的 AWS 账户启用 Security Lake 时，Security Lake 会自动为您创建服务相关角色。

创建 Security Lake 服务相关角色

Security Lake 不允许您编辑 AWSServiceRoleForSecurityLake 服务相关角色。在创建服务相关角色后，您无法更改角色的名称，因为可能有多个实体会引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

删除 Security Lake 服务相关角色

您无法从 Security Lake 中删除服务相关角色。您可以通过 IAM 控制台、API 或 AWS CLI 删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

您必须先确认服务相关角色没有活动会话并删除 AWSServiceRoleForSecurityLake 使用的任何资源，然后才能删除服务相关角色。

> **Note**
>
> 在您尝试删除资源时，如果 Security Lake 正在使用 AWSServiceRoleForSecurityLake 角色，删除可能会失败。如果发生这种情况，请等待几分钟，然后再次尝试操作。

如果您在删除 AWSServiceRoleForSecurityLake 服务相关角色后需要再次创建该角色，可以通过为账户启用 Security Lake 来再次创建角色。当您再次启用 Security Lake 时，Security Lake 会再次自动为您创建服务相关角色。

支持 Security Lake 服务相关角色的 AWS 区域

Security Lake 在提供 Security Lake 的所有 AWS 区域 都支持使用 `AWSServiceRoleForSecurityLake` 服务相关角色。有关提供 Security Lake 的区域的列表，请参阅 Amazon Security Lake 区域和端点。

Amazon Security Sake 中的数据保护

AWS 责任共担模式适用于 Amazon Security Lake 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API、AWS CLI 或 AWS SDK 处理 Security Lake 或其他 AWS 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，我们强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

Amazon Security Lake 使用 AWS 加密解决方案安全地存储静态数据。原始安全日志和事件数据存储在由 Security Lake 管理的账户中的一个多租户 Amazon Simple Storage Service（Amazon S3）桶中。Security Lake 使用来自 AWS Key Management Service (AWS KMS) 的 AWS 拥有的密钥对这些

原始数据进行加密。AWS 拥有的密钥是 AWS 服务（在本例中为 Security Lake）拥有和管理的 AWS KMS 密钥的集合，可在多个 AWS 账户中使用。

Security Lake 对原始日志和事件数据运行提取、转换和加载（ETL）任务。处理后的数据在 Security Lake 服务账户中保持加密状态。

ETL 任务完成后，Security Lake 会在您的账户中创建单租户 S3 桶（每个桶对应于您启用了 Security Lake 的每个 AWS 区域）。数据仅临时存储在多租户 S3 桶中，直到 Security Lake 能够可靠地将数据传输到单租户 S3 桶。单租户桶包含一个基于资源的策略，该策略授予 Security Lake 向桶写入日志和事件数据的权限。要加密 S3 桶中的数据，您可以选择 S3 托管加密密钥或客户托管密钥（来自 AWS KMS）。两者都使用对称加密。

使用 KMS 密钥加密您的数据

默认情况下，Security Lake 传输到 S3 桶的数据使用 Amazon S3 托管的加密密钥（SSE-S3）进行 Amazon 服务器端加密。为了提供您可以直接管理的安全层，可以改为针对 Security Lake 数据使用AWS KMS 密钥（SSE-KMS）进行服务器端加密。

Security Lake 控制台不支持 SSE-KMS。要将 SSE-KMS 用于 Security Lake API 或 CLI，请先创建 KMS 密钥或使用现有密钥。您需要向密钥附加一个策略，规定哪些用户可以使用该密钥加密和解密 Security Lake 数据。

如果使用客户托管密钥来加密写入到 S3 桶的数据，则无法选择多区域密钥。对于客户托管密钥，Security Lake 将通过向 AWS KMS 发送 `CreateGrant` 请求来代表您创建授权。AWS KMS 中的授权用于授予 Security Lake 对客户账户中的 KMS 密钥的访问权限。

Security Lake 需要该授权才能将客户托管密钥用于以下内部操作：

- 将 `GenerateDataKey` 请求发送到 AWS KMS，以生成由客户托管密钥加密的数据密钥。
- 将 `RetireGrant` 请求发送到 AWS KMS。当您对数据湖进行更新时，此操作将导致添加到 AWS KMS 密钥以用于 ETL 处理的授权停用。

Security Lake 不需要 `Decrypt` 权限。当密钥的授权用户读取 Security Lake 数据时，S3 将管理解密，授权用户可以读取未加密形式的数据。但是，订阅用户需要 `Decrypt` 权限才能使用源数据。有关订阅用户的更多信息，请参阅管理 Security Lake 订阅用户的数据访问权限。

创建密钥策略或使用具有适当权限的现有密钥策略时，您的 KMS 密钥可以接受授权请求，从而允许 Security Lake 访问该密钥。有关创建密钥策略的说明，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥策略。将以下密钥策略附加到您的 KMS 密钥：

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

使用客户托管密钥时所需的 IAM 权限

有关使用 Security Lake 时需要创建的 IAM 角色的概述，请参阅入门：先决条件部分。

添加自定义源或订阅用户时，Security Lake 会在您的账户中创建 IAM 角色。这些角色将与其他 IAM 身份共享。它们允许自定义源向数据湖写入数据，并允许订阅用户使用数据湖中的数据。名为 `AmazonSecurityLakePermissionsBoundary` 的 AWS 托管式策略将为这些角色设置权限边界。

加密 Amazon SQS 队列

创建数据湖时，Security Lake 会在委派的 Security Lake 管理员账户中创建两个未加密的 Amazon Simple Queue Service (Amazon SQS) 队列。您应该加密这些队列以保护您的数据。Amazon Simple Queue Service 提供的默认服务器端加密 (SSE) 是不够的。您必须在 AWS Key Management Service (AWS KMS) 中创建客户托管密钥来加密队列，然后授予 Amazon S3 服务主体使用加密队列的权限。有关授予这些权限的说明，请参阅 AWS 知识中心中的为什么 Amazon S3 事件通知没有发送到使用服务器端加密的 Amazon SQS 队列？

由于 Security Lake 使用 AWS Lambda 来支持对您的数据执行提取、传输和加载 (ETL) 任务，因此您还必须向 Lambda 授予管理您的 Amazon SQS 队列中消息的权限。有关信息，请参阅《AWS Lambda 开发人员指南》中的执行角色权限。

传输中加密

Security Lake 将加密 AWS 服务之间的所有传输中数据。通过使用传输层安全（TLS）1.2 加密协议自动加密所有网络间数据，Security Lake 在传输中数据进出服务时对其进行保护。发送到 Security Lake API 的直接 HTTPS 请求使用 AWS 签名版本 4 算法进行签名，以建立安全连接。

选择不使用您的数据来改善服务

您可以使用 AWS Organizations 选择退出政策，选择不将您的数据用于开发和改进 Security Lake 和其他 AWS 安全服务。即使 Security Lake 目前未收集任何此类数据，您也可以选择退出。有关如何选择退出的更多信息，请参阅《AWS Organizations 用户指南》中的 AI 服务选择退出政策。

目前，Security Lake 不会收集它代表您处理的任何安全数据，也不会收集您上传到由此服务创建的安全数据湖的安全数据。为了开发和改进 Security Lake 服务和其他 AWS 安全服务的功能，Security Lake 将来可能会收集此类数据，包括您从第三方数据源上传的数据。我们将在 Security Lake 打算收集任何此类数据时更新本页面，并说明其工作方式。您仍有机会随时选择退出。

> **Note**
>
> 要使用选择退出政策，您的 AWS 账户必须由 AWS Organizations 集中管理。如果您尚未为自己的 AWS 账户创建组织，请参阅《AWS Organizations 用户指南》中的创建和管理组织。

选择退出会带来以下影响：

- Security Lake 将删除在您选择退出之前它收集和存储的数据（如果有）。
- 在您选择退出后，Security Lake 不会再收集或存储这些数据。

Amazon Security Lake 的合规性验证

要了解某个 AWS 服务是否在特定合规性计划范围内，请参阅 合规性计划范围内的 AWS 服务，然后选择您感兴趣的合规性计划。有关常规信息，请参阅AWS 合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 AWS Artifact 中下载报告、。

您使用 AWS 服务 的合规性责任取决于数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南——这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署以安全性和合规性为重点的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计 – 该白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。

> **Note**
>
> 并非所有 AWS 服务 都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS 客户合规指南：从合规角度了解责任共担模式。这些指南总结了保护 AWS 服务 的最佳实践，并将指南映射到跨多个框架的安全控制，包括美国国家标准与技术研究院（NIST）、支付卡行业安全标准委员会（PCI）和国际标准化组织（ISO）。
- AWS Config 开发人员指南中的使用规则评估资源 – 此 AWS Config 服务评测您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub——此 AWS 服务 向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实操。有关受支持服务及控制的列表，请参阅 Security Hub 控制参考。
- AWS Audit Manager：此 AWS 服务 可帮助您持续审核您的 AWS 使用情况，以简化管理风险以及与相关法规和行业标准的合规性的方式。

Security Lake 的安全最佳实践

请参阅以下有关使用 Amazon Security Lake 的最佳实践。

授予 Security Lake 用户可能的最低权限

遵循最低权限原则，为 AWS Identity and Access Management (IAM) 用户、用户组和角色授予最少的访问策略权限。例如，您可以允许 IAM 用户查看 Security Lake 中的日志源列表，但不允许其创建日志源或订阅用户。有关更多信息，请参阅Amazon Security Lake 基于身份的策略示例。

您还可以使用 AWS CloudTrail 跟踪 Security Lake 中的 API 使用情况。CloudTrail 提供了用户、组或角色在 Security Lake 中执行的 API 操作的记录。有关更多信息，请参阅使用 AWS CloudTrail 记录 Amazon Security Lake API 调用。

查看摘要页面

Security Lake 控制台的摘要页面概述了过去 14 天内影响 Security Lake 服务和用于存储数据的 Amazon S3 桶的问题。您可以进一步调查这些问题，以帮助您减轻可能与安全相关的影响。

与 Security Hub 集成

将 Security Lake 与 AWS Security Hub 集成，以便在 Security Lake 中接收 Security Hub 的调查发现。Security Hub 可从许多不同的 AWS 服务和第三方集成生成调查发现。接收 Security Hub 调查发现可以帮助您全面了解您的合规状况，以及您是否遵守了 AWS 安全最佳实践。

有关更多信息，请参阅与集成 AWS Security Hub。

监控 Security Lake 事件

您可以使用 Amazon CloudWatch 指标监控 Security Lake。CloudWatch 每分钟收集来自 Security Lake 的原始数据，并将其处理为指标。您可以设置警报，在指标达到指定阈值时触发通知。

有关更多信息，请参阅Amazon Security Lake 的 CloudWatch 指标。

Amazon Security Lake 中的故障恢复能力

AWS 全球基础设施围绕 AWS 区域 和可用区构建。AWS 区域 提供多个在物理上独立且隔离的可用区，这些可用区与延迟率低、吞吐量高且冗余性高的网络连接在一起。这些可用区为您提供了高效的方法来设计和操作应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

Security Lake 的可用性与区域可用性息息相关。分布在多个可用区有助于该服务在任意一个可用区发生故障时依旧保持可用性。

Security Lake 数据面板的可用性与区域可用性无关。但是，Security Lake 控制面板的可用性与美国东部（弗吉尼亚州北部）区域的可用性密切相关。

有关 AWS 区域 和可用区的更多信息，请参阅 AWS 全球基础设施。

除了 AWS 全球基础设施之外，Security Lake（其中的数据由 Amazon Simple Storage Service (Amazon S3) 提供支持）也提供了多种功能来帮助满足您的数据恢复和备份需求。

生命周期配置

> 生命周期配置是一组规则，用于定义 Amazon S3 对一组对象应用的操作。利用生命周期配置规则，您可以指示 Amazon S3 将对象转换为较低成本的存储类，或者归档或删除它们。有关更多信息，请参阅《Amazon S3 用户指南》中的对象生命周期管理。

版本控制

版本控制是在相同的桶中保留对象的多个变量的方法。对于 Amazon S3 桶中存储的每个对象，您可以使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您从用户意外操作和应用程序故障中恢复。有关更多信息，请参阅《Amazon S3 用户指南》中的在 S3 桶中使用版本控制。

存储类

Amazon S3 提供一系列存储类，可供选择，具体取决于您的工作负载要求。S3 Standard-IA 和 S3 One Zone-IA 存储类用于大约每月访问一次且需要毫秒访问的数据。S3 Glacier Instant Retrieval 存储类专为长期归档数据而设计，您可以访问几毫秒的访问权限，大约每季度访问一次。对于不需要立即访问的归档数据，例如备份，您可以使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。有关更多信息，请参阅《Amazon S3 用户指南》中的使用 Amazon S3 存储类。

Amazon Security Lake 中的基础设施安全性

作为一项托管式服务，Amazon Security Lake 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问 Security Lake。客户端必须支持以下内容：

- 传输层安全性协议（TLS） 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（Ephemeral Diffie-Hellman）或 ECDHE（Elliptic Curve Ephemeral Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

Security Lake 中的配置和脆弱性分析

配置和 IT 控制是AWS和您（我们的客户）之间的共同责任。有关更多信息，请参阅AWS责任共担模型。

监控 Amazon Security Lake

Security Lake 与 AWS CloudTrail 集成，后者可提供用户、角色或其他 AWS 服务在 Security Lake 中所执行的操作的记录。这包括来自 Security Lake 控制台的操作以及对 Security Lake API 操作的编程调用。通过使用 CloudTrail 收集的信息，您可以确定向 Security Lake 发出了哪些请求。您可以确定每个请求的发出时间、来源 IP 地址、请求方以及其他详细信息。有关更多信息，请参阅使用 AWS CloudTrail 记录 Amazon Security Lake API 调用。

Security Lake 和 Amazon CloudWatch 集成，因此您可以收集、查看和分析 Security Lake 收集的日志指标。Security Lake 数据湖的 CloudWatch 指标是自动收集的，并以一分钟为间隔推送到 CloudWatch。您还可以设置警报，以便在达到某个 Security Lake 指标的指定阈值时向您发送通知。有关 Security Lake 发送到 CloudWatch 的所有指标的列表，请参阅 Security Lake 指标和维度。

Amazon Security Lake 的 CloudWatch 指标

您可以使用 Amazon CloudWatch 监控 Security Lake，此工具每分钟收集一次原始数据并将其处理为易读的近乎实时的指标。这些统计数据会保存 15 个月，使您能够访问历史信息并更好地了解数据湖中的数据。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。

主题

- Security Lake 指标和维度
- 查看 Security Lake 的 CloudWatch 指标
- 为 Security Lake 指标设置 CloudWatch 警报

Security Lake 指标和维度

`AWS/SecurityLake` 命名空间包括以下指标。

指标	描述
`ProcessedSize`	当前存储在数据湖中并来自原生支持的 AWS 服务的数据量。 单位：字节

下列维度可用于 Security Lake 指标。

维度	描述
Account	特定 AWS 账户的 ProcessedSize 指标。仅当您在 CloudWatch 上查看 Per-Account Source Version Metrics 时，此维度才可用。
Region	特定 AWS 区域的 ProcessedSize 指标。
Source	特定 AWS 日志源的 ProcessedSize 指标。
SourceVersion	特定版本的 AWS 日志源的 ProcessedSize 指标。

您可以查看特定 AWS 账户的指标 (Per-Account Source Version Metrics) 或组织中所有账户的指标 (Per-Source Version Metrics)。

查看 Security Lake 的 CloudWatch 指标

您可以使用 CloudWatch 控制台、CloudWatch 自己的命令行界面（CLI）或者通过以编程方式使用 CloudWatch API 来监控 Security Lake 的指标。选择您的首选方法，然后按照以下步骤访问 Security Lake 指标。

CloudWatch console

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择指标、所有指标。
3. 在浏览选项卡上，选择 Security Lake。
4. 选择每个账户的源版本指标或每个源版本指标。
5. 选择一个指标以查看其详细信息。您还可以选择执行以下操作：
   - 要对指标进行排序，请使用列标题。
   - 要绘制指标图表，请选择指标名称，然后选择一个绘图选项。
   - 要按指标进行筛选，请选择指标名称，然后选择添加到搜索。

CloudWatch API

要使用 CloudWatch API 访问 Security Lake 指标，请使用 `GetMetricStatistics` 操作。

AWS CLI

要使用 AWS CLI 访问 Security Lake 指标，请运行 `get-metric-statistics` 命令。

有关使用指标进行监控的更多信息，请参阅《Amazon CloudWatch 用户指南》中的使用 Amazon CloudWatch 指标。

为 Security Lake 指标设置 CloudWatch 警报

此外，CloudWatch 还允许您设置指标达到阈值时的告警。例如，您可以为 ProcessedSize 指标设置警报，以便在来自特定源的数据量超过特定阈值时收到通知。

有关设置警报的说明，请参阅《CloudWatch 用户指南》中的使用 Amazon CloudWatch 警报。

使用 AWS CloudTrail 记录 Amazon Security Lake API 调用

Amazon Security Lake 与 AWS CloudTrail 集成，后者可提供用户、角色或 AWS 服务在 Security Lake 中所执行操作的记录。CloudTrail 将 Security Lake 的 API 调用捕获为事件。捕获的调用包括来自 Security Lake 控制台的调用以及对 Security Lake API 操作的代码调用。如果您创建跟踪记录，可以将 CloudTrail 事件持续传送到 Amazon S3 桶（包括 Security Lake 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 Security Lake 发出了什么请求、发出请求的 IP 地址、请求方、请求时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 中的 Security Lake 信息

CloudTrail 将在您创建 AWS 账户时在该账户上启用。当 Security Lake 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其它 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 Security Lake 的事件），请创建跟踪。利用跟踪，CloudTrail 可以将事件作为日志文件传送至您指定的 Amazon S3 桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有 Security Lake 操作，Security Lake API 参考中介绍了这些操作。例如，对 `UpdateDataLake`、`ListLogSources` 和 `CreateSubscriber` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management 用户凭证发出的。

- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Security Lake 日志文件条目

CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例显示了用于 Security Lake `GetSubscriber` 操作的 CloudTrail 日志条目。


```
{
   "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"
}
```

为 Amazon Security Lake 资源添加标签

标签是一个可选标签，您可以定义并分配给 AWS 资源，包括某些类型的 Amazon Security Lake 资源。标签可帮助您以不同方式（例如按用途、所有者、环境或其他标准）对资源进行标识、分类和管理。例如，您可以使用标签来应用策略、分配成本、区分资源或识别支持某些合规性要求或工作流的资源。

您可以为以下类型的 Security Lake 资源分配标签：订阅者和您的 AWS 账户 个人数据湖配置 AWS 区域。

主题

标签基础知识

一个资源可具有多达 50 个标签。每个标签都包含您定义的一个标签键和一个可选的标签值。标签键是一种常见的标签，充当更具体的标签值的类别。标签值 充当标签键的描述符。

例如，如果您添加订阅用户来分析来自不同环境的安全数据（一组订阅用户用于云数据，另一组用于本地数据），则可以为这些订阅用户分配 `Environment` 标签键。关联的标签值可能`Cloud`适用于分析来自的数据的订阅者 AWS 服务，也可能`On-Premises`适用于其他用户。

在为 Amazon Security Lake 资源定义和分配标签时，请注意以下几点：

- 每个资源最多可以有 50 个标签。
- 对于每个资源，每个标签键都必须是唯一的，并且只能有一个标签值。
- 标签键和值区分大小写。作为最佳实践，我们建议您定义标签大写的策略，并在您的资源中一致地实施该策略。
- 标签键最多可以包含 128 个 UTF-8 字符。标签值最多可以包含 256 个 UTF-8 字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @

- 前aws:缀保留给使用 AWS。您不能在您定义的任何标签键或值中使用它。此外，您无法更改或删除使用此前缀的标签键或值。使用此前缀的标签不计入每个资源的 50 个标签配额中。
- 您分配的任何标签仅供您使用， AWS 账户 并且仅适用于您分配标签 AWS 区域 的标记。
- 如果您使用 Security Lake 为资源分配标签，则这些标签仅应用于适用 AWS 区域内直接存储在 Security Lake 中的资源。它们不适用于 Security Lake 在其他 AWS 服务中为您创建、使用或维护的任何关联支持资源。例如，如果您为数据湖分配标签，则这些标签仅应用于指定区域内 Security Lake 中的数据湖配置。它们不适用于存储日志和事件数据的 Amazon Simple Storage Service (Amazon S3) 桶。要同时为关联资源分配标签，您可以使用 AWS Resource Groups 或来存储资源，例如 AWS 服务 ，用于 S3 存储桶的 Amazon S3。为关联资源分配标签可帮助您标识数据湖的支持资源。
- 如果删除资源，则为该资源分配的所有标签都将被删除。

有关其他限制、提示和最佳实践，请参阅《标记 AWS 资源用户指南》中的为 AWS 资源添加标签。

> **Important**
>
> 不要在标签中存储机密或其他类型的敏感数据。许多人都可以访问标签 AWS 服务，包括 AWS Billing and Cost Management。标签不适合用于敏感数据。

要为 Security Lake 资源添加和管理标签，您可以使用 Security Lake 控制台或 Security Lake API。

在 IAM policy 中使用标签

开始为资源添加标签后，您可以在 AWS Identity and Access Management (IAM) policy 中定义基于标签的资源级权限。通过以这种方式使用标签，您可以精细控制您中的哪些用户和角色 AWS 账户 有权创建和标记资源，以及哪些用户和角色有权更笼统地添加、编辑和删除标签。要基于标签控制访问，您可以在 IAM policy 的 Condition 元素中使用与标签相关的条件键。

例如，您可以创建一个策略，允许用户拥有对所有 Amazon Security Lake 资源的完全访问权限，但前提是该资源的 Owner 标签指定了他们的用户名：

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

```
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

如果您定义基于标签的资源级权限，该权限立即生效。这意味着，您的资源在创建后会更安全，而且您可以快速开始将标签用于新资源。您还可以使用资源级权限来控制哪些标签键和值可以与新的和现有资源关联。有关更多信息，请参阅 IAM 用户指南中的使用标签控制对 AWS 资源的访问权限。

为 Amazon Security Lake 资源添加标签

要为 Amazon Security Lake 资源添加标签，您可以使用 Security Lake 控制台或 Security Lake API。

> **Important**
>
> 为资源添加标签可能会影响对该资源的访问。在向资源添加标签之前，请查看任何可能使用标签控制资源访问权限的 AWS Identity and Access Management (IAM) 策略。

Console

当您为订阅者启用 Security Lake AWS 区域 或创建订阅者时，Security Lake 控制台会提供向资源添加标签的选项，即区域或订阅者的数据湖配置。创建资源时，请按照控制台上的说明为该资源添加标签。

要使用 Security Lake 控制台为现有资源添加一个或多个标签，请按照以下步骤操作。

为资源添加标签

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 根据要为其添加标签的资源类型，执行以下任一操作：
   - 对于数据湖配置，在导航窗格中选择区域。然后，在区域表中，选择区域。
   - 对于订阅用户，在导航窗格中选择订阅用户。然后，在我的订阅用户表中，选择订阅用户。

如果该订阅用户不在表中，请使用页面右上角的 AWS 区域 选择器，选择在其中创建了该订阅用户的区域。该表仅列出当前区域的现有订阅用户。

3. 选择编辑。
4. 展开标签部分。本部分列出当前分配给该资源的所有标签。
5. 在标签部分中，选择添加新标签。
6. 在键框中，输入要为该资源添加的标签的标签键。随后，在值框中，可以选择为键输入一个标签值。

   一个标签键可包含多达 128 个字符。一个标签值可包含多达 256 个字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @
7. 要为该资源添加其他标签，请选择添加新标签，然后重复上述步骤。您可以为资源分配多达 50 个标签。
8. 完成添加标签后，选择 保存。

API

要创建资源并以编程方式向其添加一个或多个标签，请对要创建的资源类型使用相应的 `Create` 操作：

- 数据湖配置-使用CreateDataLake操作，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，则运行create-data-lake命令。
- 订阅者-使用CreateSubscriber操作，或者，如果您使用的是，则运行 create- subscriber 命令。AWS CLI

在您的请求中，使用 `tags` 形式参数为要添加到资源的每个标签指定标签键 (`key`) 和可选标签值 (`value`)。`tags` 形式参数指定一个对象数组。每个对象都指定一个标签密钥及其关联的标签值。

要向现有资源添加一个或多个标签，请使用 Security Lake API 的TagResource操作，或者，如果您使用的是 AWS CLI，则运行 tag-resou rce 命令。在您的请求中，指定您要向其添加标签的资源的 Amazon 资源名称（ARN）。使用 `tags` 形式参数为要添加的每个标签指定标签键 (`key`) 和可选标签值 (`value`)。与 `Create` 操作和命令一样，`tags` 形式参数指定一个对象数组，每个标签键及其关联的标签值对应一个对象。

例如，以下 AWS CLI 命令将带有`EnvironmentCloud`标签值的标签密钥添加到指定的订阅者。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

其中：

- `resource-arn` 指定要为其添加标签的订阅用户的 ARN。
- *`Environment`* 是要为订阅用户添加的标签的标签键。
- *`Cloud`* 是指定标签键 (*`Environment`*) 的标签值。

在以下示例中，该命令为订阅用户添加多个标签。

```
$ 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
```

对于 `tags` 数组中的每个对象，都需要 `key` 和 `value` 实际参数。但是，`value` 参数的值可以是空字符串。如果您不想将标签值与标签键相关联，请不要为 `value` 参数指定值。例如，以下命令添加一个没有关联标签值的 `Owner` 标签键：

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

如果添加标签操作成功，Security Lake 将返回一个空的 HTTP 200 响应。否则，Security Lake 将返回 HTTP 4xx 或 500 响应，并说明操作失败的原因。

查看 Amazon Security Lake 资源的标签

您可以使用 Security Lake 控制台或 Security Lake API 查看 Amazon Security Lake 资源的标签（包括标签键和标签值）。

Console

按照以下步骤，使用 Security Lake 控制台查看资源的标签。

查看资源的标签

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 根据要查看其标签的资源类型，执行以下任一操作：

   - 对于数据湖配置，在导航窗格中选择区域。在区域表中，选择区域，然后选择编辑。之后，展开标签部分。
   - 对于订阅用户，在导航窗格中选择订阅用户。然后，在我的订阅用户表中，选择订阅用户的名称。

     如果该订阅用户不在表中，请使用页面右上角的 AWS 区域 选择器，选择在其中创建了该订阅用户的区域。该表仅列出当前区域的现有订阅用户。

标签部分列出当前分配给该资源的所有标签。

API

要以编程方式检索和查看现有资源的标签，请使用 Security Lake API 的ListTagsForResource操作。在您的请求中，使用 `resourceArn` 参数指定资源的 Amazon 资源名称（ARN）。

如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行list-tags-for-resource命令并使用`resource-arn`参数指定资源的 ARN。例如：

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

在上述示例中，*arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab* 是现有订阅用户的 ARN。

如果操作成功，Security Lake 将返回一个 `tags` 数组。该数组中的每个对象都指定了当前分配给该资源的标签（包括标签键和标签值）。例如：

```
{
    "tags": [
        {
```

```
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

其中 Environment、CostCenter 和 Owner 是分配给资源的标签键。Cloud 是与 Environment 标签键关联的标签值。12345 是与 CostCenter 标签键关联的标签值。Owner 标签密钥没有关联的标签值。

编辑 Amazon Security Lake 资源的标签

要编辑 Amazon Security Lake 资源的标签（标签键或标签值），您可以使用 Security Lake 控制台或 Security Lake API。

> **Important**
>
> 编辑资源的标签可能会影响对该资源的访问。在编辑资源的标签键或值之前，请查看可能使用该标签控制资源访问权限的任何 AWS Identity and Access Management (IAM) 策略。

Console

按照以下步骤，使用 Security Lake 控制台编辑资源的标签。

编辑资源的标签

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 根据要编辑其标签的资源类型，执行以下任一操作：
   - 对于数据湖配置，在导航窗格中选择区域。然后，在区域表中，选择区域。
   - 对于订阅用户，在导航窗格中选择订阅用户。然后，在我的订阅用户表中，选择订阅用户。

如果该订阅用户不在表中，请使用页面右上角的 AWS 区域 选择器，选择在其中创建了该订阅用户的区域。该表仅列出当前区域的现有订阅用户。

3. 选择编辑。
4. 展开标签部分。标签部分列出当前分配给该资源的所有标签。
5. 执行以下任一操作：

   - 要为现有标签键添加标签值，请在标签键旁边的值框中输入值。
   - 要更改现有标签键，请选择标签旁边的删除。然后，选择添加新标签。在出现的键框中，输入新的标签键。在值框中，可以选择输入相关的标签值。
   - 要更改现有标签值，请在包含该值的 值框中选择 X。然后在值框中键入新的标签值。
   - 要删除现有标签值，请在包含该值的 值框中选择 X。
   - 要删除现有标签（标签键和标签值），请选择标签旁边的 移除。

   一个资源可具有多达 50 个标签。一个标签键可包含多达 128 个字符。一个标签值可包含多达 256 个字符。这些字符可以是字母、数字、空格或以下符号：_ . : / = + - @
6. 完成对标签的编辑之后，选择 保存。

API

当您以编程方式编辑资源的标签时，会用新值覆盖现有标签。因此，编辑标签的最佳方法取决于您是要编辑标签键、标签值还是两者都有。要编辑标签密钥，请删除当前标签并添加新标签。

要仅编辑或删除与标签键关联的标签值，请使用 Security Lake API 的TagResource操作覆盖现有值。如果您使用的是 AWS Command Line Interface (AWS CLI)，则运行 tag-resource 命令。在您的请求中，指定要编辑或删除其标签值的资源的 Amazon 资源名称 (ARN)。

要编辑标签值，请使用 `tags` 形式参数指定要更改其标签值的标签键。另外，还要指定该标签键的新标签值。例如，以下 AWS CLI 命令将分配给指定订阅`On-Premises`者的`Environment`标签密钥的标签值从`Cloud`更改为。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ 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
```

其中：

- `resource-arn` 指定订阅用户的 ARN。
- *`Environment`* 是与要更改的标签值关联的标签键。
- *`On-Premises`* 是指定标签键 (*`Environment`*) 的新标签值。

要从标签密钥中移除标签值，请不要在 `value` 参数中为该密钥的 `tags` 参数指定值。例如：

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

如果操作成功，Security Lake 将返回一个空的 HTTP 200 响应。否则，Security Lake 将返回 HTTP 4xx 或 500 响应，并说明操作失败的原因。

从 Amazon Security Lake 资源中删除标签

要从 Amazon Security Lake 资源中删除标签，您可以使用 Security Lake 控制台或 Security Lake API。

> **Important**
>
> 从资源中删除标签可能会影响对该资源的访问。在移除标签之前，请查看可能使用该标签控制资源访问权限的任何 AWS Identity and Access Management (IAM) 策略。

Console

按照以下步骤，使用 Security Lake 控制台从资源中删除一个或多个标签。

从资源中删除标签

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 根据要从中删除标签的资源类型，执行以下任一操作：
   - 对于数据湖配置，在导航窗格中选择区域。然后，在区域表中，选择区域。
   - 对于订阅用户，在导航窗格中选择订阅用户。然后，在我的订阅用户表中，选择订阅用户。

如果该订阅用户不在表中，请使用页面右上角的 AWS 区域 选择器，选择在其中创建了该订阅用户的区域。该表仅列出当前区域的现有订阅用户。

3. 选择编辑。
4. 展开标签部分。标签部分列出当前分配给该资源的所有标签。
5. 执行以下任一操作：
   - 如果仅删除标签的标签值，请在包含要删除的值的 值框中选择 X。
   - 要同时删除标签的标签键和标签值（以键值对的形式），请选择要删除的标签旁边的删除。
6. 要从资源中删除其他标签，请针对要删除的每个其他标签重复上述步骤。
7. 完成对标签的删除后，选择保存。

API

要以编程方式从资源中移除一个或多个标签，请使用 Security Lake API 的UntagResource操作。在请求中，使用 `resourceArn` 参数指定要从中删除标签的资源的 Amazon 资源名称（ARN）。使用 `tagKeys` 参数指定要删除的标签的标签键。要移除多个标签，请为要移除的每个标签附加 `tagKeys` 参数，并用和号 (&) 分隔，例如，`tagKeys=key1&tagKeys=key2`。如果仅从资源中删除特定的标签值（而不是标签键），请编辑标签而不是删除标签。

如果您使用的是 AWS Command Line Interface (AWS CLI)，请运行 untag-resource 命令从资源中移除一个或多个标签。在 `resource-arn` 参数中，指定要从中移除标签的资源的 ARN。使用 `tag-keys` 形式参数指定要删除的标签的标签键。例如，以下命令从指定订阅用户中删除 `Environment` 标签（包括标签键和标签值）：

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

其中，`resource-arn` 指定要从中删除标签的订阅用户的 ARN，*`Environment`* 是要删除的标签的标签键。

要从资源中删除多个标签，请添加每个其他标签键作为 `tag-keys` 形式参数的实际参数。例如：

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
```

```
--tag-keys Environment Owner
```

如果操作成功，Security Lake 将返回一个空的 HTTP 200 响应。否则，Security Lake 将返回 HTTP 4xx 或 500 响应，并说明操作失败的原因。

Amazon Security Lake 故障排除

如果在使用 Security Lake 时遇到问题，请参考以下主题。

对数据湖状态进行故障排除

S ec urity Lake 控制台的 “问题” 页面显示了影响您的数据湖的问题摘要。例如，如果您尚未为组织创建跟 CloudTrail 踪，Security Lake 将无法为 AWS CloudTrail 管理事件启用日志收集。问题页面涵盖了过去 14 天内发生的问题。您可以看到每个问题的描述和建议的补救步骤。

要以编程方式访问问题摘要，你可以使用 Security Lake API 的ListDataLakeExceptions操作。如果您使用的是 AWS CLI，请运行list-data-lake-exceptions命令。对于`regions`参数，您可以指定一个或多个区域代码（`us-east-1`例如，美国东部（弗吉尼亚北部）地区，以查看影响这些区域的问题。如果您不包含`regions`参数，则会返回影响所有区域的问题。有关区域代码的列表，请参阅 AWS 一般参考 中的 Amazon Security Lake 端点。

例如，以下 AWS CLI 命令列出了影响`us-east-1`和`eu-west-3`区域的问题。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securitylake list-data-lake-exceptions \
--regions "us-east-1" "eu-west-3"
```

要将问题或错误通知安全湖用户，请使用 Security Lake API 的CreateDataLakeExceptionSubscription操作。可以通过电子邮件、发送到亚马逊简单队列服务 (Amazon SQS) 队列、向函数传送或其他支持的协议来 AWS Lambda 通知用户。

例如，以下 AWS CLI 命令通过短信发送向指定账户发送有关 Security Lake 异常的通知。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securitylake create-data-lake-exception-subscription \
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

要查看有关异常订阅的详细信息，您可以使用GetDataLakeExceptionSubscription操作。要更新异常订阅，您可以使用UpdateDataLakeExceptionSubscription操作。要删除异常订阅并停止通知，您可以使用该DeleteDataLakeExceptionSubscription操作。

Lake Formation 故障排除

使用以下信息来帮助您诊断和修复在使用 Security Lake 和 AWS Lake Formation 数据库或表时可能遇到的常见问题。有关更多 Lake Formation 故障排除主题，请参阅 AWS Lake Formation 开发人员指南的故障排除部分。

未找到表

尝试创建订阅用户时可能会遇到此错误。

要纠正此错误，请确保您已在区域中添加来源。如果您在 Security Lake 服务处于预览版时添加了来源，则必须在创建订阅用户之前重新添加这些来源。有关添加来源的更多信息，请参阅 Amazon Security Lake 中的来源管理。

400 AccessDenied

添加自定义来源并调用 `CreateCustomLogSource` API 时可能会遇到此错误。

要纠正此错误，请查看您的 Lake Formation 权限。调用 API 的 IAM 角色应具有 Security Lake 数据库的创建表权限。有关更多信息，请参阅 AWS Lake Formation 开发人员指南中的使用 Lake Formation 控制台和指定的资源方法授予数据库权限。

SYNTAX_ERROR: line 1:8: SELECT * 不允许用于没有列的关系

首次在 Lake Formation 中查询来源表时，您可能会遇到此错误。

要纠正错误，请向登录时使用的 IAM 角色授予SELECT权限 AWS 账户。有关授予 SELECT 权限的说明，请参阅 AWS Lake Formation 开发人员指南中的使用 Lake Formation 控制台和指定的资源方法授予表权限。

Security Lake 未能将调用者的主体 ARN 添加到 Lake Formation 数据湖管理员。当前的数据湖管理员可能包含已不存在的无效主体。

在启用 Security Lake 或添加 AWS 服务 为日志源时，您可能会收到此错误。

要纠正此错误，请按照以下步骤操作：

1. 打开 Lake Formation 控制台：https://console.aws.amazon.com/lakeformation/。
2. 以管理用户的身份登录。
3. 在导航窗格的权限下，选择管理角色和任务。

4. 在数据湖管理员部分，选择选择管理员。
5. 清除被标记为在 IAM 中未找到的主体，然后选择保存。
6. 重试 Security Lake 操作。

Security L CreateSubscriber ake with Lake Formation 没有创建新的 RAM 资源共享邀请供接受

如果您在 Security Lake 中创建 Lake Formation 订阅用户之前，、使用 Lake Formation 版本 2 或版本 3 跨账户数据共享来共享资源，则可能会看到此错误。这是因为 Lake Formation 版本 2 和版本 3 跨账户共享通过将多个跨账户权限授予映射到一个 AWS RAM 资源共享来优化 AWS RAM 资源共享的数量。

请务必检查资源共享名称是否具有您在创建订阅用户时指定的外部 ID，以及资源共享 ARN 是否与 `CreateSubscriber` 响应中的 ARN 相匹配。

对亚马逊 Athena 中的查询进行疑难解答

使用以下信息可帮助您诊断和修复您在使用 Athena 查询存储在 Security Lake S3 存储桶中的对象时可能遇到的常见问题。有关更多 Athena 故障排除主题，请参阅 Amazon Athena 用户指南的在 Athena 中进行故障排除部分。

查询未返回数据湖中的新对象

即使 Security Lake 的 S3 存储桶中包含新对象，您的 Athena 查询也可能不会返回数据湖中的这些对象。如果您禁用了 Security Lake 然后又将其启用，则可能会发生这种情况。因此， AWS Glue 分区可能无法正确注册新对象。

要纠正此错误，请按照以下步骤操作：

1. 打开 AWS Lambda 控制台，网址为 https://console.aws.amazon.com/lambda/。
2. 在导航栏的“区域”选择器上，选择已启用 Security Lake 但 Athena 查询未返回结果的区域。
3. *######## “##”##### **SecurityLake_Glue_Partition_Updater_L** ambda_ “region>” region> ###*
4. 在配置选项卡中，选择触发器。
5. 选择函数旁边的选项，然后选择编辑。
6. 选择激活触发器，然后选择保存。函数状态会变为已启用。

无法访问 AWS Glue 表

查询访问订阅者可能无法访问包含 Security Lake 数据的 AWS Glue 表。

首先，请确保您已执行设置跨账户表共享（订阅用户步骤）中的步骤。

如果订阅用户仍然无法访问，请按照以下步骤操作：

1. 打开 AWS Glue 控制台，网址为 https://console.aws.amazon.com/glue/。
2. 在导航窗格中选择数据目录，然后选择目录设置。
3. 使用基于资源的策略向订阅者授予访问 AWS Glue 表的权限。有关创建基于资源的策略的更多信息，请参阅 AWS Glue 开发人员指南中的适用于 AWS Glue 的基于资源的策略示例。

Orgations 故障排除

使用以下信息可帮助您诊断和修复您在使用 Security Lake 和 AWS Organizations 时可能遇到的常见问题。有关更多 Organizations 故障排除主题，请参阅 AWS Organizations 用户指南的故障排除部分。

调用 CreateDataLake 操作时出现拒绝访问错误：您的账户必须是组织的委托管理员账户或独立账户。

如果您删除委托管理员账户所属的组织，然后尝试使用该账户通过 Security Lake 控制台或 CreateDataLakeAPI 来设置 Security Lake，则可能会收到此错误。

要纠正此错误，请使用来自其他组织的委托管理员账户或独立账户。

Amazon Security Lake 身份和访问故障排除

使用以下信息可帮助您诊断和修复您在使用 Security Lake 和 IAM 时可能遇到的常见问题。

我无权在 Security Lake 中执行某项操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供凭证的人员。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`subscriber`* 资源的详细信息，但不拥有虚构 `SecurityLake:`*`GetSubscriber`* 权限时，就会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 SecurityLake:*GetSubscriber* 操作访问 *subscriber* 信息。

我无权执行 iam：PassRole

如果您遇到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Security Lake。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Security Lake 中执行操作时，就会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我 AWS 账户 的 Security Lake 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Security Lake 是否支持这些功能，请参阅Amazon Security Lake 如何与 IAM 一起使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户

- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

如何确定 Security Lake 的定价

Amazon Security Lake 的定价基于两个方面：数据摄取和数据转换。Security Lake 还可以与其他 AWS 服务相结合来存储和共享您的数据，这些活动可能产生单独的费用。

当您在 Security Lake 支持的任何 AWS 区域中的 AWS 账户中首次启用日志收集时，该账户将自动注册 Security Lake 的 15 天免费试用。在免费试用期间，您仍可能因其他服务而产生费用。

数据摄取

这些费用取决于摄取的 AWS CloudTrail 日志以及其他 AWS 服务日志和事件（Amazon Route 53 Resolver 查询日志、AWS Security Hub 调查发现和 Amazon VPC 流日志）的数量。

数据转换

这些费用取决于 Security Lake 标准化为开放式网络安全架构框架 (OCSF) 架构并转换为 Apache Parquet 格式的 AWS 服务日志和事件的数量。

相关服务的费用

以下是其他 AWS 服务在安全数据湖中存储和共享数据时可能产生的一些费用：

- Amazon S3 – 这些费用来自在您的 Security Lake 账户中维护 Amazon S3 桶、在桶中存储数据以及为了进行安全和访问控制而评估和监控桶。有关更多信息，请参阅 Amazon S3 定价。
- Amazon SQS – 这些费用来自创建用于消息传输的 Amazon SQS 队列。有关更多信息，请参阅 Amazon SQS 定价。
- Amazon EventBridge – 这些费用来自 Amazon EventBridge 向订阅端点发送对象通知。有关更多信息，请参阅 Amazon EventBridge 定价。

订阅用户因查询 Security Lake 中的数据和存储查询结果而产生的费用由订阅用户承担。

有关更多信息，请参阅 Security Lake 定价。

查看 Security Lake 使用量和估算费用

通过 Amazon Security Lake 控制台的使用量页面，您可以查看当前的 Security Lake 使用量，以及将来的使用量和费用估算。如果您目前正在参与为期 15 天的免费试用，那么根据试用期内的使用量，您可以估算出在免费试用结束后使用 Security Lake 的费用。有关 Security Lake 定价的概述，请参阅如何确定 Security Lake 的定价。有关详细信息和费用示例，请参阅 Amazon Security Lake 定价。

在 Security Lake 中，估算的使用费用以美元报告，并且仅适用于当前的 AWS 区域。这些费用涵盖了组织中所有账户对 Security Lake 的使用，包括转换为开放网络安全架构框架（OCSF）和 Apache Parquet 格式。但是，预测的费用不包括与 Security Lake 配合使用的其他服务的费用，例如 Amazon Simple Storage Service（Amazon S3）和 AWS Glue。

在使用量页面上，您可以选择要查看使用量和费用数据的时间段。默认时间段为最近 1 个日历日。您必须有至少 1 天的 Security Lake 使用量才能查看费用预测。

页面顶部显示了所有账户的预计费用。这是根据您在选定时间范围内的实际使用量，为当前 AWS 区域预测的未来 30 个日历日的 Security Lake 费用。实际使用量和预计费用反映的是组织内的所有账户。

在页面的其余部分，使用量和费用数据被分为两个表，如下所示：

- 按来源划分的使用量和成本 - 这是按数据来源划分的您当前的 Security Lake 使用量，以及根据您在选定时间范围内的实际使用量估算的未来 30 个日历日的使用量和费用。实际使用量、预计使用量和预计费用反映了组织内的所有账户。如果您选择一个来源，系统将打开一个拆分面板，其中显示了哪些账户从该来源生成了日志和事件。对于每个账户，拆分面板既包含来自该来源的实际使用量，也包含预计使用量和费用。
- 按账户划分的使用情况和成本 – 这是按账户划分的您当前的 Security Lake 使用量，以及根据您在选定时间范围内的实际使用量估算的未来 30 个日历日的使用量和费用。如果您选择一个账户，系统将打开一个拆分面板，其中显示了该账户的使用量的来源。对于每个使用量来源，拆分面板既包含实际使用量，也包含预计使用量和费用。

所有受支持的 AWS 数据源都显示在上述表中，即使您尚未在 Security Lake 中添加特定源也是如此。如果您正在参与免费试用，我们建议您添加所有 AWS 源，以获取全套日志和事件的费用估算。有关添加 AWS 源的说明，请参阅从中收集数据 AWS 服务。自定义源不包含在使用量或成本计算中。

按照以下步骤在 Security Lake 控制台中查看使用量和费用数据。

查看 Security Lake 使用量和预计费用（控制台）

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 使用页面右上角的 AWS 区域选择器选择要查看使用量和费用的区域。
3. 在导航窗格中，选择设置，然后选择使用量。
4. 选择要查看使用量和费用数据的时间段。默认值为最近 1 天。
5. 选择按数据来源划分或按账户划分选项卡以详细查看使用量和费用。

Amazon Security Lake 区域和端点

有关 Security Lake 支持的区域和服务端点列表，请参阅《AWS 一般参考》中的 Amazon Security Lake 端点。

我们建议您在所有受支持的 AWS 区域启用 Security Lake。这让您可以使用 Security Lake 来检测和调查未授权或异常活动，甚至在您未主动使用的区域中也可以。

禁用 Amazon Security Lake

当您禁用 Amazon Security Lake 时，Security Lake 会停止从您的 AWS 源收集日志和事件。现有的 Security Lake 设置以及在 AWS 账户 中创建的资源将得到保留。此外，您存储在他人中或发布给其他人的数据 AWS 服务，例如 AWS Lake Formation 表和 AWS CloudTrail 日志中的敏感数据，仍然可用。存储在 Amazon Simple Storage Service（Amazon S3）桶中的数据在您的 Amazon S3 存储生命周期内可用。

从 Security Lake 控制台的 “设置” 页面禁用 Security Lake 会停止收集所有 AWS 区域 当前已启用 Security Lake 的 AWS 日志和事件。您可以使用控制台上的区域页面来停止在特定区域收集日志。Security Lake API AWS CLI 以及您在请求中指定的区域中停止日志收集。

如果您使用与的集成， AWS Organizations 并且您的账户属于集中管理多个 Security Lake 账户的组织，则只有委派的 Security Lake 管理员才能为自己和成员账户禁用 Security Lake。但是，退出组织会停止收集成员账户的日志。

当您为组织禁用 Security Lake 时，如果按照本页面上提供的禁用说明进行操作，则会保留指定的委派管理员。您无需再次指定委派管理员即可重新启用 Security Lake。

对于自定义来源，在停用 Security Lake 时，必须在 Security Lake 控制台之外禁用每个来源。未能禁用集成将导致源集成继续向 Amazon S3 发送日志。此外，您必须禁用订阅用户集成，否则订阅用户仍将能够使用来自 Security Lake 的数据。有关如何删除自定义来源或订阅用户集成的详细信息，请参阅相应提供商的文档。

本主题介绍如何使用安全湖控制台、Security Lake API 或禁用安全湖 AWS CLI。

Console

1. 打开 Security Lake 控制台：https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中的设置下，选择常规。
3. 选择禁用 Security Lake。
4. 系统提示进行确认时，输入 **`Disable`**，然后选择禁用。

API

要以编程方式禁用安全湖，请使用安全湖 API 的DeleteDataLake操作。如果您使用的是 AWS CLI，请运行该delete-date-lake命令。在您的请求中，使用`regions`列表为要禁用 Security Lake

的每个区域指定区域代码。有关区域代码的列表，请参阅 AWS 一般参考 中的 Amazon Security Lake 端点。

对于使用的 Security Lake 部署 AWS Organizations，只有为组织委派的 Security Lake 管理员才能为组织中的账户禁用 Security Lake。

例如，以下 AWS CLI 命令禁用`ap-northeast-1`和`eu-central-1`区域中的安全湖。此示例是针对 Linux、macOS 或 Unix 进行格式化的，它使用反斜杠 (\) 行继续符来提高可读性。

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

《Amazon Security Lake 用户指南》的文档历史记录

下表列出了自 Amazon Security Lake 上次发布以来对文档所做的重要更改。如需获得此文档的更新通知，您可以订阅 RSS 源。

最新文档更新：2024 年 3 月 27 日

变更	说明	日期
更新现有托管策略	Security Lake 更新了AmazonSecurityLakeMetastoreManager政策，添加了元数据清理操作，允许您删除数据湖中的元数据。	2024 年 3 月 27 日
新的源版本	更新您的角色权限以从新数据源版本提取数据。	2024 年 2 月 29 日
新的 AWS 日志源	Security La ke 将 EKS 审核 AWS 日志添加为日志源。EKS 审核日志可帮助您在 Amazon Elastic Kubernetes Service 中检测您的 EKS 集群中可能存在的可疑活动。	2024 年 2 月 29 日
更新现有托管策略	Security Lake 更新了政策，允许使用`iam:PassRole` 新`AmazonSecurityLakeMetastoreManagerV2` 角色，并允许 Security Lake 部署或更新数据湖组件。	2024 年 2 月 23 日
新的托管策略	Security Lake 添加了一个新的AWS 托管策略，即`AmazonSecurityLakeMetastoreManager` 策	2024 年 1 月 23 日

	略。此策略授予 Security Lake 管理数据湖中元数据的权限。	
区域可用性	Security Lake 现已在以下地区推出 AWS 区域：亚太地区（大阪）、加拿大（中部）、欧洲（巴黎）和欧洲（斯德哥尔摩）。有关当前提供 Security Lake 的区域的完整列表，请参阅《AWS 一般参考》中的 Amazon Security Lake 端点。	2023 年 10 月 26 日
新功能	现在，您可以为具有查询权限的订阅用户编辑某些设置。您还可以为您的 AWS 账户的 Security Lake 资源分配标签。	2023 年 7 月 20 日
新的托管策略	Security Lake 添加了一个新的AWS 托管策略，即AmazonSecurityLakeAdministrator 策略。此策略授予管理权限，允许主体拥有对所有 Security Lake 操作的完全访问权限。	2023 年 5 月 30 日
正式发布	Security Lake 现已正式发布。	2023 年 5 月 30 日
新特征	Security Lake 现在向亚马逊发送指标 CloudWatch。	2023 年 5 月 4 日
区域可用性	Security Lake 现已在以下地区推出 AWS 区域：亚太地区（新加坡）、欧洲（伦敦）和南美洲（圣保罗）。	2023 年 3 月 22 日

新特征	现在，当您使用 Security Lake 控制台启用和开始使用 Security Lake 时，Security Lake 会代表您创建 AWS Identity and Access Management (IAM) 角色。	2023 年 2 月 15 日
初始版本	这是《Amazon Security Lake 用户指南》的初始版本。	2022 年 11 月 29 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。