aws

用户指南

Amazon Security Lake

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Security Lake: 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 Amazon Security Lake？

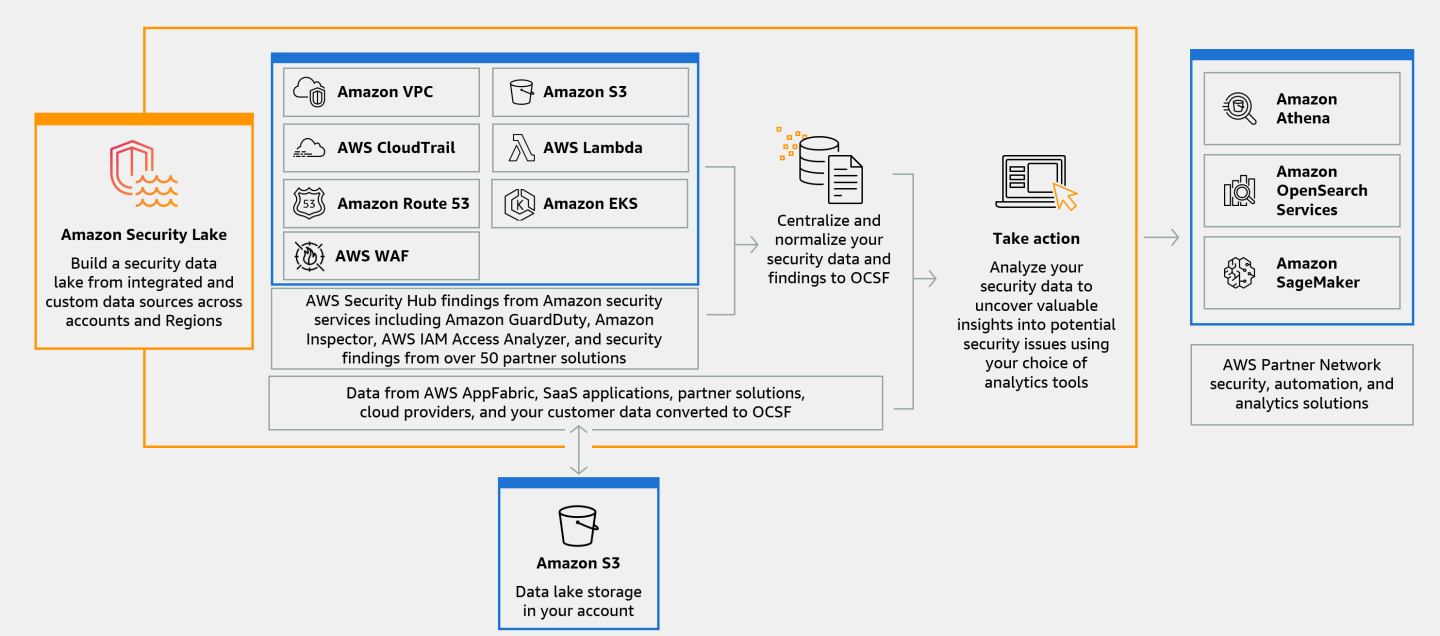
Amazon Security Lake 是一项完全托管的安全数据湖服务。您可以使用 Security Lake 自动将来自 AWS 环境、SaaS 提供商、本地、云源和第三方来源的安全数据集中到存储在您的专用的数据湖中。AWS 账户 Security Lake 可以帮助您分析安全数据，让您更全面地了解整个组织的安全状况。借助 Security Lake，您还可以改善对工作负载、应用程序和数据的保护。

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 可以标准化 AWS 并合并来自各种企业安全数据源的安全数据。

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 从多个来源（包括本地和第三方服务）收集安全日志和事件。 AWS 服务收集日志后，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 安全湖中的源代码管理

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。它还将数据从原生支持 AWS 服务 转换为开放网络安全架构框架 (OCSF) 开源架构。这使得数据与其他 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 安全湖区域和终端节点。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 管理控制台

AWS 管理控制台 是一个基于浏览器的界面，可用于创建和管理 AWS 资源。可通过 Security Lake 控制台访问您的 Security Lake 账户和资源。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，直接向该服务发出 HTTPS 请求。有关更多信息，请参阅 Security Lake API 参考。

AWS Command Line Interface (AWS CLI)

借助 AWS CLI，您可以在系统的命令行中发出命令来执行 Security Lake 任务和 AWS 任务。与控制台相比，使用命令行更快、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。有关安装和使用的信息 AWS CLI，请参阅AWS Command Line Interface。

AWS SDKs

AWS 由各种编程语言和平台（例如 Java、Go、Python、C++ 和.NET）的库和示例代码组成。SDKs 它们 SDKs 提供了对 Security Lake 和其他内容的便捷编程访问 AWS 服务。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。有关安装和使用的信息 AWS SDKs，请参阅构建工具 AWS。

相关服务

以下是 Security Lake AWS 服务 使用的其他内容：

- Amazon EventBridge — Secur EventBridge ity Lake 用于在对象写入数据湖时通知订阅者。
- AWS Glue— Security Lake 使用 AWS Glue 爬虫来创建 AWS Glue Data Catalog 表并将新写入的数据发送到数据目录。Security Lake 还会在数据目录中存储 AWS Lake Formation 表的分区元数据。
- 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 会使用 Lambda 函数来支持对原始数据进行的提取、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。
- Amazon Simple Queue 服务 — Security Lake 使用 Amazon SQS 来实现事件驱动的处理和管理通知。

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

- 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 CSPM 调查结果
- Amazon Virtual Private Cloud (Amazon VPC) 流日志
- AWS WAF v2 日志

有关这些来源的更多信息，请参阅 从 Security Lake AWS 服务 中收集数据。您可以通过创建能够读取 OCSF 架构中数据的订阅用户来使用安全数据湖中的 Amazon S3 对象。您还可以使用与之集成的亚马逊 Athena、Amazon Redshift 和第三方订阅服务来查询数据。 AWS Glue

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 AWS 区域 向汇总区域提供数据的公司。

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 用于 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。它由多个 AWS 安全领域的其他安全行业领导者开发。Security Lake 会自动将其收集的日志和事件转换为 OCSF 架构。 AWS 服务 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

整 AWS 区域 合来自一个或多个贡献地区的安全日志和事件。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。订阅者可能是其他服务 AWS 服务 或第三方服务。

Amazon Security Lake 入门

本节中的主题说明了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 管理控制台 或以编程方式启用和使用 Security Lake。无论使用哪种方法，都必须先设置一个 AWS 账户 和一个管理员用户。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。

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**
>
> Security Lake 不支持回填在启用 Security Lake 之前生成的现有 AWS 原始日志源事件。

主题

设置你的 AWS 账户

在启用 Amazon Security Lake 之前，您必须有一个 AWS 账户。如果您没有 AWS 账户，请完成以下步骤来创建一个。

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。

报名参加 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，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。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来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。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

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 管理控制台在下一页上，输入您的密码。

   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 Signing in as the root user。
2. 为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）。

创建具有管理访问权限的用户

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。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

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。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

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，请参阅在 Security Lake AWS Organizations中管理多个账户。

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。
- 当您在任何区域首次启用 Security Lake 时，它会为您的账户创建以下服务相关角色：
  - AWSServiceRoleForSecurityLake：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。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。

- AWSServiceRoleForSecurityLakeResourceManagement: Security Lake 使用此角色进行持续监控和性能改进，这有可能减少延迟和成本。该服务相关角色信任 `resource-management.securitylake.amazonaws.com` 服务担任该角色。启用此服务角色还将授予其访问 Lake Formation 的权限。

  有关这对在 2025 年 4 月 17 日之前启用 Security Lake 的现有账户有何影响的信息，请参阅Update for existing accounts。

有关服务相关角色的工作原理的信息，请参阅 IAM 用户指南中的使用服务相关角色权限。

- 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。
- 如果您要在某个地区重新启用 Security Lake，则必须从之前使用的 Security Lake 中删除该区域的相应 AWS Glue 数据库。

使用控制台启用安全湖

本教程介绍如何通过启用和配置 Security Lake AWS 管理控制台。作为其中的一部分 AWS 管理控制台，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 Security Lake 中的自定义来源收集数据。

配置日志源收集

1. 在上打开 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. 在 “选择日志和事件源” 中，选择以下选项之一进行来源选择：

   a. 载@@ 入默认 AWS 来源-选择推荐选项时， CloudTrail -S3 数据事件，默认情况下 AWS WAF 不包含在摄取中。这是因为大量摄取两种来源类型可能会显著影响使用成本。要摄取这些源，请先选择 “收录特定 AWS 来源” 选项，然后从 “日志和事件源” 列表中选择这些源。

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。有关版本的更多信息，请参阅OCSF来源识别。

> **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. 对于选择账户，请执行以下步骤：

   1. 选择 Security Lake 是从组织中的所有账户还是特定账户中提取数据。将使用您在配置期间选择的设置为这些账户启用 Security Lake。
   2. 默认情况下，“为新的组织帐户自动启用 Security Lak e” 复选框处于选中状态。 AWS 账户 当他们加入您的组织时，这些自动启用设置将适用。您可以随时编辑自动启用设置。

   > **Note**
   >
   > 自动启用设置仅适用于加入组织后的账户，不适用于现有账户。有关更多信息，请参阅在控制台中编辑新账户配置。

8. 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。
9. 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：查看和查询您自己的数据

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。

第 5 步：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 安全湖中的订阅者管理。

以编程方式启用安全湖

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AWS SDKs来访问 Security Lake。AWS

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，请运行该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 Security Lake 中的自定义来源收集数据。

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，以下命令创建一个以汇总区域ap-northeast-2为数据湖。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：查看和查询您自己的数据

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 安全湖中的订阅者管理。

在 Security Lake AWS Organizations中管理多个账户

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。

> **Important**
>
> 使用 Security Lake 的 RegisterDataLakeDelegatedAdministratorAPI 允许 Security Lake 访问您的组织并注册组织的委托管理员。
> 如果您使用 Organi APIs zations 注册委托管理员，则可能无法成功创建组织的服务相关角色。为确保全部功能，请使用安全湖 APIs。

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。

> **对于现有的安全湖账户**
>
> 如果您在 2025 年 4 月 17 日之前启用了 Security Lake，我们建议您启用用于资源管理的服务关联角色 (SLR) 权限。通过使用此单反相机，您可以继续进行持续的监控和性能改进，从而有可能减少延迟和成本。有关与此 SLR 关联的权限的信息，请参阅用于资源管理的服务关联角色 (SLR) 权限。

如果您使用 Security Lake 控制台，则会收到一条通知，提示您启用。AWSServiceRoleForSecurityLakeResourceManagement如果您使用AWS CLI，请参阅创建 Security Lake 服务相关角色。

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 安全湖中的订阅者管理。

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. 在上打开 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，输入您的日志存档账户的 12 位数字AWS 账户 ID。

   我们建议以委托的 Security Lake 管理员身份使用日志存档。有关更多信息，请参阅 委托的 Security Lake 管理员的重要注意事项。
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 CSPM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 Security Lake AWS 服务 中收集数据。

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。

编辑新组织帐户的自动启用配置

授权的 Security Lake 管理员可以在账户加入您的组织时查看和编辑其自动启用设置。Security Lake 仅根据这些设置提取新账户的数据，而非现有账户。

使用以下步骤编辑新组织帐户的配置：

1. 在上打开 Security Lake 控制台https://console.aws.amazon.com/securitylake/。
2. 在导航窗格中，选择账户。
3. 在账户页面上，展开新账户配置部分。您可以查看 Security Lake 从每个区域摄取了哪些来源。
4. 选择 “编辑” 以编辑此配置。
5. 在编辑新账户配置页面上，执行以下步骤：

    a. 在 “选择区域” 中，选择一个或多个要更新其源以从中提取数据的区域。然后选择下一步。

    b. 在 “选择来源” 中，选择以下选项之一进行来源选择：

        i. 载@@ 入默认AWS来源-选择推荐选项时， CloudTrail -S3 数据事件，默认情况下AWS WAF不包含在摄取中。这是因为大量摄取两种来源类型可能会显著影响使用成本。要摄取这些源，请先选择 “收录特定AWS来源” 选项，然后从 “日志和事件源” 列表中选择这些源。

        ii. 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。

        iii. 不要收录任何来源 — 如果您不想从上一步中选择的区域中提取任何来源，请选择此选项。

        iv. 选择下一步。

> **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。

c. 查看更改后，选择应用。

AWS 账户加入您的组织后，默认情况下，这些设置将应用于该账户。

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 CSPM 调查结果。在授权的管理员调用此操作后，新成员账户不会将 Security Hub CSPM 发现结果贡献到数据湖。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。

在安全湖中管理区域

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. 在上打开 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，将一个或多个指定 AWS 账户 IDs 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. 在上打开 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，请参阅为安全湖资源添加标签。
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"}]}}]'
```

在 Security Lake 中配置汇总区域

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。

由于 Amazon S3 的限制，不支持从客户托管密钥 (CMK) 加密的区域数据湖复制到 S3 托管加密（默认加密）区域数据湖。

> **Important**
>
> 如果您创建了自定义源，为了确保将自定义源数据正确复制到目标，Security Lake 建议遵循采集自定义源的最佳实践中描述的最佳实践。无法对不遵循页面上描述的 S3 分区数据路径格式的数据执行复制。

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。

JSON

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

```
        }
      }
    },
    {
      "Sid": "AllowS3Replication",
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[destinationRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    }
  ]
}
```

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：

JSON

```
{
    "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，网址为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. 在上打开 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. 在上打开 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"}]}}]'
```

安全湖中的源代码管理

来源是单个系统中生成的与 安全湖中的开放网络安全架构框架 (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，包括本地支持的来源 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。处理后，Security Lake 将源数据存储在生成数据的亚马逊简单存储服务 (Amazon S3) 存储桶中 AWS 账户 AWS 区域 。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。每个源在您的 S3 存储桶中都有单独的前缀，Security Lake 将来自每个源的数据整理到一组单独的 AWS Lake Formation 表中。

主题

从 Security Lake AWS 服务 中收集数据

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 CSPM 调查结果
- Amazon Virtual Private Cloud (Amazon VPC) 流日志
- AWS WAF v2 日志

Security Lake 会自动将这些数据转换为安全湖中的开放网络安全架构框架 (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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUpdatingSecurityLakeS3Buckets",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::aws-security-data-lake*",
              "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
```

```
            }
    }
    ]
}
```

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`

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 Security Lake 中的自定义来源收集数据。

Console

添加 AWS 日志源（控制台）

1. 在上打开 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="2.0"
```

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. 在上打开 Security Lake 控制台https://console.aws.amazon.com/securitylake/。
2. 在导航窗格上，选择账户。

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指定 AWS 账户 IDs 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"
```

在安全湖中更新角色权限

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. 在上打开 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，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。

如果您决定删除该角色，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 管理控制台 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从每个区域中删除。

从 Secur AWS 服务 ity Lake 中移除作为来源

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移除用作来源的原生支持的 AWS 服务 。有关移除自定义来源的更多信息，请参阅从 Security Lake 中的自定义来源收集数据。

Console

1. 在上打开 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，您可以将删除范围限制为特定`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="2.0"
```

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="2.0"
```

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。

CloudTrail 安全湖中的事件日志

AWS CloudTrail 为您提供账户的 AWS API 调用历史记录，包括使用、 AWS 管理控制台、命令行工具和某些 AWS 服务进行的 API 调用。 AWS SDKs CloudTrail 还允许您识别哪些用户和帐户呼叫 AWS APIs 了支持的服务 CloudTrail、发出呼叫的源 IP 地址以及呼叫发生的时间。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)

安全湖中的 Amazon 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。此过程旨在无需额外设置，也不影响您可能拥有的现有 Amazon EKS 控制平面日志配置。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。

只有 OCSF v1.1.0 支持 Amazon EKS 审核日志。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 存储库中针对 Amazon EKS 审核日志事件 (v1.1.0) 的映射参考。

安全湖中的 Route 53 解析器查询日志

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 CSPM 在安全湖中发现的结果

Security Hub CSPM 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 CSPM 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 CSPM 控制进行检查。Security Hub CSPM 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。

当你将 Security Hub CSPM 发现作为来源添加到 Security Lake 中时，Security Lake 会立即开始通过独立且重复的事件流直接从 Security Hub CSPM 收集你的发现。Security Lake 还会将调查发现从 ASFF 转换为安全湖中的开放网络安全架构框架 (OCSF) (OCSF)。

Security Lake 不会管理你的 Security Hub CSPM 发现，也不会影响你的 Security Hub CSPM 设置。要管理 Security Hub CSPM 调查结果，必须使用 Security Hub CSPM 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 CSPM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 CSPM 调查结果标准化为 OCSF。

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

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

安全湖中的 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使用来自 Amazon VPC 的 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)

AWS WAF 登录安全湖

当你在 Security Lake 中添加 AWS WAF 为日志源时，Security Lake 会立即开始收集日志。 AWS WAF 是一种 Web 应用程序防火墙，可用于监控最终用户向您的应用程序发送的 Web 请求并控制对您的内容的访问。记录的信息包括从您的 AWS 资源 AWS WAF 收到网络请求的时间、有关该请求的详细信息以及请求匹配的规则的详细信息。

Security Lake AWS WAF 通过独立且重复的 AWS WAF 日志流直接使用日志。此过程旨在无需额外设置或影响现有 AWS WAF 配置。Security Lake 日志仅检索 AWS WAF Web 访问控制列表 (Web ACL) 配置允许的数据。如果在 Security Lake 账户中为 Web ACL 启用了数据保护，则将根据您的 Web ACL 设置对生成的数据进行编辑或哈希处理。有关使用 AWS WAF 保护应用程序资源的信息，请参阅《AWS WAF 开发人员指南》中的 AWS WAF 工作原理。

> **Important**
>
> 如果您使用 Amazon CloudFront 分发作为中的资源类型 AWS WAF，则必须选择美国东部（弗吉尼亚北部）才能在 Security Lake 中提取全球日志。

AWS WAF 只有 OCSF v1.1.0 支持日志。有关 Security Lake 如何将 AWS WAF 日志事件标准化为 OCSF 的信息，请参阅 OCSF AWS WAF 日志存储库 (v1. GitHub 1.0) 中的映射参考。

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移除用作来源的原生支持的 AWS 服务 。有关移除自定义来源的更多信息，请参阅从 Security Lake 中的自定义来源收集数据。

Console

1. 在上打开 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，您可以将删除范围限制为特定`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="2.0"
```

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="2.0"
```

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。

从 Security Lake 中的自定义来源收集数据

Amazon Security Lake 可以从自定义的第三方源收集安全日志和事件。Security Lake 自定义源是一种第三方服务，用于向 Amazon Security Lake 发送安全日志和事件。在发送数据之前，自定义源必须将日志和事件转换为开放网络安全架构框架 (OCSF)，并满足 Security Lake 的源要求，包括分区、parquet 文件格式以及对象大小和速率要求。

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。

> **Note**
>
> 一个账户中最多可以添加 50 个自定义日志源。

要向 Security Lake 添加自定义源，它必须满足以下要求。不满足这些要求可能会影响性能，并可能影响查询等分析用例。

- 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。
- 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。
- 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。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。
- 分区-必须按区域、 AWS 账户、EventDay 对对象进行分区。对象前缀应为。*source location*/region=*region*/accountId=*accountID*/eventDay=*yyyyMMdd*/
- 对象大小和速率 — 发送到 Security Lake 的文件应在 5 分钟到 1 个活动日之间按增量发送。如果文件大小超过 256MB，则客户发送文件的频率可能超过 5 分钟。对象和大小要求是针对查询性能优化 Security Lake。不遵守自定义源代码要求可能会影响您的 Security Lake 性能。
- 排序-在每个 Parquet 格式的对象中，应按时间对记录进行排序，以降低查询数据的成本。

> **Note**
>
> 使用 OCSF 验证工具验证自定义源是否与兼容。OCSF Schema对于自定义来源，Security Lake 支持 OCSF 1.3 及更早版本。

在 Security Lake 中提取自定义源的分区要求

为了便于高效的数据处理和查询，在向 Security Lake 添加自定义源时，我们需要满足分区、对象和大小要求：

分区

应按源位置、 AWS 区域 AWS 账户、和日期对对象进行分区。

- 分区数据路径的格式为

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

  带有示例存储桶名称的示例分区是aws-security-data-lake-*us-west-2-lake-uid*/ext/*custom-source-name*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/。

以下列表描述了 S3 路径分区中使用的参数：

- 安全湖存储您的自定义源数据的 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 将数据上传到其中。例如，您必须使用将数据上传US East (N. Virginia)到位于美国东部（弗吉尼亚北部）地区的 Security Lake 存储桶。
- accountId— 源分区中记录所属的 AWS 账户 ID。对于与之外的账户相关的记录 AWS，我们建议使用诸如external或之类的字符串external_externalAccountId。通过采用这种命名对流，您可以避免在命名外部帐户时出现歧义， IDs这样它们就不会与其他身份管理系统 IDs 维护的 AWS 帐户 IDs 或外部帐户发生冲突。
- eventDay— 记录的 UTC 时间戳，截断为小时，格式为八个字符的字符串 ()。YYYYMMDD如果记录在事件时间戳中指定了不同的时区，则必须将该分区键的时间戳转换为 UTC。

在 Security Lake 中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

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:CreateDatabase
- glue:CreateTable
- 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:CreateGrantkms:DescribeKey、和kms:GenerateDataKey的权限。

> **Important**
>
> 如果您计划使用 Security Lake 控制台添加自定义源，则可以跳过下一步继续操作在 Security Lake 中添加自定义来源。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 添加自定义来源，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和 create/update AWS Glue 数据目录中的表。

JSON

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

```
    ]
}
```

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：

JSON

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

```
}
```

在 Security Lake 中添加自定义来源

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. 在上打开 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。

支持的 OCSF 事件类

开放网络安全架构框架 (OCSF) 事件类描述了自定义源将发送到 Security Lake 的数据类型。支持的事件类列表有：

```
public enum OcsfEventClass {
    ACCOUNT_CHANGE,
    API_ACTIVITY,
    APPLICATION_LIFECYCLE,
    AUTHENTICATION,
    AUTHORIZE_SESSION,
    COMPLIANCE_FINDING,
    DATASTORE_ACTIVITY,
    DEVICE_CONFIG_STATE,
```

```
    DEVICE_CONFIG_STATE_CHANGE,
    DEVICE_INVENTORY_INFO,
    DHCP_ACTIVITY,
    DNS_ACTIVITY,
    DETECTION_FINDING,
    EMAIL_ACTIVITY,
    EMAIL_FILE_ACTIVITY,
    EMAIL_URL_ACTIVITY,
    ENTITY_MANAGEMENT,
    FILE_HOSTING_ACTIVITY,
    FILE_SYSTEM_ACTIVITY,
    FTP_ACTIVITY,
    GROUP_MANAGEMENT,
    HTTP_ACTIVITY,
    INCIDENT_FINDING,
    KERNEL_ACTIVITY,
    KERNEL_EXTENSION,
    MEMORY_ACTIVITY,
    MODULE_ACTIVITY,
    NETWORK_ACTIVITY,
    NETWORK_FILE_ACTIVITY,
    NTP_ACTIVITY,
    PATCH_STATE,
    PROCESS_ACTIVITY,
    RDP_ACTIVITY,
    REGISTRY_KEY_ACTIVITY,
    REGISTRY_VALUE_ACTIVITY,
    SCHEDULED_JOB_ACTIVITY,
    SCAN_ACTIVITY,
    SECURITY_FINDING,
    SMB_ACTIVITY,
    SSH_ACTIVITY,
    USER_ACCESS,
    USER_INVENTORY,
    VULNERABILITY_FINDING,
    WEB_RESOURCE_ACCESS_ACTIVITY,
    WEB_RESOURCES_ACTIVITY,
    WINDOWS_RESOURCE_ACTIVITY,
    // 1.3 OCSF event classes
    ADMIN_GROUP_QUERY,
    DATA_SECURITY_FINDING,
    EVENT_LOG_ACTIVITY,
    FILE_QUERY,
    FILE_REMEDIATION_ACTIVITY,
```

```
    FOLDER_QUERY,
    JOB_QUERY,
    KERNEL_OBJECT_QUERY,
    MODULE_QUERY,
    NETWORK_CONNECTION_QUERY,
    NETWORK_REMEDIATION_ACTIVITY,
    NETWORKS_QUERY,
    PERIPHERAL_DEVICE_QUERY,
    PROCESS_QUERY,
    PROCESS_REMEDIATION_ACTIVITY,
    REMEDIATION_ACTIVITY,
    SERVICE_QUERY,
    SOFTWARE_INVENTORY_INFO,
    TUNNEL_ACTIVITY,
    USER_QUERY,
    USER_SESSION_QUERY,
    // 1.3 OCSF event classes (Win extension)
    PREFETCH_QUERY,
    REGISTRY_KEY_QUERY,
    REGISTRY_VALUE_QUERY,
    WINDOWS_SERVICE_ACTIVITY
}
```

从 Security Lake 中删除自定义来源

删除自定义源可以停止将数据从该源发送到 Security Lake。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来移除自定义来源。有关移除原生支持的内容的信息， AWS 服务请参阅。从 Security Lake AWS 服务 中收集数据

在 Security Lake 中删除自定义源时，必须使用该源禁用 Security Lake 控制台之外的每个源。未能禁用集成可能会导致源集成继续向 Amazon S3 发送日志。

Console

1. 在上打开 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
```

安全湖中的订阅者管理

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。有关来源的更多信息，请参阅安全湖中的源代码管理。

Security Lake 支持两种类型的订阅用户访问：

- 数据访问当数据写入 S3 存储桶时，有权访问 Amazon Security Lake 中源数据的订阅者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。
- 查询访问权限-具有查询权限的订阅者可以查询 Security Lake 收集的数据。这些订阅者使用亚马逊 Athena 等服务直接查询 S3 存储桶中的 AWS Lake Formation 表。

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，请参阅在安全湖中管理区域。

> **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。

当某个源的新 Amazon S3 对象写入安全湖数据湖时，订阅者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。

主题

在 Security Lake 中创建具有数据访问权限的订阅者的先决条件

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。

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。

有关外部的更多信息 IDs，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，继续执行在 Security Lake 中创建具有数据访问权限的订户。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：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInvokeApiDestination",
            "Effect": "Allow",
            "Action": [
                "events:InvokeApiDestination"
            ],
            "Resource": [
            "arn:aws:events:us-east-1:123456789012: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：

JSON

```
{
    "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。

在 Security Lake 中创建具有数据访问权限的订户

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. 在上打开 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，请参阅为安全湖资源添加标签。

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": 2.0}}] \
--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 区域中自定义来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": 2.0}}] \
--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

以下示例以 JSON 结构格式显示了`CreateSubscriberNotification`操作的事件通知。

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

更新 Security Lake 中的数据订阅者

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，请参阅为安全湖资源添加标签。

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. 在上打开 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。

从安全湖移除数据订阅者

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. 在上打开 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。

订阅者使用 Amazon Athena 等服务从您 S3 存储桶中的 AWS Lake Formation 表中查询源数据。此订阅类型`LAKEFORMATION`在 CreateSubscriberAPI 的`accessTypes`参数中标识。

> **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：查看和查询您自己的数据。

主题

- 在 Security Lake 中创建具有查询权限的订阅者的先决条件
- 在 Security Lake 中创建具有查询权限的订阅者
- 在 Security Lake 中编辑具有查询权限的订阅者

在 Security Lake 中创建具有查询权限的订阅者的先决条件

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。

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。

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

> **Important**
>
> 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，网址为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。

在 Security Lake 中创建具有查询权限的订阅者

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。有关外部的更多信息 IDs，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. 在上打开 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，请参阅为安全湖资源添加标签。
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": 2.0}}] \
--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 在 Security Lake 中编辑具有查询权限的订阅者。

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. 创建共享数据库的资源链接-订阅者必须在（如果使用控制台）或 AWS Lake Formation AWS Glue（如果使用 API/AWS CLI）中创建指向共享 Lake Formation 数据库的资源链接。此资源链接将订阅者的账户指向共享数据库。选择以下访问方法之一：
   - 有关控制台和的信息 AWS CLI，请参阅创建指向共享数据目录数据库的资源链接。 在《AWS Lake Formation 开发人员指南》中。
   - 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。

在 Security Lake 中编辑具有查询权限的订阅者

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. 在上打开 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. 在上打开 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. 在上打开 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. 在上打开 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. 在上打开 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-此操作会移除之前的 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。

使用保留设置查询数据

> Amazon S3 生命周期设置会影响数据的保存时间，而这反过来又会影响您可以查询多久以前。如果您在 Security Lake 中配置了保留设置，则必须在查询中包含基于时间的筛选器，以确保结果集的范围仅限于未过期的数据文件。有关 Security Lake 中数据保留的更多信息，请参阅生命周期管理。

以下各节中的查询示例包括基于时间的过滤器，例如`eventDay`或`time_dt`，以演示这种最佳实践。

主题

- Security Lake 查询AWS源版本 1 (OCSF 1.0.0-rc.2)
- AWS源版本 2 的 Security Lake 查询 (OCSF 1.1.0)

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

以下部分提供了有关从 Security Lake 中查询数据的指导，并包括源版本 1 中原生支持的AWSAWS源代码的一些查询示例。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。

以下查询包括基于时间的过滤器，`eventDay`用于确保您的查询在配置的保留设置范围内。有关更多信息，请参阅 Querying data with retention settings。

例如，如果超过 60 天的数据已过期，则您的查询应包含时间限制，以防止访问过期的数据。对于 60 天的保留期，请在查询中加入以下子句：

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

该条款使用 59 天（而不是 60 天）来避免 Amazon S3 和 Apache Iceberg 之间出现任何数据或时间重叠。

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 CSPM调查结果
- `vpc_flow_1_0` – Amazon Virtual Private Cloud (Amazon VPC) 流日志

示例：表中所有来自 us-east **`sh_findings_1_0`** -1 区域的 Security Hub CSPM 调查结果

```
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

以下示例列出了在（2023 年 3 月 1 日）之后*20230301*（2023 年 3 月 1 日）记录的*cloud_trail_mgmt_1_0*来自源 IP *192.0.2.1* 的所有 CloudTrail 活动*us-east-1*DB_Region。

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > '20230301' AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

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
```

Security Lake 查询 CloudTrail 数据的示例

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AWS源版本 1 的一些 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 解析器查询日志的安全湖查询示例

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AWS源版本 1 的 Route 53 解析器查询日志的一些示例查询：

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 Lake 对 Security Hub CSPM 调查结果的查询示例

Security Hub CSPM 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 CSPM 会生成用于安全检查的结果，并接收来自第三方服务的调查结果。

以下是 Security Hub CSPM 调查结果的一些示例查询：

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 = 'amzn-s3-demo-bucket')
   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 CSPM 发送调查结果的产品数量

```
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 流日志的安全湖查询示例

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AWS源版本 1 的 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)

以下部分提供了有关从 Security Lake 中查询数据的指导，并包括源版本 2 原生支持的AWSAWS源代码的一些查询示例。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。

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。

以下查询包括基于时间的过滤器，`eventDay`用于确保您的查询在配置的保留设置范围内。有关更多信息，请参阅 Querying data with retention settings。

例如，如果超过 60 天的数据已过期，则您的查询应包含时间限制，以防止访问过期的数据。对于 60 天的保留期，请在查询中加入以下子句：

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

```
...
```

该条款使用 59 天（而不是 60 天）来避免 Amazon S3 和 Apache Iceberg 之间出现任何数据或时间重叠。

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 CSPM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
- `waf_2_0`—AWS WAF v2 日志

示例：表中所有来自 us-east **`sh_findings_2_0`** -1 区域的 Security Hub CSPM 调查结果

```
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

以下示例列出了在（2023 年 3 月 1 日）之后*20230301*（2023 年 3 月 1 日）记录的*vpc_flow_2_0*来自源 IP *192.0.2.1* 的所有 Amazon VPC 活动*us-west-2*DB_Region。

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
    WHERE time_dt > TIMESTAMP '2023-03-01'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time_dt desc
LIMIT 25
```

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_dtregion、和accountid实现分区。而 Security Lake 1.0 通过eventDayregion、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。可观察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 UIDs IPs、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
```

Security Lake 查询 CloudTrail 数据的示例

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：

以下是一些针对AWS源版本 2 CloudTrail 的数据查询示例：

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
```

最近 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：

以下是AWS源版本 2 的 Route 53 reesolver 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_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 Lake 对 Security Hub CSPM 调查结果的查询示例

Security Hub CSPM 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 CSPM 会生成用于安全检查的结果，并接收来自第三方服务的调查结果。

以下是AWS源版本 2 的 Security Hub CSPM 发现结果的一些查询示例：

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 = 'amzn-s3-demo-bucket')
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 CSPM 发送调查结果的产品数量

```
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 流日志的安全湖查询示例

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AWS源版本 2 的 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
```

Amazon EKS 审核日志的安全湖查询示例

Amazon EKS 日志跟踪控制平面活动直接从 Amazon EKS 控制平面向您的账户提供审计和诊断 CloudWatch 日志。这些日志可让您轻松地保护和运行您的集群。订阅者可以查询 EKS 日志以了解以下类型的信息。

以下是AWS源版本 2 的 Amazon EKS 审核日志的一些查询示例：

过去 7 天内对特定 URL 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
```

AWS WAF v2 日志的 Security Lake 查询示例

AWS WAF是一种 Web 应用程序防火墙，可用于监控最终用户向您的应用程序发送的 Web 请求并控制对您的内容的访问。

以下是AWS源版本 2 的AWS WAF v2 日志查询示例：

在过去 7 天内发布来自特定源 IP 的请求

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    http_request.http_headers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '100.123.123.123'
AND activity_name = 'Post'
LIMIT 25
```

过去 7 天内与防火墙类型 MANAGED_RULE_GROUP 匹配的请求

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

```
AND firewall_rule.type = 'MANAGED_RULE_GROUP'
LIMIT 25
```

过去 7 天内与防火墙规则中的正则表达式匹配的请求

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

拒绝获取过去 7 天内触发AWS WAF规则的AWS凭证请求

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

获取过去 7 天内按国家/地区分组的AWS凭证申请

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

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

要管理您的数据以实现经济高效的存储，您可以使用 Security Lake 中的生命周期设置为数据配置保留期。这些保留设置可帮助您指定首选的 Amazon S3 存储类别，以及 Amazon S3 对象在过渡到其他存储类到期之前在该存储类别中保留的时间段。

> **Warning**
>
> 我们建议通过 Security Lake 控制台、API 或 CLI 管理保留设置。这是因为直接在 Amazon S3 服务中修改 Amazon S3 生命周期设置可能会删除元数据并阻止您访问数据。

Security Lake 中保留设置的重要注意事项

在 Security Lake 中管理数据保留时，请查看以下注意事项：

- 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。
- 默认的 Amazon S3 存储类是 S3 Standard。如果您未配置保留设置，Security Lake 会使用 Amazon S3 生命周期配置的默认设置，即使用 S3 标准存储类无限期存储数据。
- 在 Security Lake 中，您可以在区域级别指定留存设置。例如，您可以将特定中的所有 S3 对象配置 AWS 区域 为在写入数据湖 30 天后过渡到 S3 标准-IA 存储类别。
- 虽然保留设置仅适用于存储在 S3 存储桶中的数据，但 Apache Iceberg 元数据不包括在保留策略中。

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。

Console

1. 在上打开 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 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. 在上打开 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update-data-lake命令。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。

Security Lake API 的UpdateDataLake操作作为 “upsert” 操作，如果指定的项目或记录不存在，则执行插入，如果已存在，则执行更新。Security Lake 使用 AWS 加密解决方案安全地存储您的静态数据。

在当前使用 KMS `encryptionConfiguration` 的更新调用中包含的区域中省略该密钥将保留该区域的 KMS 密钥，但指定密钥将在同一区域重置该密钥。

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，请参阅在 Security Lake 中配置汇总区域。

安全湖中的开放网络安全架构框架 (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 为常见安全事件提供了标准架构，定义了版本控制标准以促进架构的演变，还包括安全日志生成者和使用者的自治流程。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
CloudTrail 管理活动	CloudTrail	AWS	Management	API Activity、Au	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
				ation 或 Account Change	
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 CSPM	Security Hub CSPM	AWS	匹配 Security Hub CSPM 值 ProductName	Security Finding	1.0.0-rc.2
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 ation 或	1.1.0

来源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	类名	元数据版本
				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 CSPM	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
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
AWS WAF v2 日志	AWS WAF	AWS	–	HTTP 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 Security Lake 与其他软件 AWS 服务集成 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
- 数据以安全湖中的开放网络安全架构框架 (OCSF) 架构到达
- 数据以 Apache Parquet 格式到达

订阅者集成可以通过以下方式之一访问 Security Lake 数据：

- 通过 HTTPS 端点从安全湖读取源数据
- 通过亚马逊简单队列服务 (Amazon SQS) 从安全湖读取源数据 Amazon Queue
- 通过使用直接查询源数据 AWS Lake Formation

下表提供了 Security Lake 支持的 AWS 服务 集成列表。

AWS 服务	集成类型	说明	集成的工作方式
Amazon Bedrock	订阅者	生成 AI 驱动的见解以分析 Security Lake 数据。	Amazon Bedrock 集成
Amazon Detective	订阅者	通过查询 Security Lake，分析、调查	Amazon Detective 集成

AWS 服务	集成类型	说明	集成的工作方式
		并快速确定安全发现或可疑活动的根本原因。	
亚马逊 OpenSearch 服务	订阅者	使用 OpenSearch 服务摄取，从 Security Lake 数据中生成安全见解。	亚马逊 OpenSearch 服务集成
亚马逊 OpenSearch 服务摄取管道	订阅者，来源	将日志、指标和跟踪数据流式传输到 OpenSearch 服务和安全湖。	亚马逊 OpenSearch 服务摄取管道集成
亚马逊 OpenSearch 服务 zero-ETL	订阅者（查询）	使用零 ETL 在 Security Lake 中查询数据。	亚马逊 OpenSearch 服务零 ETL 直接查询集成
快点	订阅者	使用 Quick 可视化、浏览和解释 Security Lake 中的日志。	快速集成
亚马逊 SageMaker AI	订阅者	生成 AI 驱动的见解以分析 Security Lake 数据。	亚马逊 SageMaker AI 集成
AWS AppFabric	来源	采集软件即服务 (SaaS) 应用程序日志并将其标准化为 Security Lake 标准格式。	AWS AppFabric 集成
AWS Security Hub CSPM	来源	以 Security Lake 标准格式集中和存储来自 Security Hub CSPM 的安全调查结果。	AWS Security Hub CSPM 整合

与 Amazon Bedrock 集成

Amazon Bedrock 是一项完全托管的服务，它通过统一的 API 提供来自领先的人工智能初创公司和亚马逊的高性能基础模型 (FMs) 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 SageMaker 人工智能功能和 AI 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，请参阅使用亚马逊 AI Studio 和 Amazon Bedrock 为亚马逊安全湖生成 SageMaker 人工智能驱动的见解。

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 AWS 资源收集日志数据。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 将数据提取到您的 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 服务摄取将来自不同来源的安全数据发送到 OpenSearch 服务。有关如何配置 OpenSearch 服务提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 Amazon OpenSearch 服务摄取管道集成

集成类型：订阅者、来源

Amazon Serv OpenSearch ice Ingestion 是一个完全托管的无服务器数据收集器，可将日志、指标和跟踪数据流式传输到 OpenSearch 服务和安全湖。

使用 OpenSearch 摄取管道将数据发送到 Security Lake

> 你可以在 Ingestion OpenSearch 中使用亚马逊简单存储服务 (Amazon S3) Service sink 插件将数据从任何支持的来源发送到 Security Lake。Security Lake 会自动将来自 AWS 环境、本地环境和 SaaS 提供商的安全数据集中到专门构建的数据湖中。有关更多信息，请参阅使用以 Amazon Security Lake 为接收器的 OpenSearch 摄取管道。

OpenSearch 使用 OpenSearch摄取管道将数据从 Security Lake 发送到

> 您可以使用 Amazon S3 源插件将数据采集到您的 OpenSearch摄取管道中。有关更多信息，请参阅使用以 Amazon Security Lake 为来源的 OpenSearch 摄取管道。

与亚马逊 OpenSearch 服务集成 zero-ETL 直接查询

集成类型：订阅者（查询）

您可以使用 OpenSearch 服务直接查询来分析 Amazon 安全湖中的数据。 OpenSearch Service 提供零 ETL 集成，可以直接使用 OpenSearch SQL 或 OpenSearch 管道处理语言 (PPL) 在 Security Lake 中查询数据，而不会因构建摄取管道或在分析工具之间切换而产生摩擦。这种方法无需移动或复制数据，允许您使用 OpenSearch 服务仪表板中的 Discover 体验来分析数据所在的位置。当你想从查询静态数据切换到使用仪表板主动监控时，你可以对查询结果构建索引视图，然后将其提取到 OpenSearch 服务索引中。有关直接查询的更多信息，请参阅《Amazon S OpenSearch ervice 开发者指南》中的使用直接查询。

OpenSearch 服务使用 OpenSearch 无服务器集合直接查询 Security Lake 中的数据并存储您的索引视图。为此，您需要创建一个数据源，使您能够在 Security Lake 数据上使用 OpenSearch 零 ETL 功能。创建数据来源时，您可以直接搜索存储在 Security Lake 中的数据，从中获取见解并分析这些数据。您可以提高查询性能，并使用按需索引对选定的 Security Lake 数据集进行高级 OpenSearch 分析。

- 有关创建 OpenSearch 服务数据源集成的详细信息，请参阅《亚马逊 OpenSearch 服务开发者指南》中的创建 Amazon Security Lake 数据源集成。
- 有关在 OpenSearch 服务中配置安全湖数据源的详细信息，请参阅《Amazon OpenSearch Service 开发者指南》中的 “ OpenSearch 服务控制面板” 中的配置安全湖数据源。

有关使用带有 Security Lake 的 OpenSearch 服务的更多信息，请使用以下资源。

- 引入亚马逊 OpenSearch 服务和 Amazon Security Lake 集成，以简化安全分析
- Amazon Security Lake OpenSearch 服务中的零 ETL 简介

Amazon Security Lake OpenSearch 服务中的零 ETL 简介

与 Amazon Quick 集成

集成类型：订阅用户

Amazon Quick 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。快速连接到您在云中的数据，并合并来自许多不同来源的数据。Quick 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。

快速仪表板

在 Quick 中可视化您的 Amazon Security Lake 数据，创建所需的 AWS 对象，并将基本数据源、数据集、分析、控制面板和用户组部署到 Quick 中安全湖。有关详细说明，请参阅与 Amazon Quick 集成。

有关使用 Quick 可视化 Security Lake 数据的更多信息，请参阅以下资源。

使用 Quick：2024 快速学习系列可视化 Security Lake 数据

使用 Security Lake 操作 AWS WAF Web ACL 日志

与 Amazon A SageMaker I 集成

集成类型：订阅用户

Amazon SageMaker AI 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 AI ML 工具可在多个集成开发环境中使用（IDEs）。

SageMaker 人工智能见解

您可以使用 SageMaker AI Studio 为 Security Lake 生成机器学习见解。此 Studio 是一个用于机器学习的 Web 集成开发环境 (IDE)，可为数据科学家提供准备、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 CSPM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 Amazon A SageMaker I 为亚马逊安全湖数据生成机器学习见解。

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 和安全应用程序使用标准架构和中央存储库。

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 Security Lake 中的自定义来源收集数据。

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 或 AWS CLI 将其 AppFabric 作为自定义来源删除。有关说明，请参阅从 Security Lake 中删除自定义来源。

与集成 AWS Security Hub CSPM

集成类型：源

AWS Security Hub CSPM为您提供安全状态的全面视图， AWS 并帮助您的环境符合安全行业标准和最佳实践。Security Hub CSPM 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。

当你启用 Security Hub CSPM 并将 Security Hub CSPM 发现作为来源添加到 Security Lake 时，Security Hub CSPM 就会开始向 Security Lake 发送新的发现和现有发现的更新。

Security Lake 如何收到 Security Hub CSPM 调查结果

在 Security Hub CSPM 中，安全问题按调查发现进行跟踪。有些发现来自其他合作伙伴 AWS 服务 或第三方合作伙伴发现的问题。Security Hub CSPM 还通过根据规则运行自动和持续的安全检查来生成自己的调查结果。这些规则由安全控件来表示。

Security Hub CSPM 中的所有调查发现都使用名为 AWS 安全调查发现格式（ASFF）的标准 JSON 格式。

Security Lake 收到 Security Hub CSPM 的调查结果并将其转换为. 安全湖中的开放网络安全架构框架 (OCSF)

将你的 Security Hub CSPM 调查结果发送到 Security Lake

要将 Security Hub CSPM 调查结果发送到 Security Lake，您必须启用这两项服务，并将 Security Hub CSPM 调查结果作为来源添加到 Security Lake 中。有关添加 AWS 来源的说明，请参阅将添加 AWS 服务 为来源。

如果您希望 Security Hub CSPM 生成控制结果并将其发送到 Security Lake，则必须在中启用相关安全标准并按区域开启资源记录。 AWS Config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 收到 Security Hub CSPM 的调查结果

要停止接收 Security Hub CSPM 调查结果，你可以使用 Security Hub CSPM 控制台、Security Hub CSPM API 或用户指南 AWS CLI 中的以下主题中的内容：AWS Security Hub

- 禁用和启用来自集成的结果流（控制台）
- 禁用来自集成（Security Hub API、AWS CLI）的结果流

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

- 数据以安全湖中的开放网络安全架构框架 (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 CSPM 集成，则还可以在安全湖中查看这些发现。 AWS Security Hub CSPM有关启用集成的说明，请参阅与集成 AWS Security Hub CSPM。有关向 Security Hub CSPM 发送调查结果的第三方集成列表，请参阅《用户指南》中的可用第三方合作伙伴产品集成。AWS Security Hub

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。在查询数据之前，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。

- Cribl – Search
- IBM – QRadar

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

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

Bosch Software and Digital Solutions – AIShield

集成类型：源

AIShieldpowered by 通过与 Security Lake 集成，为 AI 资产Bosch提供自动漏洞分析和端点保护。

集成文档

ChaosSearch

集成类型：订阅用户

ChaosSearch为开放模式（ APIs 例如 Elasticsearch 和 SQL ）或原生包含 Kibana 和 Superset 的用户提供多模型数据访问权限。 UIs 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有助于xDome保护网络中的扩展物联网 (XIoT) 资产（包括物联网、 IIo T 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 应用程序和微服务中提供实时漏洞检测。APIsAssess 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

CrowdStrike – Next Gen SIEM

集成类型：订阅用户

使用具有原生 OCSF 架构解析器的数据连接器，简化 Secur CrowdStrike Falcon Next-Gen SIEM ity Lake 数据的摄取。 Falcon NG SIEM通过将无与伦比的安全深度和广度整合到一个统一的平台中来阻止漏洞，彻底改变了威胁检测、调查和响应。

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

Cyber Security Cloud – Cloud Fastener

集成类型：订阅用户

CloudFastener利用 Security Lake 可以更轻松地整合来自云环境的安全数据。

集成文档

DataBahn

集成类型：源

使用 Security Data Fabric 将您的安全数据集中在DataBahn's安全湖中。

集成文档（登录 DataBahn 门户查看文档）

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

您可以通过在 OCSF 架构中集成网络数据（包括对 Security Lake 的检测、来自 IOCsExtraHop Reveal(x) 360、到 Security Lake 的检测）来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

Fortinet - Cloud Native Firewall

集成类型：源

在中创建 FortiGate CNF 实例时 AWS，您可以将 Amazon Security Lake 指定为日志输出目标。

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

HTCD – AI-First Cloud Security Platform

集成类型：订阅用户

实现即时合规自动化、安全发现的优先级排序和量身定制的补丁。HTCD 可以查询 Security Lake，通过自然语言查询和 AI 驱动的见解来帮助您发现威胁。

集成文档

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汇总云原生环境 VMs 中的漏洞检测数据，并将其发送到 Security Lake。

集成文档

Palo Alto Networks – XSOAR

集成类型：订阅者

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

集成文档

Panther

集成类型：订阅用户

Panther支持摄取 Security Lake 日志以用于搜索和检测。

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

Query.AI – Query Federated Search

集成类型：订阅用户

Query Federated Search可以通过 Amazon Athena 直接查询任何 Security Lake 表，以支持事件响应、调查、威胁搜寻以及对 OCSF 架构中各种可观察对象、事件和对象的常规搜索。

集成文档

Rapid7 – InsightIDR

集成类型：订阅用户

InsightIDR，Rapid7 SIEM/XDR 解决方案，可以在 Security Lake 中提取日志，用于威胁检测和调查可疑活动。

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 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

安全湖的安全

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方 AWS 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：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon Security Lake 的合规计划，请参阅按合规计划提供的范围内的AWSAWS 服务按合规计划服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，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。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Security Lake 资源。

主题

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) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅Amazon Security Lake 身份和访问故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅安全湖如何与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅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 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问，AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，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，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

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。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。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。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。您必须在基于资源的策略中指定主体。

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。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在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。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。

安全湖如何与 IAM 配合使用

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 功能	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
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	否
服务关联角色	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》中的使用客户管理型策略定义自定义 IAM 权限。

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。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 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。您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。

要启用跨账户访问，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。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Security Lake 服务会为存储数据的 Amazon S3 存储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 存储桶。Security Lake 会代表您自动创建这些策略。

示例资源是一个 S3 存储桶，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 存储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：

JSON

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

```
                    "aws:SecureTransport": "false"
                }
            }
        },
        {
            "Sid": "PutSecurityLakeObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "securitylake.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-
identifier}"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-
east-1:111122223333:*"
                }
            }
        }
    ]
}
```

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。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 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。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，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 您可以使用在策略中指定这些类型的资源 ARNs。

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 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。

`Condition` 元素根据定义的条件指定语句何时执行。您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。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 Security Lake 基于身份的策略示例。

Security Lake 中的访问控制列表 (ACLs)

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 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 ACLs，这意味着你无法将 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，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `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》中的使用 ABAC 授权定义权限。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，请参阅为安全湖资源添加标签。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 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

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。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 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

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

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。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担任、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

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入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关联角色的权限。

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 在 Security Lake 中使用服务相关角色。

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。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。

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（控制台）。

有关 Security Lake 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 Amazon Security Lake 的操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践
- 使用 Security Lake 控制台
- 示例：允许用户查看自己的权限
- 示例：允许组织管理账户指定和移除委托的管理员
- 示例：允许用户根据标签查看订阅用户

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，请遵循以下指南和建议：

- 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 策略设置权限时，请仅授予执行任务所需的权限。为此，您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 策略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，您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的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 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 策略，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 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您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》中的使用 IAM Access Analyzer 验证策略。
- 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 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 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 中的安全最佳实践。

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。

JSON

```
{
    "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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewSubscriberDetailsIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:GetSubscriber",
            "Resource": "arn:aws:securitylake:*:*:subscriber/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListSubscribersIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:ListSubscribers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

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，请参阅为安全湖资源添加标签。

AWS 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使用案例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。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AmazonSecurityLakeMetastoreManager。

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。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AmazonSecurityLakePermissionsBoundary。

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：

> **Note**
>
> 为了提供足够的权限来授予基于 Lake Formation 的订阅者访问权限，Security Lake 建议添加以下`glue:PutResourcePolicy`权限。

JSON

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

```
  "Statement": [
    {
      "Sid": "AllowPutLakeFormationSettings",
      "Effect": "Allow",
      "Action": "lakeformation:PutDatalakeSettings",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowGlueActions",
      "Effect": "Allow",
      "Action": ["glue:PutResourcePolicy", "glue:DeleteResourcePolicy"],
      "Resource": [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    }
  ]
}
```

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。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AmazonSecurityLakeAdministrator。

AWS 托管策略： SecurityLakeServiceLinkedRole

Security Lake 使用名为AWSServiceRoleForSecurityLake的服务相关角色来创建和操作安全数据湖。

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 Security Lake 的服务相关角色权限。

AWS 托管策略： SecurityLakeResourceManagementServiceRolePolicy

Security Lake 使用名为的服务关联角色AWSServiceRoleForSecurityLakeResourceManagement来执行持续监控和性能改进，从而减少延迟和成本。提供管理由 Security Lake 创建的资源的权限。让 Security Lake 能够删除 SecurityLake _Glue_Partition_Updater_Lambda。对于已执行冰山迁移并转向 v2 源代码的客户，此 lambda 已被弃用。这个 lambda 使用的是 Python 3.9 运行时，该运行时将于 12 月被弃用。与其为这些客户更新此 lambda 的运行时，不如将其删除。我们有一个恢复流程，可以确定客户是否还需要 lambda，如果他们不需要，则将其删除。为了允许我们删除那个 lambda，需要进行这个 SLR 更新。

您不能将 SecurityLakeResourceManagementServiceRolePolicy 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，请参阅资源管理的服务关联角色权限。

权限详细信息

该策略包含以下权限。

- events— 允许委托人列出和管理 Security Lake 事件处理 EventBridge 规则。
- lambda— 允许委托人管理 Security Lake 元数据处理的 Lambda 函数和配置，包括能够删除已弃用的分区更新程序函数。
- glue— 允许委托人在 Security Lake 元数据管理 AWS Glue 的数据目录中创建分区、管理表和访问数据库。
- s3— 允许委托人管理安全湖数据湖操作的 Amazon S3 存储桶配置、生命周期策略和元数据对象。
- logs— 允许委托人访问 CloudWatch 日志流并查询 Security Lake Lambda 函数的日志数据。
- sqs— 允许委托人管理 Security Lake 数据处理工作流程的 Amazon SQS 队列和消息。
- lakeformation— 允许委托人检索数据湖设置和 Security Lake 资源管理权限。

要查看有关策略（包括 JSON 策略文档的最新版本）的更多信息，请参阅《AWS 托管式策略参考指南》中的 SecurityLakeResourceManagementServiceRolePolicy。

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 Security Lake 中的自定义来源收集数据。

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
SecurityLakeResourceManagementServiceRolePolicy— 更新了现有政策	Security Lake 更新了托管策略SecurityLakeResourceManagementServiceRolePolicy ，为已弃用的 SecurityLake _Glue_Partition_Updater_Lambda 函数添加了lambda:DeleteFunction 权限。这允许 Security Lake 在迁移到 v2 源代码和冰山格式的过程中清理已弃用的 Lambda 函数。	2025 年 11 月 18 日
AWSServiceRoleForSecurityLakeResourceManagement— 更新了现有政策	此政策已更新，将StringLike 运算符替换为ArnLike运算符，以评估aws:ResourceAccount 条件块lambda:FunctionArn 中的 ARN 类型密钥。这可确保策略执行更加安全。	2025 年 9 月 25 日
Amazon Security Lake 的服务相关角色 — 新的服务相关角色	我们添加了一个新的服务相关角色AWSServiceRoleForSecurityLakeResourceManagement 。此服务相关角色向 Security Lake 提供执行持续监控和性能改进的权限，从而减少延迟和成本。	2024 年 11 月 14 日
Amazon Security Lake 的服务相关角色 — 更新现有服务相关角色权限	我们在该策略的 AWS 托管策略中添加了 AWS WAF SecurityLakeServiceLinkedRole 操作。在 Security Lake 中启用为 AWS WAF 日志源时，其他操作允许 Security Lake 收集日志。	2024 年 5 月 22 日

更改	描述	日期
AmazonSecurityLake PermissionsBoundary：对现有策略的更新	Security Lake 在策略中添加了 SID 操作。	2024 年 5 月 13 日
AmazonSecurityLake MetastoreManager：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：对现有策略的更新	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
AmazonSecurityLake MetastoreManager：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 托管策略的更改。	2022 年 11 月 29 日

在 Security Lake 中使用服务相关角色

Security Lake 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是直接关联到 Security Lake 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 在所有可用 Security Lake AWS 区域 的地方都使用此服务相关角色。

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、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务关联角色权限。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，并在服务相关角色列中查找标有 “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 的服务关联角色 (SLR) 权限
- 用于资源管理的服务关联角色 (SLR) 权限

Security Lake 的服务关联角色 (SLR) 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。有关 Amazon Security Lake AWS 托管策略的更多信息，请参阅AWS 管理亚马逊安全湖的策略。

该角色的权限策略是一个名为的 AWS 托管策略`SecurityLakeServiceLinkedRole`，允许 Security Lake 创建和操作安全数据湖。该策略还允许 Security Lake 对指定资源执行以下操作：

- 使用 AWS Organizations 操作检索关联账户的相关信息
- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 检索有关 Amazon VPC 流日志的信息
- 使用 AWS CloudTrail 操作检索有关服务相关角色的信息
- 在 Security AWS WAF Lake 中启用日志作为日志源后，使用 AWS WAF 操作收集日志
- 使用`LogDelivery`操作创建或删除 AWS WAF 日志传输订阅。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 SecurityLakeServiceLinkedRole。

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

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。当您为自己启用 Security Lake 时 AWS 账户，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。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

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。相反，您可以从 IAM 控制台、API 或 AWS CLI中删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

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 AWS 区域 Security Lake 服务关联角色

Security Lake 支持在所有可用 Security Lake AWS 区域 的地方使用AWSServiceRoleForSecurityLake服务相关角色。有关提供 Security Lake 的区域的列表，请参阅 安全湖区域和终端节点。

用于资源管理的服务关联角色 (SLR) 权限

Security Lake 使用名为的服务关联角色AWSServiceRoleForSecurityLakeResourceManagement来执行持续监控和性能改进，从而减少延迟和成本。该服务相关角色信任 resource-management.securitylake.amazonaws.com 服务担任该角色。启用AWSServiceRoleForSecurityLakeResourceManagement后还将授予其

访问 Lake Formation 的权限，并自动在所有区域向 Lake Formation 注册您的 Security Lake 托管的 S3 存储桶，以提高安全性。

该角色的权限策略是一个名为的 AWS 托管策略`SecurityLakeResourceManagementServiceRolePolicy`，允许访问管理由 Security Lake 创建的资源，包括管理数据湖中的元数据。有关亚马逊安全湖 AWS 托管策略的更多信息，请参阅亚马逊安全湖AWS 托管策略。

此服务相关角色允许 Security Lake 监控安全湖部署到您的账户的资源（S3 存储桶、 AWS Glue 表、Amazon SQS 队列、Metastore Manager (MSM) Lambda 函数和规则）的运行状况。EventBridge Security Lake 可使用此服务相关角色执行的一些操作示例如下：

- Apache Iceberg 清单文件压缩，可提高查询性能并降低 Lambda MSM 处理时间和成本。
- 监控 Amazon SQS 的状态以检测摄取问题。
- 优化跨区域数据复制以排除元数据文件。

> **Note**
>
> 如果您不安装`AWSServiceRoleForSecurityLakeResourceManagement`服务相关角色，Security Lake 将继续运行，但强烈建议您接受此服务相关角色，以便 Security Lake 可以监控和优化您账户中的资源。

权限详细信息

该角色使用以下权限策略进行配置：

- `events`— 允许委托人管理日志源和日志订阅者所需的 EventBridge 规则。
- `lambda`— 允许委托人管理用于在 AWS 源数据传输和跨区域复制之后更新 AWS Glue 表分区的 lambda。
- `glue`— 允许委托人对 AWS Glue 数据目录表执行特定的写入操作。这还允许 AWS Glue 抓取工具识别数据中的分区，并允许 Security Lake 管理你的 Apache Iceberg 表的 Apache Iceberg 元数据。
- `s3`— 允许委托人对包含日志数据和 Glue 表元数据的 Security Lake 存储桶执行特定的读写操作。
- `logs`— 允许委托人读取权限将 Lambda 函数 CloudWatch 的输出记录到日志中。
- `sqs`— 允许委托人对在数据湖中添加或更新对象时接收事件通知的 Amazon SQS 队列执行特定的读写操作。

- `lakeformation`— 允许校长读取 Lake Formation 设置以监控配置错误。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 SecurityLakeResourceManagementServiceRolePolicy。

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

创建 Security Lake 服务相关角色

您可以使用 Security Lake 控制台或 Security Lake 创建`AWSServiceRoleForSecurityLakeResourceManagement`服务相关角色。 AWS CLI

要创建服务相关角色，您必须向您的 IAM 用户或 IAM 角色授予以下权限。在所有启用安全湖的区域中，IAM 角色必须是 Lake Formation 管理员。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLakeFormationActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIamActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:PutRolePolicy"
```

```
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/resource-
management.securitylake.amazonaws.com/
AWSServiceRoleForSecurityLakeResourceManagement",
        "arn:*:iam::*:role/*AWSServiceRoleForLakeFormationDataAccess",
        "arn:*:iam::aws:policy/service-role/AWSGlueServiceRole",
        "arn:*:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager",
        "arn:*:iam::aws:policy/aws-service-role/
SecurityLakeResourceManagementServiceRolePolicy"
      ],
      "Condition": {
        "StringLikeIfExists": {
          "iam:AWSServiceName": [
            "securitylake.amazonaws.com",
            "resource-management.securitylake.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowGlueActionsViaConsole",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:*:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ]
    }
  ]
}
```

Console

1. 在上打开 Security Lake 控制台https://console.aws.amazon.com/securitylake/。
2. 单击 “摘要” 页面信息栏中的 “启用服务相关角色”，接受新的服务相关角色。

启用服务相关角色后，将来使用 Security Lake 时无需重复此过程。

CLI

要以编程方式创建AWSServiceRoleForSecurityLakeResourceManagement服务相关角色，请使用以下 CLI 命令。

```
$ aws iam create-service-linked-role
--aws-service-name resource-management.securitylake.amazonaws.com
```

使用创建AWSServiceRoleForSecurityLakeResourceManagement服务相关角色时 AWS CLI，您还必须向其授予 Security Lake Glue 数据库上所有表的 Lake Formation 表级权限（ALTER、DESCRIBE），以管理表元数据和访问数据。如果任何区域中的 Glue 表引用了之前启用安全湖的 S3 存储桶，则必须暂时授予服务相关角色的 DATA_LOCATION_ACCESS 权限，以允许 Security Lake 纠正这种情况。

您还必须向账户的AWSServiceRoleForSecurityLakeResourceManagement服务相关角色授予 Lake Formation 权限。

以下示例说明如何向指定区域中的服务相关角色授予 Lake Formation 权限。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 lakeformation grant-permissions --region {region} --principal
 DataLakePrincipalIdentifier={AWSServiceRoleForSecurityLakeResourceManagement ARN} \
--permissions ALTER DESCRIBE --resource '{ "Table": { "DatabaseName":
 "amazon_security_lake_glue_db_{region}", "TableWildcard": {} } }'
```

以下示例显示了角色 ARN 的外观。您必须编辑角色 ARN 以匹配您的区域。

```
"AWS": "arn:[partition]:iam::[accountid]:role/aws-service-
role/resource-management.securitylake.amazonaws.com/
AWSServiceRoleForSecurityLakeResourceManagement"
```

您也可以使用 CreateServiceLinkedRoleAPI 调用。在请求中，指定 a AWSServiceName s resource-management.securitylake.amazonaws.com。

启用该AWSServiceRoleForSecurityLakeResourceManagement角色后，如果您使用 AWS KMS 客户托管密钥 (CMK) 进行加密，则必须允许服务相关角色将加密对象写入存在 CMK 的 AWS 区域中的 S3 存储桶。在 AWS KMS 控制台中，将以下策略添加到 CMK 存在的 AWS 区域中的 KMS 密

钥。有关如何更改 KMS 密钥策略的详细信息，请参阅《 AWS Key Management Service 开发人员指南》AWS KMS中的密钥策略。

```
{
    "Sid": "Allow SLR",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::[regional-datalake-s3-
bucket-name]"
        },
        "StringLike": {
            "kms:ViaService": "s3.[region].amazonaws.com"
        }
    }
},
```

创建 Security Lake 服务相关角色

Security Lake 不允许您编辑 AWSServiceRoleForSecurityLakeResourceManagement 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。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

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。相反，您可以从 IAM 控制台、API 或 AWS CLI中删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

您必须先确认服务相关角色没有活动会话并删除 AWSServiceRoleForSecurityLakeResourceManagement 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 `AWSServiceRoleForSecurityLakeResourceManagement` 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 `AWSServiceRoleForSecurityLakeResourceManagement` 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 AWS 区域 Security Lake 服务关联角色

Security Lake 支持在所有可用 Security Lake AWS 区域 的地方使用`AWSServiceRoleForSecurityLakeResourceManagement`服务相关角色。有关提供 Security Lake 的区域的列表，请参阅 安全湖区域和终端节点。

Amazon Security Sake 中的数据保护

分 AWS 担责任模式适用于亚马逊安全湖中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。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 Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

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) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。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）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 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 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 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 140-3 版》。

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）。这包括您 AWS 服务 使用控制台、API 或与 Security Lake 或其他人合作时 AWS SDKs。 AWS CLI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，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您的静态数据。原始安全日志和事件数据存储在特定于源的多租户亚马逊简单存储服务 (Amazon S3) Simple Storage S3 存储桶中，该存储桶由安全湖管理的账户。每个日志源都有自己的多租户存储桶。Security Lake 使用来自 AWS Key Management Service (AWS KMS) 的AWS 自有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 Securit AWS KMS y Lake）拥有和管理的密钥集合，供多个账户使用。 AWS

Security Lake 对原始日志和事件数据运行提取、转换和加载（ETL）任务。

ETL 任务完成后，Security Lake 会在您的账户中创建单租户 S3 存储桶（您在其中启用 Security Lake AWS 区域 的每个存储桶对应一个存储桶）。只有在 Security Lake 能够可靠地将数据传送到单租户 S3 存储分段之前，数据才会暂时存储在多租户 S3 存储桶中。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 存储桶中的数据，您可以选择 S3 托管的加密密钥或客户托管的密钥（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 存储桶的数据使用 Amazon S3 托管的加密密钥（SSE-S3）进行 Amazon 服务器端加密。要提供您可以直接管理的安全层，您可以改为使用带有 AWS KMS 密钥的服务器端加密 (SSE-KMS) 来处理您的 Sec urity Lake 数据。

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 存储桶的数据，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。中的授权 AWS KMS 用于授予 Security Lake 访问客户账户中的 KMS 密钥的权限。

Security Lake 需要该授权才能将客户托管密钥用于以下内部操作：

- 向发送GenerateDataKey请求 AWS KMS 以生成由您的客户托管密钥加密的数据密钥。
- 向RetireGrant... 发送请求 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。

如果要使用现有的 KMS 密钥来加密 Security Lake 数据，则必须修改 KMS 密钥的密钥策略。密钥策略必须允许与 Lake Formation 数据湖位置关联的 IAM 角色使用 KMS 密钥解密数据。有关如何更改 KMS 密钥的密钥策略的说明，请参阅 AWS Key Management Service 开发人员指南中的更改密钥策略。

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。名为的 AWS 托管策略AmazonSecurityLakePermissionsBoundary设置了这些角色的权限边界。

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？ 在 AWS 知识中心中。

由于 Security Lake 用于支持 AWS Lambda 对您的数据进行提取、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 对 AWS 服务之间传输的所有数据进行加密。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。发送到安全湖 APIs 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进服务

您可以使用选择退出政策，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。AWS Organizations 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 账户必须由集中管理。 AWS Organizations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

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

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，为您的 AWS Identity and Access Management (IAM) 用户、用户组和角色授予最低访问策略权限。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 Security Lake 基于身份的策略示例。

您还可以使用 AWS CloudTrail 来跟踪 Security Lake 中的 API 使用情况。 CloudTrail 提供用户、群组或角色在 Security Lake 中执行的 API 操作的记录。有关更多信息，请参阅 使用记录安全湖 API 调用 CloudTrail。

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 存储桶的问题。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 CSPM 集成

集成 Security Lake 并在 AWS Security Hub CSPM 安全湖中接收 Security Hub CSPM 调查结果。Security Hub CSPM 从许多不同的 AWS 服务 第三方集成中生成调查结果。接收 Security Hub CSPM 调查结果有助于你大致了解自己的合规状况以及是否符合 AWS 安全最佳实践。

有关更多信息，请参阅 与集成 AWS Security Hub CSPM。

删除 AWS Lambda

删除 AWS Lambda 函数时，我们建议不要先将其禁用。在删除之前禁用 Lambda 函数可能会干扰数据查询功能，并可能影响其他功能。最好直接删除 Lambda 函数而不将其禁用。有关删除 Lambda 函数的更多信息，请参阅AWS Lambda 开发者指南。

监控 Security Lake 事件

您可以使用 Amazon CloudWatch 指标监控安全湖。 CloudWatch 每分钟从 Security Lake 收集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 CloudWatch 亚马逊安全湖的指标。

Amazon Security Lake 中的故障恢复能力

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。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结构相比，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 全球基础设施外，Security Lake（其中的数据由亚马逊简单存储服务 (Amazon S3) Service 提供支持）还提供多项功能来帮助支持您的数据弹性和备份需求。

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存储桶中保留对象的多个变量的方法。对于 Amazon S3 存储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 存储桶中使用版本控制。

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 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问安全湖。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（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

Security Lake 中的配置和脆弱性分析

配置和 IT 控制由您（我们的客户）共同 AWS 负责。有关更多信息，请参阅责任 AWS 共担模型。

Amazon 安全湖和接口 VPC 终端节点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点在您的 VPC 和 Amazon Security Lake 之间建立私有连接。接口端点由一项技术提供支持 AWS PrivateLink，该技术使您 APIs 无需互联网网关、NAT 设备、VPN 连接或 Di AWS rect Connect 连接即可私密访问 Security Lake。您的 VPC 中的实例不需要公有 IP 地址即可与安全湖通信 APIs。您的 VPC 和安全湖之间的流量不会离开亚马逊网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅 AWS PrivateLink 指南中的接口 VPC 端点 (AWS PrivateLink)。

安全湖 VPC 终端节点的注意事项

在为 Security Lake 设置接口 VPC 终端节点之前，请务必查看AWS PrivateLink 指南中的接口终端节点属性和限制。

Security Lake 支持从您的 VPC 调用其所有 API 操作。

Security Lake 仅在以下存在 FIPS 的区域支持 FIPS VPC 终端节点：

- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（北加利福尼亚）
- 美国西部（俄勒冈州）

为安全湖创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为安全湖服务创建 VPC 终端节点。有关更多信息，请参阅《AWS PrivateLink 指南》中的创建接口端点。

使用以下服务名称为安全湖创建 VPC 终端节点：

- com.amazonaws。 *region*. securityL
- com.amazonaws。 *region*.securitylake-fips（FIPS 端点）

例如，如果您为终端节点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 Security Lake 发出 API 请求`securitylake.us-east-1.amazonaws.com`。

有关更多信息，请参阅 AWS PrivateLink 指南中的通过接口端点访问服务。

为安全湖创建 VPC 终端节点策略

您可以将终端节点策略附加到控制安全湖访问权限的 VPC 终端节点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅 AWS PrivateLink 指南中的使用 VPC 端点控制对服务的访问。

示例：安全湖操作的 VPC 终端节点策略

以下是 Security Lake 的终端节点策略示例。当连接到终端节点时，此策略向所有资源的所有委托人授予访问列出的 Security Lake 操作的权限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers"
         ],
         "Resource":"*"
      }
   ]
}
```

共享子网

您无法在与您共享的子网中创建、描述、修改或删除 VPC 端点。但是，您可以在与您共享的子网中使用 VPC 端点。有关 VPC 共享的信息，请参阅《Amazon VPC 用户指南》中的与其他账户共享 VPC。

监控 Amazon Security Lake

Security Lake 与 AWS CloudTrail集成，后者是一项服务，用于记录用户、角色或其他角色在 Security Lake 中执行的操作 AWS 服务。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。通过使用收集的信息 CloudTrail，您可以确定向 Security Lake 提出了哪些请求。对每一个请求，您可以识别请求的时间、发出请求的源 IP 地址以及其他详细信息。有关更多信息，请参阅使用记录安全湖 API 调用 CloudTrail。

Security Lake 和 Amazon CloudWatch 是集成的，因此您可以收集、查看和分析 Security Lake 收集的日志的指标。 CloudWatch 系统会自动收集 Security Lake 数据湖的指标，并每隔 CloudWatch 一分钟推送一次。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 发送到的所有指标的列表 CloudWatch，请参阅Security Lake 指标和维度。

CloudWatch 亚马逊安全湖的指标

您可以使用 Amazon 监控 Security Lake CloudWatch，亚马逊每分钟收集一次原始数据，并将其处理成可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。还可以设置特定阈值监视警报，在达到对应阈值时发送通知或采取行动。

主题

Security Lake 指标和维度

AWS/SecurityLake 命名空间包括以下指标。

指标	说明
ProcessedSize	当前存储在您的数据湖中的来自原生支持 AWS 服务 的数据量。 单位：字节

下列维度可用于 Security Lake 指标。

维度	说明
Account	特定 AWS 账户的 ProcessedSize 指标。此维度仅在您查看开启时可用 CloudWatch。Per-Account Source Version Metrics
Region	特定 AWS 区域的 ProcessedSize 指标。
Source	ProcessedSize 特定 AWS 日志源的指标。
SourceVersion	ProcessedSize AWS 日志源特定版本的指标。

您可以查看组织中特定账户 AWS 账户 (`Per-Account Source Version Metrics`) 或所有账户 (`Per-Source Version Metrics`) 的指标。

查看安全湖的 CloudWatch 指标

您可以使用 CloudWatch 控制台、 CloudWatch自己的命令行界面 (CLI) 或使用 CloudWatch API 以编程方式监控 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. 打开 CloudWatch 控制台，网址为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 访问安全湖指标，请使用`GetMetricStatistics`操作。

AWS CLI

要使用访问安全湖指标 AWS CLI，请运行`get-metric-statistics`命令。

有关使用指标进行监控的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch指标。

为安全湖指标设置 CloudWatch 警报

CloudWatch 还允许您在指标达到阈值时设置警报。例如，您可以为该ProcessedSize指标设置警报，以便在来自特定来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，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch警报。

使用记录安全湖 API 调用 CloudTrail

Amazon Secur AWS CloudTrail ity Lake 与一项服务集成，该服务提供用户、角色或 AWS 服务在安全湖中采取的操作的记录。 CloudTrail 将安全湖的 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，则可以将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括安全湖的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 Security Lake 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

安全湖中的信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Security Lake 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的事件 AWS 账户，包括 Security Lake 的事件，请创建跟踪。跟踪允许 CloudTrail 将事件作为日志文件传输到您指定的 Amazon S3 存储桶。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。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

Security Lake 操作由 Sec urity Lake API 参考记录 CloudTrail 并记录在案。例如，对`UpdateDataLakeListLogSources`、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。身份信息有助于您确定以下内容：

- 请求是使用根凭证还是 AWS Identity and Access Management 用户凭证发出的。

- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 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。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

以下示例显示了 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"
}
```

为安全湖资源添加标签

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，并且每个标签键只能有一个标签值。
- 标签键和值区分大小写。作为最佳实践，我们建议您定义一个利用标签的策略，并在所有资源中一致地实施该策略。
- 一个标签键最多可包含 128 个 UTF-8 字符。一个标签值最多可包含 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。您不能在自己定义的任何标签键或值中使用此前缀。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 个标签限额中。

- 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 账单与成本管理。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）策略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：

JSON

```
{
    "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，而且您可以快速地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. 在上打开 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。然后，在值框中，可以选择输入标签键的标签值。

   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。此示例的格式适用于 Linux、macOS 或 Unix，它使用了反斜杠 (\) 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` 实际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` 实际参数指定值。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。

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. 在上打开 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，可以选择输入关联的标签值。
   - 要更改现有标签值，请在包含该值的值框中选择 X。然后，在值框中输入新的标签值。
   - 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（包括标签键和标签值），请选择标签旁边的删除。

   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. 完成对标签的编辑后，选择保存。

API

当您以编程方式编辑资源的标签时，将使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、标签值还是两者兼而有之。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。此示例的格式适用于 Linux、macOS 或 Unix，它使用了反斜杠 (\) 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。

要从标签键中删除标签值，请不要在 `tags` 形式参数中为该标签键的 `value` 实际参数指定值。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。

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. 在上打开 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
```

在前面的示例中，*arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab*是现有订阅者的 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。

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. 在上打开 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：

   - 要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. 完成删除标签后，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` 形式参数指定要删除的标签的标签键。要删除多个标签，请为要删除的每个标签添加 `tagKeys` 形式参数和实际参数，并用和符号（&）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。

对安全湖中的问题进行故障排除

如果您在使用 Amazon Security Lake 时遇到问题，请使用以下疑难解答资源。

以下主题为您可能遇到的与数据湖状态、Lake Formation、在 Amazon Athena AWS Organizations 中查询和 IAM 相关的错误和问题提供了疑难解答建议。如果您发现此处未列出的问题，则可以使用此页面上的Feedback按钮进行举报。

如果在使用 Security Lake 时遇到问题，请参考以下主题。

主题

- 对数据湖状态进行故障排除
- Lake Formation 故障排除
- 对亚马逊 Athena 中的查询进行疑难解答
- Orgations 故障排除
- Amazon Security Lake 身份和访问故障排除

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 安全湖中的源代码管理。

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，网址为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. 从导航窗格中选择 Functions，然后根据源版本从以下列表中选择函数：
   - `Source version 1 (OCSF 1.0.0-rc.2)` — SecurityLake_glue_Partition_Updater_***#region>*** Lambda_ 函数。
   - `Source version 2 (OCSF 1.1.0)`— AmazonSecurityLakeMetastoreManager_***#region>*** 函数。
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 管理控制台 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。

我想将权限扩展到托管策略之外

订阅者或自定义日志源创建的所有 IAM 角色 APIs 都受`AmazonSecurityLakePermissionsBoundary`托管策略的约束。如果要将权限扩展到托管策略之外，可以将托管策略从角色的权限边界中移除。但是，在与变更 DataLak APIs es 和订阅者的 Security Lake 交互时，必须附加权限边界，IAM 才能更改 IAM 角色。

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。您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 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

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，请参阅安全湖如何与 IAM 配合使用。
- 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
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）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 中的跨账户资源访问。

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。

当你在 Security Lake 支持的任何 AWS 区域 一个 AWS 账户 中首次开启日志收集功能时，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。

> **Note**
>
> 在 15 天免费试用期结束后继续使用 Security Lake 时，您将自动开始产生使用费用。为了防止在免费试用期结束后产生费用，您必须禁用 Security Lake。

要了解 Security Lake 定价背后的方法，请观看以下视频：Amazon Security Lake 定价-->

数据摄取

这些费用来自摄取的 AWS CloudTrail 日志以及其他 AWS 服务 日志和事件（Amazon Route 53 解析器查询日志、 AWS Security Hub CSPM 调查结果和 Amazon VPC 流日志）的数量。

数据转换

这些成本来自于 Security Lake 标准化为安全湖中的开放网络安全架构框架 (OCSF)架构并转换为 Apache Parquet 格式的 AWS 服务 日志和事件量。

相关服务的费用

以下是您在安全数据湖中存储和共享数据可能会产生的一些费用： AWS 服务

- Amazon S3 – 这些费用来自在您的 Security Lake 账户中维护 Amazon S3 存储桶、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。
- 亚马逊 EventBridge — 这些费用来自亚马逊 EventBridge 向订阅终端节点发送对象通知。有关更多信息，请参阅 Amazon EventBridge 定价。
- AWS Glue — 每月费用由每千兆字节从 AWS 服务中摄取的日志和事件数据量决定。您的数据存储在亚马逊简单存储服务中，并收取标准的 Amazon S3 费用。Security Lake 还会代表您协调其他 AWS 服务。对于作为安全数据湖一部分使用的 AWS 服务和设置的资源，您将分别收取费用。查看亚马逊AWS Glue、 EventBridgeAWS Lambda、亚马逊 SQS 和亚马逊简单通知服务的定价。您应承担因从 Security Lake 查询数据和存储查询结果而产生的费用。

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。

有关费用和辅助服务的完整列表，请参阅 Sec urity 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。这是根据您在所选时间段内的实际使用情况，在未来 30 个日历日内预测的 Security Lake 当前 AWS 区域 成本。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。

即使您尚未在 Security Lake 中添加特定 AWS 数据源，所有支持的数据源都显示在前面的表中。如果您正在参与免费试用，我们建议您添加所有 AWS 来源，以获取全套日志和事件的成本估算。有关添加 AWS 源的说明，请参阅从 Security Lake AWS 服务 中收集数据。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. 在上打开 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。

安全湖区域和终端节点

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 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。

如果您在 Security Lake 中配置了一个或多个自定义源并禁用了该服务，则还必须独立于 Security Lake 禁用每个源。否则，自定义源将继续向 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。

Important

如果您禁用 Security Lake，请同时删除数据湖的现有 AWS Glue 资源。否则，如果您稍后再次启用 Security Lake，则后续查询将无法正常运行。尽管删除 AWS Glue 资源是主要要求，但组织可以灵活地管理与数据湖相关的额外资源。

如果您选择移除 AWS Glue 组件之外的资源，那么遵循 “要么全有要么全无” 的方法至关重要。如果您决定删除辅助资源，则必须全面删除所有关联的组件。这些额外资源包括：安全湖 SQS 队列 (`AmazonSecurityLakeManager-xxx`)、安全湖 Lambda 函数、事件源映射以及相关的 IAM 角色，例如角色。`AmazonSecurityLakeMetaStoreManagerV2`

在此过程中，您无需移除存储数据湖数据的 Amazon S3 存储桶。Organizations 可以在不影响清理程序的情况下保留这些存储桶。关键的考虑因素是避免部分移除资源，这可能会在未来的部署中导致配置问题。

计划停用数据湖时，请仔细评估是只删除 AWS Glue 资源还是要执行彻底的资源清理。如果您选择全面删除，请确保遵循系统的删除流程并移除所有相关组件。

重新启用安全湖后，将在新的 Amazon S3 存储桶中创建一个新的数据湖，并将数据收集到这个新的 S3 存储桶中。如果您之前删除过 AWS Glue 表，则会创建一组新的 AWS Glue 表。

在禁用 Security Lake 之前收集的所有数据都将保留在之前的 Amazon S3 存储桶中。如果要查询旧数据，则必须使用 Amazon S3 Sync 命令将数据移动到新存储桶。有关更多详细信息，请参阅《命令参考》中的 “同步” AWS CLI 命令。

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. 在上打开 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：2025 年 4 月 24 日

变更	说明	日期
更新了托管策略	Security Lake 已更新托管策略`SecurityLakeResourceManagementServiceRolePolicy` ，为已弃用的 SecurityLake _Glue_Partition_Updater_Lambda 函数添加`lambda:DeleteFunction` 权限。这允许 Security Lake 在迁移到 v2 源代码和冰山格式的过程中清理已弃用的 Lambda 函数。有关信息，请参阅 Security Lake 对 AWS 托管策略的更新。	2025 年 11 月 18 日
更新了服务相关角色权限	Security Lake 已AWSServiceRoleForSecurityLakeResourceManagement通过`StringLike` 替换为来更新`ArnLike`。	2025 年 9 月 25 日
更新了功能-服务相关角色	现在，Security AWSServiceRoleForSecurityLakeResourceManagement Lake 会在创建数据湖期间自动创建 SLR。有关更多信息，请参阅注意事项。	2025 年 4 月 24 日

大幅重写的话题—— AWS 集成	更新了指定 Security Lake 集成的具体内容 AWS 服务。有关更多信息，请参阅AWS 服务集成。	2025 年 3 月 31 日
更新了功能-管理多个账户	Security Lake 控制台现在支持管理账户加入组织时的自动启用配置。有关更多信息，请参阅在控制台中编辑新账户配置。	2025 年 3 月 10 日
更新了功能- AWS WAF 日志中的数据保护	在 Security Lake 账户的 Web ACL 中启用数据保护后，增加了对数据保护的支持。有关更多信息，请参阅 Sec urity Lake 中的AWS WAF 日志。	2025 年 2 月 17 日
新功能 – 增加了对 VPC 端点的支持	Security Lake 现已与 VPC 终端节点集成 AWS PrivateLink 并支持。有关 AWS PrivateLink 集成的更多信息，请参阅 Amazon Security Lake 和接口 VPC 终端节点 (AWS PrivateLink)。	2025 年 2 月 4 日
新特征	Security Lake 现在支持 OpenSearch 服务直接查询，以分析安全湖中的数据。有关更多详细信息，请参阅与 OpenSearch 服务集成。	2024 年 12 月 1 日

新服务相关角色	我们添加了一个新的服务相关角色AWSServiceRoleForSecurityLakeResourceManagement。此服务相关角色向 Security Lake 提供执行持续监控和性能改进的权限，从而减少延迟和成本。	2024 年 11 月 14 日
区域可用性	Security Lake 现已在 AWS GovCloud（美国东部）和 AWS GovCloud（美国西部）推出。 AWS 区域有关当前提供 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。	2024 年 6 月 10 日
对现有托管策略的更新	我们在该策略的 AWS 托管策略中添加了 AWS WAF SecurityLakeServiceLinkedRole 操作。在 Security Lake 中启用为 AWS WAF 日志源时，其他操作允许 Security Lake 收集日志。	2024 年 5 月 22 日
新的 AWS 日志源	Security Lake 添加了 AWS WAF 日志作为 AWS 日志源。AWS WAF 帮助您监控最终用户向应用程序发送的 Web 请求。	2024 年 5 月 22 日
对现有托管策略的更新	我们在AmazonSecurityLakePermissionsBoundary策略中添加了 SID 操作。	2024 年 5 月 13 日

对现有托管策略的更新	我们更新了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 Lake 将 EKS 审计 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
对现有托管策略的更新	我们更新了政策，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
新托管式策略	我们添加了一个新的AWS托管策略，即 `AmazonSecurityLakeMetastoreManager` 策略。此策略授予 Security Lake 管理数据湖中元数据的权限。	2024 年 1 月 23 日

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
新特征	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
新托管式策略	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。