



使用者指南

# Amazon Security Lake



# Amazon Security Lake: 使用者指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 Amazon Security Lake ? .....	1
Security Lake 概觀 .....	1
Security Lake 的功能 .....	1
存取 Security Lake .....	3
相關服務 .....	3
概念和術語 .....	5
開始使用 .....	6
設定您的 AWS 帳戶 .....	6
註冊 AWS 帳戶 .....	6
建立具有管理存取權的使用者 .....	7
識別您將用來啟用 Security Lake 的帳戶 .....	8
啟用 Security Lake 時的考量事項 .....	8
使用主控台 .....	9
步驟 1：設定來源 .....	9
步驟 2：定義儲存設定和彙總區域（選用） .....	11
步驟 3：檢閱和建立資料湖 .....	11
步驟 4：檢視和查詢您自己的資料 .....	11
步驟 5：建立訂閱者 .....	12
使用 AWS CLI 或 API .....	12
步驟 1：建立 IAM 角色 .....	12
步驟 2：啟用 Amazon Security Lake .....	13
步驟 3：設定來源 .....	14
步驟 4：設定儲存設定和彙總區域（選用） .....	14
步驟 5：檢視和查詢您自己的資料 .....	16
步驟 6：建立訂閱者 .....	16
管理多個 帳戶 .....	17
委派 Security Lake 管理員的重要考量事項 .....	18
指定委派管理員所需的 IAM 許可 .....	18
指定委派的 Security Lake 管理員並新增成員帳戶 .....	19
在主控台中編輯新帳戶組態 .....	21
移除委派的 Security Lake 管理員 .....	22
Security Lake 受信任存取 .....	22
管理 區域 .....	24
檢查區域狀態 .....	24

變更區域設定 .....	25
設定彙總區域 .....	26
資料複寫的 IAM 角色 .....	27
用於註冊 AWS Glue 分割區的 IAM 角色 .....	30
新增彙總區域 .....	30
更新或移除彙總區域 .....	31
來源管理 .....	33
從 收集資料 AWS 服務 .....	33
先決條件：驗證許可 .....	34
新增 AWS 服務 做為來源 .....	35
取得來源集合的狀態 .....	36
更新角色許可 .....	37
移除 AWS 服務 做為來源 .....	38
CloudTrail 事件日誌 .....	40
Amazon EKS 稽核日誌 .....	41
Route 53 Resolver 查詢日誌 .....	41
Security Hub 調查結果 .....	41
VPC 流量日誌 .....	42
AWS WAF 日誌 .....	43
移除 AWS 服務 做為來源 .....	38
從自訂來源收集資料 .....	44
擷取自訂來源的分割區需求 .....	46
新增自訂來源的先決條件 .....	46
新增自訂來源 .....	49
刪除自訂來源 .....	53
訂閱者管理 .....	55
訂閱者資料存取 .....	55
先決條件 .....	56
建立具有資料存取權的訂閱者 .....	59
更新資料訂閱者 .....	62
移除資料訂閱者 .....	63
訂閱者查詢存取 .....	64
先決條件 .....	64
建立具有查詢存取權的訂閱者 .....	66
編輯具有查詢存取權的訂閱者 .....	69
Security Lake 查詢 .....	73

Security Lake 查詢來源版本 1 .....	73
日誌來源資料表 .....	74
資料庫區域 .....	75
分割區日期 .....	75
CloudTrail 資料的查詢 .....	77
Route 53 解析程式查詢日誌的查詢 .....	79
Security Hub 調查結果的查詢 .....	81
Amazon VPC 流程日誌的查詢 .....	84
Security Lake 查詢來源版本 2 .....	88
日誌來源資料表 .....	74
資料庫區域 .....	75
分割區日期 .....	75
查詢 Security Lake 可觀測項目 .....	91
CloudTrail 資料的查詢 .....	92
Route 53 解析程式查詢日誌的查詢 .....	94
Security Hub 調查結果的查詢 .....	96
Amazon VPC 流程日誌的查詢 .....	99
Amazon EKS 稽核日誌的查詢 .....	102
v AWS WAF 2 日誌的查詢 .....	103
生命週期管理 .....	107
保留管理 .....	107
Security Lake 中保留設定的重要考量事項 .....	107
啟用 Security Lake 時設定保留設定 .....	107
更新保留設定 .....	109
彙總區域 .....	110
Open Cybersecurity Schema Framework (OCSF) .....	111
什麼是 OCSF ? .....	111
OCSF 事件類別 .....	111
OCSF 來源識別 .....	111
整合 .....	114
AWS 服務 整合 .....	114
Amazon Bedrock 整合 .....	116
Amazon Detective 整合 .....	116
Amazon OpenSearch Service 整合 .....	116
Amazon OpenSearch Service Ingestion 管道整合 .....	117
Amazon OpenSearch Service 零 ETL 直接查詢整合 .....	117

QuickSight 整合 .....	118
Amazon SageMaker AI 整合 .....	119
AWS AppFabric 整合 .....	119
AWS Security Hub 整合 .....	120
第三方整合 .....	121
查詢整合 .....	122
Accenture – MxDR .....	122
Aqua Security .....	122
Barracuda – Email Protection .....	123
Booz Allen Hamilton .....	123
Bosch Software and Digital Solutions – AIShield .....	123
ChaosSearch .....	123
Cisco Security – Secure Firewall .....	123
Claroty – xDome .....	124
CMD Solutions .....	124
Confluent – Amazon S3 Sink Connector .....	124
Contrast Security .....	124
Cribl – Search .....	125
Cribl – Stream .....	125
CrowdStrike – Falcon Data Replicator .....	125
CrowdStrike – Next Gen SIEM .....	125
CyberArk – Unified Identify Security Platform .....	125
Cyber Security Cloud – Cloud Fastener .....	126
DataBahn .....	126
Darktrace – Cyber AI Loop .....	126
Datadog .....	126
Deloitte – MXDR Cyber Analytics and AI Engine (CAE) .....	126
Devo .....	127
DXC – SecMon .....	127
Eviden – Alsaac ( 先前為 Atos) .....	127
ExtraHop – Reveal(x) 360 .....	127
Falcosidekick .....	128
Fortinet - Cloud Native Firewall .....	128
Gigamon – Application Metadata Intelligence .....	128
Hoop Cyber .....	128
HTCD – AI-First Cloud Security Platform .....	128

---

IBM – QRadar .....	129
Infosys .....	129
Insbuilt .....	129
Kyndryl – AIOps .....	129
Lacework – Polygraph .....	130
Laminar .....	130
MegazoneCloud .....	130
Monad .....	130
NETSCOUT – Omnis Cyber Intelligence .....	130
Netskope – CloudExchange .....	131
New Relic ONE .....	131
Okta – Workforce Identity Cloud .....	131
Orca – Cloud Security Platform .....	131
Palo Alto Networks – Prisma Cloud .....	132
Palo Alto Networks – XSOAR .....	132
Panther .....	132
Ping Identity – PingOne .....	132
PwC – Fusion center .....	132
Query.AI – Query Federated Search .....	133
Rapid7 – InsightIDR .....	133
RipJar – Labyrinth for Threat Investigations .....	133
Sailpoint .....	133
Securonix .....	134
SentinelOne .....	134
Sentra – Data Lifecycle Security Platform .....	134
SOC Prime .....	134
Splunk .....	134
Stellar Cyber .....	135
Sumo Logic .....	135
Swimlane – Turbine .....	135
Sysdig Secure .....	135
Talon .....	136
Tanium .....	136
TCS .....	136
Tego Cyber .....	136
Tines – No-code security automation .....	136

Torq – Enterprise Security Automation Platform .....	137
Trellix – XDR .....	137
Trend Micro – CloudOne .....	137
Uptycs – Uptycs XDR .....	138
Vectra AI – Vectra Detect for AWS .....	138
VMware Aria Automation for Secure Clouds .....	138
Wazuh .....	138
Wipro .....	138
Wiz – CNAPP .....	139
Zscaler – Zscaler Posture Control .....	139
安全 .....	140
身分與存取管理 .....	140
目標對象 .....	141
使用身分驗證 .....	141
使用政策管理存取權 .....	144
Security Lake 如何與 IAM 搭配使用 .....	146
身分型政策範例 .....	153
AWS 受管政策 .....	157
使用服務連結角色 .....	179
資料保護 .....	195
靜態加密 .....	195
傳輸中加密 .....	198
選擇不使用您的資料以改善服務 .....	198
法規遵循驗證 .....	198
Security Lake 的安全最佳實務 .....	199
授予 Security Lake 使用者最低可能許可 .....	199
檢視摘要頁面 .....	199
與 Security Hub 整合 .....	200
刪除 AWS Lambda .....	200
監控 Security Lake 事件 .....	200
恢復能力 .....	200
基礎架構安全 .....	201
Security Lake 中的組態和漏洞分析 .....	202
VPC 端點 (AWS PrivateLink) .....	202
Security Lake VPC 端點的考量事項 .....	202
為 Security Lake 建立介面 VPC 端點 .....	202

為 Security Lake 建立 VPC 端點政策 .....	203
共用子網路 .....	203
監控 .....	204
Amazon Security Lake 的 CloudWatch 指標 .....	204
記錄 API 呼叫 .....	207
CloudTrail 中的 Security Lake 資訊 .....	207
了解 Security Lake 日誌檔案項目 .....	208
標記 資源 .....	210
標記基礎知識 .....	210
在 IAM 政策中使用標籤 .....	211
將標籤新增至資源 .....	212
編輯 資源的標籤 .....	214
檢閱資源的標籤 .....	216
移除資源的標籤 .....	218
故障診斷 .....	220
對資料湖狀態進行故障診斷 .....	220
對 Lake Formation 問題進行故障診斷 .....	221
找不到資料表 .....	221
400 AccessDenied .....	221
SYNTAX_ERROR .....	221
無法將發起人的主要 ARN 新增至 Lake Formation .....	222
具有 Lake Formation 的 CreateSubscriber 未建立新的 RAM 資源共享邀請 .....	222
對 Amazon Athena 中的查詢進行故障診斷 .....	222
查詢不會在資料湖中傳回新物件 .....	223
無法存取 AWS Glue 資料表 .....	223
對 Organizations 問題進行故障診斷 .....	223
存取遭拒錯誤 .....	224
IAM 問題疑難排解 .....	224
我無權在 Security Lake 中執行動作 .....	224
我想要將許可擴展到受管政策之外 .....	224
我未獲授權執行 iam:PassRole .....	224
我想要允許 以外的人員 AWS 帳戶 存取我的 Security Lake 資源 .....	225
Security Lake 定價 .....	226
檢閱用量和預估成本 .....	227
支援的區域和端點 .....	229
停用 Security Lake .....	230

---

文件歷史紀錄 .....	232
.....	CCXXXVII

# 什麼是 Amazon Security Lake ？

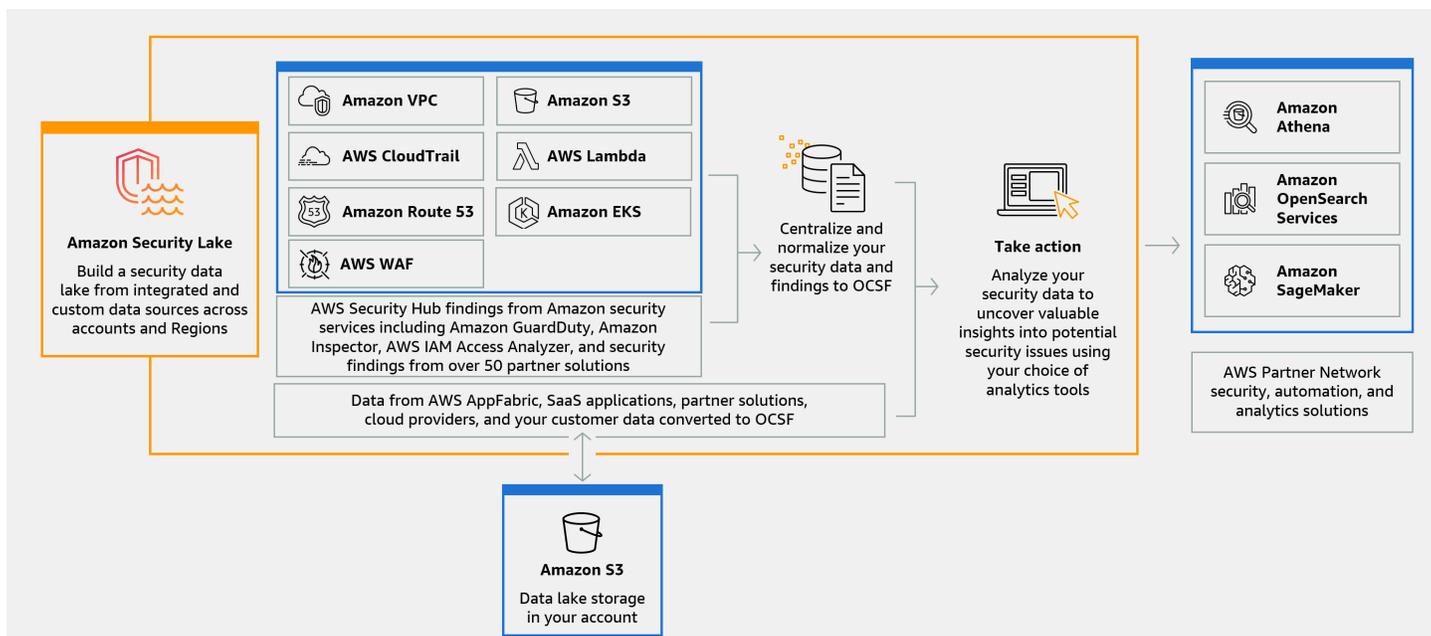
Amazon Security Lake 是完全受管的安全資料湖服務。您可以使用 Security Lake，將 AWS 環境、SaaS 提供者、內部部署、雲端來源和第三方來源的安全資料自動集中到存放在 中的專用資料湖 AWS 帳戶。Security Lake 可協助您分析安全資料，因此您可以更完整地瞭解整個組織的安全狀態。透過 Security Lake，您還可以改善工作負載、應用程式和資料的保護。

資料湖由 Amazon Simple Storage Service (Amazon S3) 儲存貯體提供支援，您可以保留資料的所有權。

Security Lake 會自動從整合和第三方服務收集與安全相關的日誌 AWS 服務 和事件資料。它還可協助您使用可自訂的保留和複寫設定來管理資料的生命週期。Security Lake 將擷取的資料轉換為 Apache Parquet 格式，以及稱為開放式網路安全結構描述架構 (OCSF) 的標準開放原始碼結構描述。透過 OCSF 支援，Security Lake 會標準化和合併來自 AWS 和各種企業安全資料來源的安全性資料。

其他 AWS 服務 和第三方服務可以訂閱存放在 Security Lake 中的資料，以進行事件回應和安全資料分析。

## Security Lake 概觀



## Security Lake 的功能

以下是 Security Lake 協助您集中、管理和訂閱安全相關日誌和事件資料的一些重要方式。

## 將資料彙總至您的帳戶

Security Lake 會在您的帳戶中建立專用安全資料湖。Security Lake 會從雲端、內部部署和跨帳戶和區域的自訂資料來源收集日誌和事件資料。資料湖由 Amazon Simple Storage Service (Amazon S3) 儲存貯體提供支援，您可以保留資料的所有權。

## 各種支援的日誌和事件來源

Security Lake 會從多個來源收集安全日誌和事件，包括內部部署 AWS 服務和第三方服務。擷取日誌之後，無論來源為何，您都可以集中存取它們，並管理其生命週期。如需 Security Lake 收集日誌和事件來源的詳細資訊，請參閱 [Security Lake 中的來源管理](#)

## 資料轉換和標準化

Security Lake 會自動分割來自原生支援 AWS 服務的資料，並將其轉換為具有儲存和查詢效率的 Parquet 格式。它也會 AWS 服務 將資料從原生支援轉換為開放式網路安全結構描述架構 (OCSF) 開放原始碼結構描述。這可讓資料與其他 AWS 服務 和第三方供應商相容，而不需要後製處理。由於 Security Lake 會標準化資料，因此許多安全解決方案可以平行使用這些資料。

## 訂閱者的多重存取層級

訂閱者會使用存放在 Security Lake 中的資料。您可以選擇訂閱者的存取資料層級。訂閱者只能使用 AWS 區域您指定的來源和 中的資料。訂閱者在寫入資料湖時，可能會收到新物件的自動通知。或者，訂閱者可以從資料湖查詢資料。Security Lake 會自動建立和交換 Security Lake 與訂閱者之間所需的登入資料。

## 多帳戶和多區域資料管理

您可以在所有可用區域以及多個區域集中啟用 Security Lake AWS 帳戶。在 Security Lake 中，您也可以指定彙總區域來合併來自多個區域的安全日誌和事件資料。這可協助您遵守資料駐留合規要求。

## 可設定且可自訂

Security Lake 是一項可設定且可自訂的服務。您可以指定要設定日誌集合的來源、帳戶和區域。您也可以指定訂閱者對資料湖的存取層級。

## 資料生命週期管理和最佳化

Security Lake 使用可自訂的保留設定來管理資料的生命週期，並使用自動化儲存分層來管理儲存成本。Security Lake 會自動分割傳入的安全資料並將其轉換為儲存體，並查詢有效的 Apache Parquet 格式。

# 存取 Security Lake

如需目前可使用 Security Lake 的區域清單，請參閱 [Security Lake 區域和端點](#)。若要進一步了解區域，請參閱 [AWS 服務端點](#) [AWS 一般參考](#)。

在每個區域中，您可以透過下列任何方式存取 Security Lake：

## AWS Management Console

AWS Management Console 是以瀏覽器為基礎的介面，可用來建立和管理 AWS 資源。Security Lake 主控台可讓您存取 Security Lake 帳戶和資源。您可以使用 Security Lake 主控台來執行大多數 Security Lake 任務。

## Security Lake API

若要以程式設計方式存取 Security Lake，請使用 Security Lake API，並直接向服務發出 HTTPS 請求。如需詳細資訊，請參閱 [Security Lake API 參考](#)。

## AWS Command Line Interface (AWS CLI)

使用 AWS CLI，您可以在系統的命令列發出命令，以執行 Security Lake 任務和 AWS 任務。使用命令列可以比使用主控台更快、更方便。若您想要建構執行任務的指令碼，命令列工具也非常實用。如需有關安裝和使用的資訊 AWS CLI，請參閱 [AWS Command Line Interface](#)。

## AWS SDKs

AWS 提供包含程式庫和範例程式碼 SDKs，適用於各種程式設計語言和平台，例如 Java、Go、Python、C++ 和 .NET。SDKs 提供對 Security Lake 和其他的便利、程式設計存取 AWS 服務。他們也會處理密碼編譯簽署請求、管理錯誤和自動重試請求等任務。如需安裝和使用 AWS SDKs 的詳細資訊，請參閱 [要建置的工具 AWS](#)。

# 相關服務

以下是 AWS 服務 Security Lake 使用的其他項目：

- [Amazon EventBridge](#) – Security Lake 使用 EventBridge 在物件寫入資料湖時通知訂閱者。
- [AWS Glue](#) – Security Lake 使用 AWS Glue 爬蟲程式來建立 AWS Glue Data Catalog 資料表，並將新寫入的資料傳送至 Data Catalog。Security Lake 也會在 Data Catalog 中存放 AWS Lake Formation 資料表的分割區中繼資料。

- [AWS Lake Formation](#) – Security Lake 會為每個來源建立單獨的 Lake Formation 資料表，將資料貢獻給 Security Lake。Lake Formation 資料表包含每個來源的資料相關資訊，包括結構描述、分割區和資料位置資訊。訂閱者可以選擇查詢 Lake Formation 資料表來使用資料。
- [AWS Lambda](#) – Security Lake 使用 Lambda 函數來支援原始資料上的擷取、轉換和載入 (ETL) 任務，以及註冊來源資料的分割區 AWS Glue。
- [Amazon S3](#) – Security Lake 會將您的資料儲存為 Amazon S3 物件。儲存類別和保留設定是以 Amazon S3 產品為基礎。Security Lake 不支援 Amazon S3 Select。
- [Amazon Simple Queue Service](#) – Security Lake 使用 Amazon SQS 來啟用事件驅動的處理和管理通知。

Security Lake 會從自訂來源收集資料，除了下列項目之外 AWS 服務：

- AWS CloudTrail 管理和資料事件 (S3、Lambda)
- Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌
- Amazon Route 53 Resolver 查詢日誌
- AWS Security Hub 問題清單
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌
- AWS WAF v2 日誌

如需這些來源的詳細資訊，請參閱在 [Security Lake AWS 服務 中從 收集資料](#)。您可以透過建立可在 OCSF 結構描述中讀取資料的訂閱者，來取用安全資料湖中的 Amazon S3 物件。您也可以使用 Amazon Athena、Amazon Redshift 和與整合的第三方訂閱服務來查詢資料 AWS Glue。

# 概念和術語

本節說明可協助您使用 Amazon Security Lake 的重要概念和術語。

## 貢獻區域

一或多個 AWS 區域 將資料貢獻至彙總區域。

## 資料湖

存放在 Amazon Simple Storage Service (Amazon S3) 中並由 Security Lake 管理的持久性資料。Security Lake 使用 AWS Glue 將新寫入的資料傳送至 Data Catalog。Security Lake 也會為每個來源建立 AWS Lake Formation 資料表，將資料貢獻至資料湖。資料湖通常會存放下列項目：

- 結構化和非結構化資料
- 原始和轉換的資料

Security Lake 是一種資料湖服務，旨在收集與安全相關的日誌和事件。

## Open Cybersecurity Schema Framework (OCSF)

安全性日誌和事件的標準化[開放原始碼結構描述](#)。它由 AWS 和 和其他安全產業領導者跨各種安全網域開發。Security Lake 會自動將從 收集 AWS 服務 的日誌和事件轉換為 OCSF 結構描述。自訂來源在將其日誌和事件傳送到 Security Lake 之前，將其轉換為 OCSF。

## 彙總區域

AWS 區域 合併一或多個貢獻區域的安全日誌和事件。指定一或多個彙總區域可協助您符合區域合規要求。

## 來源

從單一系統產生的一組日誌和事件，符合 [OCSF](#) 中的特定事件類別。Security Lake 可以從來源收集資料。來源可能是另一個 AWS 服務 或第三方服務。對於第三方來源，您必須先將資料轉換為 OCSF 結構描述，然後再將其傳送至 Security Lake。

## Subscriber

使用來自 Security Lake 的日誌和事件的服務。訂閱者可以是另一個 AWS 服務 或第三方服務。

# Amazon Security Lake 入門

本節中的主題說明如何啟用和開始使用 Security Lake。您將了解如何設定您的資料湖設定和設定日誌收集。您可以透過 AWS Management Console 或以程式設計方式啟用和使用 Security Lake。無論您使用哪種方法，您必須先設定 AWS 帳戶和管理使用者。之後的步驟會根據存取方法而有所不同。

Security Lake 主控台提供簡化的入門程序，並建立建立資料湖所需的所有必要 AWS Identity and Access Management (IAM) 角色。

如果您以程式設計方式存取 Security Lake，則必須建立某些 AWS Identity and Access Management (IAM) 角色，才能設定您的資料湖。

## Important

Security Lake 不支援回填啟用 Security Lake 之前產生的現有 AWS 原始日誌來源事件。

## 主題

- [設定您的 AWS 帳戶](#)
- [啟用 Security Lake 時的考量事項](#)
- [使用主控台啟用 Security Lake](#)
- [以程式設計方式啟用 Security Lake](#)

## 設定您的 AWS 帳戶

您必須先有 [AWS 帳戶](#)，才能啟用 Amazon Security Lake AWS 帳戶。如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

### 註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

#### 註冊 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
2. 請遵循線上指示進行。

部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行 [需要根使用者存取權的任務](#)。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 建立具有管理存取權的使用者

註冊後 AWS 帳戶，請保護您的 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立管理使用者，如此您就不會將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者 [AWS Management Console](#) 身分登入。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的 [以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需說明，請參閱《IAM 使用者指南》中的 [為您的 AWS 帳戶根使用者（主控台）啟用虛擬 MFA 裝置](#)。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的 [啟用 AWS IAM Identity Center](#)。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱 AWS IAM Identity Center 《使用者指南》中的 [使用預設值設定使用者存取 IAM Identity Center 目錄](#)。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 [《使用者指南》](#) 中的 [登入 AWS 存取入口網站](#)。

## 指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的 [建立許可集](#)。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的 [新增群組](#)。

## 識別您將用來啟用 Security Lake 的帳戶

Security Lake 與 整合 AWS Organizations ，以管理組織中多個帳戶的日誌收集。如果您想要為組織使用 Security Lake ，您必須使用 Organizations 管理帳戶來指定委派的 Security Lake 管理員。然後，您必須使用委派管理員的登入資料來啟用 Security Lake、新增成員帳戶，以及為其啟用 Security Lake。如需詳細資訊，請參閱 [在 Security Lake AWS Organizations 中使用 管理多個帳戶](#)。

或者，您可以為不屬於組織的獨立帳戶使用 Security Lake ，而不需要 Organizations 整合。

## 啟用 Security Lake 時的考量事項

啟用 Security Lake 之前，請考慮下列事項：

- Security Lake 提供跨區域管理功能，這表示您可以跨 建立資料湖並設定日誌收集 AWS 區域。若要 [在所有支援的區域中](#) 啟用 Security Lake ，您可以選擇任何支援的 區域端點。您也可以新增 [彙總區域](#)，將多個區域的資料彙總到單一區域。
- 建議您在所有支援的 中啟用 Security Lake AWS 區域。如果您這樣做，Security Lake 可以收集連線至未經授權或異常活動的資料，即使在您未主動使用的區域中也是如此。如果 Security Lake 未在所有支援的區域中啟用，其從您在多個區域中使用的其他 服務收集資料的能力會降低。
- 當您第一次在任何區域中啟用 Security Lake 時，它會為您的帳戶建立下列服務連結角色：
  - [AWSServiceRoleForSecurityLake](#)：此角色包含 AWS 服務 代表您呼叫其他 並操作安全資料湖的許可。如果您啟用 Security Lake 做為 [委派的 Security Lake 管理員](#)，Security Lake 會在 [組織中的每個成員帳戶中建立服務連結角色](#)。

- [AWSServiceRoleForSecurityLakeResourceManagement](#) : Security Lake 使用此角色來執行持續的監控和效能改善，這可能會降低延遲和成本。此服務連結角色信任 `resource-management.securitylake.amazonaws.com` 服務擔任該角色。啟用此服務角色也會授予 Lake Formation 的存取權。

如需有關這如何影響 2025 年 4 月 17 日之前啟用 Security Lake 的現有帳戶的資訊，請參閱 [Update for existing accounts](#)。

如需有關服務連結角色如何運作的資訊，請參閱《IAM 使用者指南》中的 [使用服務連結角色許可](#)。

- Security Lake 不支援 Amazon S3 物件鎖定。建立資料湖儲存貯體時，預設會停用 S3 物件鎖定。在儲存貯體上啟用物件鎖定會中斷將標準化日誌資料交付至資料湖。
- 如果您要在區域中重新啟用 Security Lake，您必須從先前使用的 Security Lake 中刪除該區域的對應 AWS Glue 資料庫。

## 使用主控台啟用 Security Lake

本教學說明如何透過 啟用和設定 Security Lake AWS Management Console。作為的一部分 AWS Management Console，Security Lake 主控台提供簡化的入門程序，並建立建立資料湖所需的所有必要 AWS Identity and Access Management (IAM) 角色。

### 步驟 1：設定來源

Security Lake 會從各種來源以及您的 和 收集日誌 AWS 帳戶 和事件資料 AWS 區域。請依照這些指示來識別您希望 Security Lake 收集哪些資料。您只能使用這些指示來新增原生支援的 AWS 服務 做為來源。如需新增自訂來源的詳細資訊，請參閱 [從 Security Lake 中的自訂來源收集資料](#)。

#### 設定日誌來源集合

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選取區域。您可以在加入時在目前區域和其他區域中啟用 Security Lake。
3. 選擇開始使用。
4. 針對選取日誌和事件來源，選擇下列其中一個來源選項：
  - a. 擷取預設 AWS 來源 – 當您選擇建議的選項時，CloudTrail - S3 資料事件預設 AWS WAF 不會包含用於擷取。這是因為擷取大量這兩種來源類型可能會大幅影響使用成本。若要擷取這些來源，請先選取擷取特定 AWS 來源選項，然後從日誌和事件來源清單中選取這些來源。

- b. 擷取特定 AWS 來源 – 使用此選項，您可以選取要擷取的一或多個日誌和事件來源。

 Note

當您第一次在帳戶中啟用 Security Lake 時，所有選取的日誌和事件來源都將是 15 天免費試用期的一部分。如需用量統計資料的詳細資訊，請參閱 [檢閱用量和預估成本](#)。

5. 針對版本，選擇您要從中擷取日誌和事件來源的資料來源版本。如需有關版本的詳細資訊，請參閱 [OCSF 來源識別](#)。

 Important

如果您沒有在指定區域中啟用新版本 AWS 日誌來源所需的角色許可，請聯絡您的 Security Lake 管理員。如需詳細資訊，請參閱 [更新角色許可](#)。

6. 針對選取區域，選擇是否從所有支援的區域或特定區域擷取日誌和事件來源。如果您選擇特定區域，請選取要擷取資料的區域。
7. 對於選取帳戶，請執行下列步驟：
  1. 選擇 Security Lake 是否會從組織中的所有帳戶或特定帳戶擷取資料。系統會使用您在此組態期間選擇的設定，為這些帳戶啟用 Security Lake。
  2. 預設會選取自動為新組織帳戶啟用 Security Lake 核取方塊。這些自動啟用設定將在加入您的組織 AWS 帳戶時套用到。您可以隨時編輯自動啟用設定。

 Note

自動啟用設定只會在帳戶加入您的組織時套用，而不會套用到現有帳戶。如需詳細資訊，請參閱 [在主控台中編輯新帳戶組態](#)。

8. 對於服務存取，建立新的 IAM 角色或使用現有 IAM 角色，授予 Security Lake 從您的來源收集資料並將其新增至資料湖的許可。您啟用 Security Lake 的所有區域都會使用一個角色。
9. 選擇下一步。

## 步驟 2：定義儲存設定和彙總區域（選用）

您可以指定您希望 Security Lake 存放資料的 Amazon S3 儲存類別，以及存放資料的時間長度。您也可以指定彙總區域來合併來自多個區域的資料。這些是選用步驟。如需詳細資訊，請參閱[Security Lake 中的生命週期管理](#)。

### 設定儲存和彙總設定

1. 如果您想要將多個貢獻區域的資料合併至彙總區域，請在選取彙總區域中選擇新增彙總區域。指定彙總區域和將對其做出貢獻的區域。您可以設定一或多個彙總區域。
2. 針對選取儲存類別，選擇 Amazon S3 儲存類別。預設儲存類別為 S3 Standard。如果您希望資料在該時間之後轉換到另一個儲存類別，請提供保留期間（以天為單位），然後選擇新增轉換。保留期間結束後，物件會過期，Amazon S3 會將其刪除。如需 Amazon S3 儲存類別和保留的詳細資訊，請參閱[保留管理](#)。
3. 如果您在第一個步驟中選取了彙總區域，對於服務存取，請建立新的 IAM 角色或使用現有 IAM 角色，授予 Security Lake 跨多個區域複寫資料的許可。
4. 選擇下一步。

## 步驟 3：檢閱和建立資料湖

檢閱 Security Lake 將從中收集資料的來源、您的彙總區域，以及您的保留設定。然後，建立您的資料湖。

### 若要檢閱和建立資料湖

1. 啟用 Security Lake 時，請檢閱日誌和事件來源、區域、彙總區域和儲存類別。
2. 選擇建立。

建立資料湖後，您會在 Security Lake 主控台上看到摘要頁面。此頁面提供區域和彙總區域數量、訂閱者相關資訊和問題的概觀。

問題功能表會顯示過去 14 天內影響 Security Lake 服務或 Amazon S3 儲存貯體的問題摘要。如需有關每個問題的其他詳細資訊，您可以前往 Security Lake 主控台的問題頁面。

## 步驟 4：檢視和查詢您自己的資料

建立資料湖後，您可以使用 Amazon Athena 或類似服務來檢視和查詢 AWS Lake Formation 資料庫和資料表中的資料。當您使用主控台時，Security Lake 會自動將資料庫檢視許可授予您用來啟用

Security Lake 的角色。角色至少必須具有資料分析師許可。如需許可層級的詳細資訊，請參閱 [Lake Formation 角色和 IAM 許可參考](#)。如需授予 SELECT 許可的指示，請參閱《AWS Lake Formation 開發人員指南》中的 [使用具名資源方法授予資料目錄許可](#)。

## 步驟 5：建立訂閱者

建立您的資料湖之後，您可以新增訂閱者以取用您的資料。訂閱者可以透過直接存取 Amazon S3 儲存貯體中的物件或查詢資料湖來取用資料。如需訂閱者的詳細資訊，請參閱 [Security Lake 中的訂閱者管理](#)。

## 以程式設計方式啟用 Security Lake

本教學課程說明如何以程式設計方式啟用和開始使用 Security Lake。Amazon Security Lake API 可讓您以程式設計方式存取 Security Lake 帳戶、資料和資源。或者，您可以使用 AWS 命令列工具 - [AWS Command Line Interface](#) 或 [AWS Tools for PowerShell](#) - 或 [AWS SDKs](#) 來存取 Security Lake。

### 步驟 1：建立 IAM 角色

如果您以程式設計方式存取 Security Lake，則必須建立某些 AWS Identity and Access Management (IAM) 角色，才能設定您的資料湖。

#### Important

如果您使用 Security Lake 主控台來啟用和設定 Security Lake，則不需要建立這些 IAM 角色。

如果您要採取下列一或多個動作，則必須在 IAM 中建立角色（選擇連結以查看每個動作的 IAM 角色詳細資訊）：

- [建立自訂來源](#) – 自訂來源是原生支援以外的來源 AWS 服務，可將資料傳送至 Security Lake。
- [建立具有資料存取的訂閱者](#) – 具有許可的訂閱者可以直接從您的資料湖存取 S3 物件。
- [建立具有查詢存取權的訂閱者](#) – 具有許可的訂閱者可以使用 Amazon Athena 等服務從 Security Lake 查詢資料。
- [設定彙總區域](#) – 彙總區域會合併來自多個的資料 AWS 區域。

建立先前提及的角色後，請將 [AmazonSecurityLakeAdministrator](#) AWS 受管政策連接至您用來啟用 Security Lake 的角色。此政策授予管理許可，允許委託人加入 Security Lake 並存取所有 Security Lake 動作。

連接 [AmazonSecurityLakeMetaStoreManager](#) AWS 受管政策，以建立您的資料湖或從 Security Lake 查詢資料。Security Lake 需要此政策，才能支援從來源接收之原始日誌和事件資料的擷取、轉換和載入 (ETL) 任務。

## 步驟 2：啟用 Amazon Security Lake

若要以程式設計方式啟用 Security Lake，請使用 Security Lake API [CreateDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [create-data-lake](#) 命令。在您的請求中，使用 configurations 物件的 region 欄位來指定要啟用 Security Lake 之區域的區域代碼。如需區域代碼清單，請參閱《》中的 [Amazon Security Lake 端點](#) AWS 一般參考。

### 範例 1

下列範例命令會在 us-east-1 和 us-east-2 區域中啟用 Security Lake。在這兩個區域中，此資料湖都會使用 Amazon S3 受管金鑰加密。物件會在 365 天後過期，物件會在 60 天後轉換為 ONEZONE\_IA S3 儲存類別。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ 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"
```

### 範例 2

下列範例命令會在 us-east-2 區域中啟用 Security Lake。此資料湖會使用在 AWS Key Management Service (KMS) 中建立的客戶受管金鑰加密 AWS KMS。物件會在 500 天後過期，而物件會在 30 天後轉換為 GLACIER S3 儲存類別。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ 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

如果您已啟用 Security Lake，並想要更新區域或來源的組態設定，請使用 [UpdateDataLake](#) 操作，或使用 AWS CLI [update-data-lake](#) 命令。請勿使用 CreateDataLake 操作。

## 步驟 3：設定來源

Security Lake 會從各種來源以及您的 和 收集日誌 AWS 帳戶 和事件資料 AWS 區域。請依照這些指示來識別您希望 Security Lake 收集哪些資料。您只能使用這些指示來新增原生支援的 AWS 服務 做為來源。如需新增自訂來源的詳細資訊，請參閱 [從 Security Lake 中的自訂來源收集資料](#)。

若要以程式設計方式定義一或多個集合來源，請使用 Security Lake API 的 [CreateAwsLogSource](#) 操作。針對每個來源，指定 `sourceName` 參數的區域唯一值。選擇性地使用其他參數，將來源的範圍限制為特定帳戶 (accounts) 或特定版本 (`sourceVersion`)。

#### Note

如果您未在請求中包含選用參數，Security Lake 會根據您排除的參數，將您的請求套用至指定來源的所有帳戶或所有版本。例如，如果您是組織的委派 Security Lake 管理員，而且您排除 `accounts` 參數，Security Lake 會將您的請求套用到組織中的所有帳戶。同樣地，如果您排除 `sourceVersion` 參數，Security Lake 會將您的請求套用至指定來源的所有版本。

如果您的請求指定您尚未啟用 Security Lake 的區域，則會發生錯誤。若要解決此錯誤，請確定 `regions` 陣列僅指定您已啟用 Security Lake 的區域。或者，您可以在 區域中啟用 Security Lake，然後再次提交您的請求。

當您第一次在帳戶中啟用 Security Lake 時，所有選取的日誌和事件來源都將是 15 天免費試用期的一部分。如需用量統計資料的詳細資訊，請參閱 [檢閱用量和預估成本](#)。

## 步驟 4：設定儲存設定和彙總區域（選用）

您可以指定您希望 Security Lake 存放資料的 Amazon S3 儲存類別，以及存放資料的時間長度。您也可以指定彙總區域來合併來自多個區域的資料。這些是選用步驟。如需詳細資訊，請參閱 [Security Lake 中的生命週期管理](#)。

若要在啟用 Security Lake 時以程式設計方式定義目標目標，請使用 Security Lake API [CreateDataLake](#) 的操作。如果您已啟用 Security Lake 並想要定義目標目標，請使用 [UpdateDataLake](#) 操作，而非 CreateDataLake 操作。

對於任一操作，請使用支援的參數來指定您想要的組態設定：

- 若要指定彙總區域，請使用 region 欄位來指定您要將資料貢獻至彙總區域的區域。在 replicationConfiguration 物件 regions 陣列中，指定每個彙總區域的區域代碼。如需區域代碼清單，請參閱《》中的 [Amazon Security Lake 端點AWS 一般參考](#)。
- 若要指定資料的保留設定，請使用 lifecycleConfiguration 參數：
  - 針對 transitions，指定您要在特定 Amazon S3 儲存類別 (days) 中存放 S3 物件的總天數 (storageClass)。Amazon S3
  - 針對 expiration，指定建立物件後，使用任何儲存類別，在 Amazon S3 中儲存物件的總天數。當此保留期結束時，物件會過期，Amazon S3 會將其刪除。

Security Lake 會將指定的保留設定套用至您在 configurations 物件的 region 欄位中指定的區域。

例如，下列命令會使用 建立資料湖 ap-northeast-2 做為彙總區域。us-east-1 區域會將資料貢獻至 ap-northeast-2 區域。此範例也會為新增至資料湖的物件建立 10 天的過期期間。

```
$ 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"
```

您現在已建立您的資料湖。使用 Security Lake API [ListDataLakes](#) 的操作來驗證在每個區域中啟用 Security Lake 和您的資料湖設定。

如果在建立資料湖時發生問題或錯誤，您可以使用 [ListDataLakeExceptions](#) 操作來檢視例外狀況清單，並通知使用者 [CreateDataLakeExceptionSubscription](#) 操作的例外狀況。如需詳細資訊，請參閱 [對資料湖狀態進行故障診斷](#)。

## 步驟 5：檢視和查詢您自己的資料

建立資料湖後，您可以使用 Amazon Athena 或類似服務來檢視和查詢 AWS Lake Formation 資料庫和資料表中的資料。當您以程式設計方式啟用 Security Lake 時，不會自動授予資料庫檢視許可。中的資料湖管理員帳戶 AWS Lake Formation 必須將SELECT許可授予您要用來查詢相關資料庫和資料表的 IAM 角色。角色至少必須具有資料分析師許可。如需許可層級的詳細資訊，請參閱 [Lake Formation 角色和 IAM 許可參考](#)。如需授予SELECT許可的指示，請參閱《AWS Lake Formation 開發人員指南》中的[使用具名資源方法授予資料目錄許可](#)。

## 步驟 6：建立訂閱者

建立您的資料湖之後，您可以新增訂閱者以取用您的資料。訂閱者可以透過直接存取 Amazon S3 儲存貯體中的物件或查詢資料湖來取用資料。如需訂閱者的詳細資訊，請參閱 [Security Lake 中的訂閱者管理](#)。

# 在 Security Lake AWS Organizations 中使用 管理多個帳戶

您可以使用 Amazon Security Lake 從多個 收集安全日誌和事件 AWS 帳戶。為了協助自動化和簡化多個帳戶的管理，強烈建議您將 Security Lake 與 整合 [AWS Organizations](#)。

在 Organizations 中，您用來建立組織的帳戶稱為管理帳戶。若要將 Security Lake 與 Organizations 整合，管理帳戶必須為組織指定委派的 Security Lake 管理員帳戶。

委派的 Security Lake 管理員可以啟用 Security Lake 並為成員帳戶設定 Security Lake 設定。委派管理員可以在啟用 AWS 區域 Security Lake 的所有（無論他們目前正在使用哪個區域端點）中收集整個組織的日誌和事件。委派管理員也可以設定 Security Lake 自動收集新組織帳戶的日誌和事件資料。

委派的 Security Lake 管理員可以存取相關聯成員帳戶的日誌和事件資料。因此，他們可以設定 Security Lake 來收集關聯成員帳戶擁有的資料。他們也可以授予訂閱者使用相關聯成員帳戶所擁有資料的許可。

若要為組織中的多個帳戶啟用 Security Lake，組織管理帳戶必須先為組織指定委派的 Security Lake 管理員帳戶。委派管理員接著可以為組織啟用和設定 Security Lake。

## Important

使用 Security Lake 的 [RegisterDataLakeDelegatedAdministrator](#) API 來允許 Security Lake 存取您的組織並註冊 Organizations 的委派管理員。

如果您使用 Organizations 的 APIs 註冊委派管理員，可能不會成功建立 Organizations 的服務連結角色。若要確保完整功能，請使用 Security Lake APIs。

如需有關設定 Organizations 的資訊，請參閱 AWS Organizations 《使用者指南》中的 [建立和管理組織](#)。

## 對於現有的 Security Lake 帳戶

如果您在 2025 年 4 月 17 日之前啟用 Security Lake，我們建議您啟用 [資源管理的服務連結角色 \(SLR\) 許可](#)。透過使用此 SLR，您可以繼續執行持續的監控和效能改進，這可能會降低延遲和成本。如需與此 SLR 相關聯許可的資訊，請參閱 [資源管理的服務連結角色 \(SLR\) 許可](#)。

如果您使用 Security Lake 主控台，您將會收到通知，提示您啟用

`AWSServiceRoleForSecurityLakeResourceManagement`。如果您使用 AWS CLI，請參閱 [建立 Security Lake 服務連結角色](#)。

## 委派 Security Lake 管理員的重要考量事項

請記下下列因素，這些因素會定義委派管理員在 Security Lake 中的行為：

委派管理員在所有區域中都相同。

當您建立委派管理員時，它會成為您啟用 Security Lake 的每個區域的委派管理員。

我們建議將 Log Archive 帳戶設定為 Security Lake 委派管理員。

Log Archive 帳戶是 AWS 帳戶，專門用於擷取和封存所有與安全相關的日誌。此帳戶的存取權通常僅限於少數使用者，例如稽核人員和安全團隊，以進行合規調查。我們建議您將 Log Archive 帳戶設定為 Security Lake 委派管理員，以便以最少的內容切換來檢視與安全相關的日誌和事件。

此外，我們建議只有最少的使用者才能直接存取 Log Archive 帳戶。在此選取群組之外，如果使用者需要存取 Security Lake 收集的資料，您可以將他們新增為 Security Lake 訂閱者。如需新增訂閱者的資訊，請參閱 [Security Lake 中的訂閱者管理](#)。

如果您不使用 AWS Control Tower 服務，則可能沒有 Log Archive 帳戶。如需 Log Archive 帳戶的詳細資訊，請參閱 [安全參考架構中的 Security OU – Log Archive 帳戶](#)。AWS

組織只能有一個委派管理員。

每個組織只能有一個委派的 Security Lake 管理員。

組織管理帳戶不能是委派管理員。

根據 AWS 安全最佳實務和最低權限原則，您的組織管理帳戶不能是委派管理員。

委派管理員必須是作用中組織的一部分。

當您刪除組織時，委派的管理員帳戶無法再管理 Security Lake。您必須指定來自不同組織的委派管理員，或使用 Security Lake 搭配不屬於組織的獨立帳戶。

## 指定委派管理員所需的 IAM 許可

指定委派的 Security Lake 管理員時，您必須具有啟用 Security Lake 的許可，並使用下列政策陳述式中列出的特定 AWS Organizations API 操作。

您可以將下列陳述式新增至 AWS Identity and Access Management (IAM) 政策的結尾，以授予這些許可。

```
{
```

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

## 指定委派的 Security Lake 管理員並新增成員帳戶

選擇您的存取方法，為您的組織指定委派的 Security Lake 管理員帳戶。只有組織管理帳戶可以為其組織指定委派管理員帳戶。組織管理帳戶不能是其組織的委派管理員帳戶。

### Note

- 組織管理帳戶應使用 Security Lake RegisterDataLakeDelegatedAdministrator 操作來指定委派的 Security Lake 管理員帳戶。不支援透過 Organizations 指定委派的 Security Lake 管理員。
- 如果您想要變更組織的委派管理員，您必須先 [移除目前的委派管理員](#)。然後，您可以指定新的委派管理員。

### Console

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。  
使用組織的管理帳戶的登入資料登入。
2.
  - 如果尚未啟用 Security Lake，請選取開始使用，然後在啟用 Security Lake 頁面上指定委派的 Security Lake 管理員。
  - 如果已啟用 Security Lake，請在設定頁面上指定委派的 Security Lake 管理員。
3. 在將管理委派給另一個帳戶下，輸入 Log Archive 帳戶的 12 位數 AWS 帳戶 ID。

我們建議您使用 Log Archive 做為委派的 Security Lake 管理員。如需詳細資訊，請參閱[委派 Security Lake 管理員的重要考量事項](#)。

4. 選擇委派。如果尚未啟用 Security Lake，則指定委派管理員將在您目前的區域中為該帳戶啟用 Security Lake。

## API

若要以程式設計方式指定委派管理員，請使用 Security Lake API [RegisterDataLakeDelegatedAdministrator](#) 的操作。您必須從組織管理帳戶叫用操作。如果您使用的是 AWS CLI，請從組織管理帳戶執行 [register-data-lake-delegated-administrator](#) 命令。在您的請求中，使用 `accountId` 參數指定 AWS 帳戶，要指定為組織委派管理員帳戶的 12 位數帳戶 ID。

例如，下列 AWS CLI 命令會指定委派的管理員。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

委派管理員也可以選擇自動收集新組織帳戶的 AWS 日誌和事件資料。使用此組態，當帳戶新增至組織時，Security Lake 會在新帳戶中自動啟用 AWS Organizations。身為委派管理員，您可以使用 Security Lake API [CreateDataLakeOrganizationConfiguration](#) 的操作來啟用此組態，如果您使用的是 AWS CLI，則可執行 [create-data-lake-organization-configuration](#) 命令。您也可以指定新帳戶的特定組態設定。

例如，下列 AWS CLI 命令會自動在新的組織帳戶中啟用 Security Lake 和 Amazon Route 53 解析程式查詢日誌、AWS Security Hub 尋找和 Amazon Virtual Private Cloud (Amazon VPC) 流程日誌的集合。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

在組織管理帳戶指定委派管理員之後，管理員可以為組織啟用和設定 Security Lake。這包括啟用和設定 Security Lake 以收集組織中個別帳戶的 AWS 日誌和事件資料。如需詳細資訊，請參閱[在 Security Lake AWS 服務中從收集資料](#)。

您可以使用 [GetDataLakeOrganizationConfiguration](#) 操作來取得組織目前新成員帳戶組態的詳細資訊。

## 編輯新組織帳戶的自動啟用組態

委派的 Security Lake 管理員可以在帳戶加入您的組織時，檢視和編輯帳戶的自動啟用設定。Security Lake 僅根據新帳戶的這些設定擷取資料，而非現有帳戶。

使用下列步驟來編輯新組織帳戶的組態：

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。
2. 在導覽窗格中，選擇帳戶。
3. 在帳戶頁面上，展開新帳戶組態區段。您可以檢視從每個區域擷取哪些來源安全湖。
4. 選擇編輯以編輯此組態。
5. 在編輯新帳戶組態頁面上，執行下列步驟：
  - a. 針對選取區域，選取您要更新來源以擷取資料的一或多個區域。然後選擇下一步。
  - b. 針對選取來源，選擇下列其中一個來源選項：
    - i. 擷取預設 AWS 來源 – 當您選擇建議的選項時，CloudTrail - S3 資料事件，預設 AWS WAF 不會包含用於擷取。這是因為擷取大量這兩種來源類型可能會大幅影響使用成本。若要擷取這些來源，請先選取擷取特定 AWS 來源選項，然後從日誌和事件來源清單中選取這些來源。
    - ii. 擷取特定 AWS 來源 – 使用此選項，您可以選取要擷取的一或多個日誌和事件來源。
    - iii. 請勿擷取任何來源 – 當您不想從您在上一個步驟中選取的區域擷取任何來源時，請選取此選項。
    - iv. 選擇下一步。

### Note

當您第一次在帳戶中啟用 Security Lake 時，所有選取的日誌和事件來源都將是 15 天免費試用期的一部分。如需用量統計資料的詳細資訊，請參閱 [檢閱用量和預估成本](#)。

- c. 檢閱變更後，選擇套用。

當 AWS 帳戶 加入您的組織時，這些設定預設會套用到該帳戶。

## 移除委派的 Security Lake 管理員

只有組織管理帳戶可以移除其組織的委派 Security Lake 管理員。如果您想要變更組織的委派管理員，請移除目前的委派管理員，然後指定新的委派管理員。

### Important

移除委派的 Security Lake 管理員會刪除您的資料湖，並停用組織中帳戶的 Security Lake。

您無法使用 Security Lake 主控台變更或移除委派管理員。這些任務只能以程式設計方式執行。

若要以程式設計方式移除委派管理員，請使用 Security Lake API

[DeregisterDataLakeDelegatedAdministrator](#) 的操作。您必須從組織管理帳戶叫用操作。如使用 AWS CLI，請從組織管理帳戶執行 [deregister-data-lake-delegated-administrator](#) 命令。

例如，下列 AWS CLI 命令會移除委派的 Security Lake 管理員。

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

若要保留委派的管理員指定，但變更新成員帳戶的自動組態設定，請使用 Security Lake API

[DeleteDataLakeOrganizationConfiguration](#) 的操作，或者，如果您使用的是 AWS CLI [delete-data-lake-organization-configuration](#) 命令。只有委派管理員可以變更組織的這些設定。

例如，下列 AWS CLI 命令會停止從加入組織的新成員帳戶自動收集 Security Hub 問題清單。委派管理員調用此操作後，新成員帳戶不會將 Security Hub 調查結果貢獻至資料湖。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

## Security Lake 受信任存取

為組織設定 Security Lake 後，AWS Organizations 管理帳戶可以使用 Security Lake 啟用受信任存取。受信任存取可讓 Security Lake 建立 IAM 服務連結角色，並在您的組織及其帳戶中代表您執行任務。如需詳細資訊，請參閱 AWS Organizations 《使用者指南》中的 [將 AWS Organizations 與其他 AWS 服務 搭配使用](#)。

身為組織管理帳戶的使用者，您可以停用 Security Lake in 的受信任存取 AWS Organizations。如需停用受信任存取的指示，請參閱AWS Organizations 《使用者指南》中的[如何啟用或停用受信任存取](#)。

如果委派管理員的 AWS 帳戶 被暫停、隔離或關閉，我們建議您停用受信任的存取。

# 管理 Security Lake 中的區域

Amazon Security Lake 可以收集 AWS 區域 您啟用服務的安全日誌和事件。對於每個區域，您的資料會存放在不同的 Amazon S3 儲存貯體中。您可以為不同的區域指定不同的資料湖組態（例如，不同的來源和保留設定）。您也可以定義一或多個彙總區域，以合併來自多個區域的資料。

## 檢查區域狀態

Security Lake 可以跨多個 收集資料 AWS 區域。若要追蹤資料湖的狀態，了解每個區域的目前設定方式會很有幫助。選擇您偏好的存取方法，並依照下列步驟取得區域的目前狀態。

### Console

#### 檢查區域狀態

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 在導覽窗格中，選擇區域。區域頁面隨即出現，提供目前啟用 Security Lake 的區域概觀。
3. 選取區域，然後選擇編輯以查看該區域的詳細資訊。

### API

若要取得目前區域中日誌集合的狀態，請使用 Security Lake API [GetDataLakeSources](#) 的操作。如果您使用的是 AWS CLI，請執行 [get-data-lake-sources](#) 命令。針對 `accounts` 參數，指定一或多個 AWS 帳戶 IDs 做為清單。如果您的請求成功，Security Lake 會傳回目前區域中這些帳戶的快照，包括 Security Lake 正在從哪個 AWS 來源收集資料，以及每個來源的狀態。如果您未包含 `accounts` 參數，則回應會包含目前區域中設定 Security Lake 之所有帳戶的日誌收集狀態。

例如，下列 AWS CLI 命令會擷取目前區域中指定帳戶的日誌收集狀態。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

下列 AWS CLI 命令列出指定區域中所有帳戶和已啟用來源的日誌收集狀態。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securitylake get-data-lake-sources \  

```

```
--regions "us-east-1" \  
--query 'dataLakeSources[].[account,sourceName]'
```

若要判斷是否已為區域啟用 Security Lake，請使用 [ListDataLakes](#) 操作。如果您使用的是 AWS CLI，請執行 [list-data-lakes](#) 命令。針對 regions 參數，指定區域的區域代碼，例如美國東部（維吉尼亞北部）us-east-1 區域。如需區域代碼清單，請參閱 [Amazon Security Lake 端點AWS 一般參考](#)。ListDataLakes 操作會傳回您在請求中指定之每個區域的資料湖組態設定。如果您未指定區域，Security Lake 會傳回每個可用 Security Lake 區域中資料湖的狀態和組態設定。

例如，以下 AWS CLI 命令顯示 eu-central-1 區域中資料湖的狀態和組態設定。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

## 變更區域設定

選擇您偏好的方法，並遵循這些指示來更新一或多個資料湖中的設定 AWS 區域。

### Console

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。
2. 在導覽窗格中，選擇區域。
3. 選取區域，然後選擇編輯。
4. 選取 <Region> 中所有帳戶的覆寫來源核取方塊，以確認您在此處的選擇覆寫此區域的先前選擇。
5. 針對選取儲存類別，選擇新增轉換，為您的資料新增儲存類別。
6. 對於標籤，選擇性地指派或編輯區域的標籤。標籤是您可以定義和指派給特定類型 AWS 資源的標籤，包括 AWS 帳戶 特定區域中的資料湖組態。如需進一步了解，請參閱 [標記 Security Lake 資源](#)。
7. 若要將區域轉換為彙總區域，請在導覽窗格中選擇彙總區域（在設定下）。然後選擇 Modify（修改）。在選取彙總區域區段中，選擇新增彙總區域。選取貢獻區域，並向 Security Lake 提供跨多個區域複寫資料的許可。完成後，請選擇儲存以儲存變更。

## API

若要以程式設計方式更新資料湖的區域設定，請使用 Security Lake API [UpdateDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [update-data-lake](#) 命令。針對 region 參數，指定您要變更其設定之區域的區域代碼，例如美國東部（維吉尼亞北部）us-east-1 區域。如需區域代碼清單，請參閱 [Amazon Security Lake 端點](#) AWS 一般參考。

使用其他參數來指定您要變更的每個設定的新值，例如加密金鑰 (encryptionConfiguration) 和保留設定 (lifecycleConfiguration)。

例如，下列 AWS CLI 命令會更新 us-east-1 區域的資料過期和儲存類別轉換設定。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

## 在 Security Lake 中設定彙總區域

彙總區域會合併一或多個貢獻區域的資料。指定彙總區域可協助您符合區域合規要求。

由於 Amazon S3 的限制，不支援從客戶受管金鑰 (CMK) 加密區域資料湖複製到 S3 受管加密（預設加密）區域資料湖。

### Important

如果您建立了自訂來源，為了確保自訂來源資料正確複製至目的地，Security Lake 建議遵循 [擷取自訂來源的最佳實務中所述的最佳實務](#)。複製無法對未遵循 S3 分割區資料路徑格式的資料執行，如 頁面所述。

在新增彙總區域之前，您必須先在 AWS Identity and Access Management (IAM) 中建立兩個不同的角色：

- [資料複製的 IAM 角色](#)
- [用於註冊 AWS Glue 分割區的 IAM 角色](#)

**Note**

當您使用 Security Lake 主控台時，Security Lake 會建立這些 IAM 角色或代表您使用現有的角色。不過，在使用 Security Lake API 或 時，您必須建立這些角色 AWS CLI。

## 資料複寫的 IAM 角色

此 IAM 角色授予許可給 Amazon S3，以複寫跨多個區域的來源日誌和事件。

若要授予這些許可，請建立開頭為字首的 IAM 角色 SecurityLake，並將下列範例政策連接至角色。當您在 Security Lake 中建立彙總區域時，將需要角色的 Amazon Resource Name (ARN)。在此政策中，sourceRegions 正在貢獻區域，destinationRegions 是彙總區域。

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

```

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

```

將下列信任政策連接至您的角色，以允許 Amazon S3 擔任該角色：

```

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

```

如果您使用來自 AWS Key Management Service (AWS KMS) 的客戶受管金鑰來加密 Security Lake 資料湖，除了資料複寫政策中的許可之外，還必須授予下列許可。

```

{

```

```

    "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}"
    ]
  }
}

```

如需複寫角色的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[設定許可](#)。

## 用於註冊 AWS Glue 分割區的 IAM 角色

此 IAM 角色會授予 Security Lake 使用的分割區更新程式 AWS Lambda 函數的許可，以註冊從其他區域複製的 S3 物件的 AWS Glue 分割區。如果不建立此角色，訂閱者就無法從這些物件查詢事件。

若要授予這些許可，請建立名為 `AmazonSecurityLakeMetaStoreManager` (您可能已在加入 Security Lake 時建立此角色)。如需此角色的詳細資訊，包括範例政策，請參閱 [步驟 1：建立 IAM 角色](#)。

在 Lake Formation 主控台中，您還必須依照下列步驟，以資料湖管理員身分授予 `AmazonSecurityLakeMetaStoreManager` 許可：

1. 開啟 Lake Formation 主控台，網址為 <https://console.aws.amazon.com/lakeformation/>。
2. 以管理使用者身分登入。
3. 如果出現歡迎使用 Lake Formation 視窗，請選擇您在步驟 1 中建立或選取的使用者，然後選擇開始使用。
4. 如果您沒有看到歡迎使用 Lake Formation 視窗，請執行下列步驟來設定 Lake Formation 管理員。
  1. 在導覽窗格中的許可下，選擇管理角色和任務。在主控台頁面的資料湖管理員區段中，選擇選擇管理員。
  2. 在管理資料湖管理員對話方塊中，針對 IAM 使用者和角色，選擇您建立的 `AmazonSecurityLakeMetaStoreManager` IAM 角色，然後選擇儲存。

如需變更資料湖管理員許可的詳細資訊，請參閱《AWS Lake Formation 開發人員指南》中的 [建立資料湖管理員](#)。

## 新增彙總區域

選擇您偏好的存取方法，並依照下列步驟新增彙總區域。

### Note

區域可以將資料貢獻至多個彙總區域。不過，彙總區域不能是另一個彙總區域的貢獻區域。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。

2. 在導覽窗格中的設定下，選擇彙總區域。
3. 選擇修改，然後選擇新增彙總區域。
4. 指定彙總區域和貢獻區域。如果您想要新增多個彙總區域，請重複此步驟。
5. 如果這是您第一次新增彙總區域，對於服務存取，請建立新的 IAM 角色或使用現有 IAM 角色，授予 Security Lake 跨多個區域複寫資料的許可。
6. 完成後，請選擇儲存。

您也可以加入 Security Lake 時新增彙總區域。如需詳細資訊，請參閱[Amazon Security Lake 入門](#)。

## API

若要以程式設計方式新增彙總區域，請使用 Security Lake API [UpdateDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [update-data-lake](#) 命令。在請求中，使用 `region` 欄位指定您要將資料貢獻至彙總區域的區域。在 `replicationConfiguration` 參數 `regions` 陣列中，指定每個彙總區域的區域代碼。如需區域代碼清單，請參閱 [Amazon Security Lake 端點](#) AWS 一般參考。

例如，下列命令會 `ap-northeast-2` 設定為彙總區域。`us-east-1` 區域會將資料貢獻至 `ap-northeast-2` 區域。此範例也會為新增至資料湖的物件建立 365 天的過期期間。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

您也可以加入 Security Lake 時新增彙總區域。若要這樣做，請使用 [CreateDataLake](#) 操作（或者，如果使用 AWS CLI，則為 [create-data-lake](#) 命令）。如需在加入期間設定彙總區域的詳細資訊，請參閱[Amazon Security Lake 入門](#)。

## 更新或移除彙總區域

選擇您偏好的存取方法，並依照下列步驟更新或移除 Security Lake 中的彙總區域。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。

2. 在導覽窗格中的設定下，選擇彙總區域。
3. 選擇 Modify (修改)。
4. 若要變更彙總區域的貢獻區域，請在彙總區域的 列中指定更新的貢獻區域。
5. 若要移除彙總區域，請在彙總區域的資料列中選擇移除。
6. 完成後，請選擇儲存。

## API

若要以程式設計方式設定彙總區域，請使用 Security Lake API [UpdateDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [update-data-lake](#) 命令。在您的請求中，使用支援的參數來指定彙總設定：

- 若要新增貢獻區域，請使用 `region` 欄位指定要新增的區域的區域代碼。在 `replicationConfiguration` 物件 `regions` 陣列中，指定每個彙總區域的區域代碼，以貢獻資料。如需區域代碼清單，請參閱 [Amazon Security Lake 端點AWS 一般參考](#)。
- 若要移除貢獻區域，請使用 `region` 欄位來指定要移除區域的區域代碼。針對 `replicationConfiguration` 參數，請勿指定任何值。

例如，下列命令會將 `us-east-1` 和 `us-east-2` 設定為 `us-east-2` 貢獻區域。這兩個區域都會將資料貢獻至 `ap-northeast-3` 彙總區域。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

# Security Lake 中的來源管理

來源是從單一系統產生的日誌和事件，符合[Security Lake 中的開放式網路安全結構描述架構 \(OCSF\)](#)結構描述中的特定事件類別。Amazon Security Lake 可以從各種來源收集日誌和事件，包括原生支援 AWS 服務 和第三方自訂來源。

Security Lake 會在原始來源資料上執行擷取、轉換和載入 (ETL) 任務，並將資料轉換為 Apache Parquet 格式和 OCSF 結構描述。處理後，Security Lake 會將來源資料存放在 AWS 區域 產生資料的 AWS 帳戶 中的 Amazon Simple Storage Service (Amazon S3) 儲存貯體中。Security Lake 會為您啟用服務的每個區域建立不同的 Amazon S3 儲存貯體。每個來源都會在您的 S3 儲存貯體中取得個別的字首，而 Security Lake 會將來自每個來源的資料整理在一組不同的 AWS Lake Formation 資料表中。

## 主題

- [在 Security Lake AWS 服務 中從 收集資料](#)
- [從 Security Lake 中的自訂來源收集資料](#)

## 在 Security Lake AWS 服務 中從 收集資料

Amazon Security Lake 可以從下列原生支援的 收集日誌和事件 AWS 服務：

- AWS CloudTrail 管理和資料事件 (S3、Lambda)
- Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌
- Amazon Route 53 Resolver 查詢日誌
- AWS Security Hub 問題清單
- Amazon Virtual Private Cloud (Amazon VPC) 流程日誌
- AWS WAF v2 日誌

Security Lake 會自動將此資料轉換為 [Security Lake 中的開放式網路安全結構描述架構 \(OCSF\)](#) 和 Apache Parquet 格式。

### Tip

若要在 Security Lake 中新增一個或多個上述服務做為日誌來源，您不需要分別設定這些服務中的記錄，CloudTrail 管理事件除外。如果您在這些服務中已設定記錄，則不需要變更記錄組

態，即可在 Security Lake 中將其新增為日誌來源。Security Lake 透過獨立且重複的事件串流，直接從這些服務提取資料。

## 先決條件：驗證許可

若要在 Security Lake 中新增 AWS 服務 做為來源，您必須擁有必要的許可。確認連接至您用來新增來源之角色的 AWS Identity and Access Management (IAM) 政策具有執行下列動作的許可：

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

建議角色具有 和 S3:getObjects3:PutObject 許可的下列條件和資源範圍。

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

```
}
```

這些動作可讓您從 收集日誌和事件 AWS 服務 ，並將其傳送至正確的 AWS Glue 資料庫和資料表。

如果您使用 AWS KMS 金鑰進行資料湖的伺服器端加密，您也需要 的許可 `kms:DescribeKey`。

## 新增 AWS 服務 做為來源

將 新增 AWS 服務 做為來源後，Security Lake 會自動開始從中收集安全日誌和事件。這些指示說明如何在 Security Lake 中新增原生支援的 AWS 服務 來源。如需新增自訂來源的說明，請參閱 [從 Security Lake 中的自訂來源收集資料](#)。

### Console

#### 新增 AWS 日誌來源 ( 主控台 )

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 從導覽窗格中選擇來源。
3. 選取您要從中收集資料 AWS 服務的 ，然後選擇設定。
4. 在來源設定區段中，啟用來源，然後選取您要用於資料擷取的資料來源版本。根據預設，Security Lake 會擷取最新版本的資料來源。

#### Important

如果您沒有在指定區域中啟用新版本 AWS 日誌來源所需的角色許可，請聯絡您的 Security Lake 管理員。如需詳細資訊，請參閱 [更新角色許可](#)。

若要讓訂閱者擷取選取的資料來源版本，您也必須更新訂閱者設定。如需如何編輯訂閱者的詳細資訊，請參閱 [Amazon Security Lake 中的訂閱者管理](#)。

或者，您可以選擇僅擷取最新版本，並停用用於資料擷取的所有先前來源版本。

5. 在區域區段中，選取您要收集來源資料的區域。Security Lake 將從來源收集所選區域中所有帳戶的資料。
6. 選擇 啟用 。

### API

#### 新增 AWS 日誌來源 (API)

若要以程式設計方式新增 AWS 服務 做為來源，請使用 Security Lake API 的 [CreateAwsLogSource](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [create-aws-log-source](#) 命令。sourceName 和 regions 是必要參數。或者，您可以將來源的範圍限制為特定 accounts 或特定 sourceVersion。

#### Important

當您未在命令中提供參數時，Security Lake 會假設缺少的參數會參照整個集。例如，如果您不提供 accounts 參數，則命令會套用至組織中的整個帳戶集。

下列範例新增 VPC 流程日誌做為指定帳戶和區域中的來源。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

#### Note

如果您將此請求套用至您尚未啟用 Security Lake 的區域，您將會收到錯誤。您可以在該區域中啟用 Security Lake 來解決錯誤，或使用 regions 參數來指定您已啟用 Security Lake 的區域。

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

## 取得來源集合的狀態

選擇您的存取方法，並依照步驟取得目前區域中已啟用日誌收集的帳戶和來源快照。

### Console

取得目前區域中日誌集合的狀態

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。
2. 在導覽窗格中，選擇帳戶。
3. 將游標停留在來源欄中的數字上，以查看為所選帳戶啟用哪些日誌。

## API

若要取得目前區域中日誌集合的狀態，請使用 Security Lake API 的 [GetDataLakeSources](#) 操作。如果您使用的是 AWS CLI，請執行 `get-data-lake-sources` 命令。對於 `accounts` 參數，您可以將一或多個 AWS 帳戶 IDs 指定為清單。如果您的請求成功，Security Lake 會傳回目前區域中這些帳戶的快照，包括 Security Lake 正在從哪個 AWS 來源收集資料，以及每個來源的狀態。如果您未包含 `accounts` 參數，則回應會包含目前區域中設定 Security Lake 之所有帳戶的日誌收集狀態。

例如，下列 AWS CLI 命令會擷取目前區域中指定帳戶的日誌收集狀態。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

## 在 Security Lake 中更新角色許可

如果您沒有從新版本的資料來源擷取資料所需的角色許可或資源 — 新 AWS Lambda 函數和 Amazon Simple Queue Service (Amazon SQS) 佇列，您必須更新 AmazonSecurityLakeMetaStoreManagerV2 角色許可並建立新的資源集，以處理來自來源的資料。

選擇您偏好的方法，並依照指示更新您的角色許可，並建立新的資源，以處理指定區域中新版本的 AWS 日誌來源中的資料。這是一次性動作，因為許可和資源會自動套用至未來的資料來源版本。

### Console

#### 更新角色許可 (主控台)

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。  
使用委派 Security Lake 管理員的登入資料登入。
2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。
3. 選擇更新角色許可。
4. 在服務存取區段中，執行下列其中一項：
  - 建立和使用新的服務角色 — 您可以使用 Security Lake 建立的 AmazonSecurityLakeMetaStoreManagerV2 角色。
  - 使用現有的服務角色 — 您可以從服務角色名稱清單中選擇現有的服務角色。

## 5. 選擇套用。

### API

#### 更新角色許可 (API)

若要以程式設計方式更新許可，請使用 Security Lake API [UpdateDataLake](#) 的操作。若要使用更新許可 AWS CLI，請執行 [update-data-lake](#) 命令。

若要更新您的角色許可，您必須將 [AmazonSecurityLakeMetastoreManager](#) 政策連接至角色。

### 刪除 AmazonSecurityLakeMetaStoreManager 角色

#### Important

將角色許可更新為後 AmazonSecurityLakeMetaStoreManagerV2，請先確認資料湖正常運作，再移除舊 AmazonSecurityLakeMetaStoreManager 角色。建議在移除角色之前等待至少 4 小時。

如果您決定移除角色，您必須先從中刪除 AmazonSecurityLakeMetaStoreManager 角色 AWS Lake Formation。

請依照下列步驟，從 Lake Formation 主控台移除 AmazonSecurityLakeMetaStoreManager 角色。

1. 登入 AWS Management Console，然後開啟 Lake Formation 主控台，網址為 <https://console.aws.amazon.com/lakeformation/>。
2. 在 Lake Formation 主控台的導覽窗格中，選擇管理角色和任務。
3. AmazonSecurityLakeMetaStoreManager 從每個區域移除。

### 從 Security Lake 移除 AWS 服務 做為來源

選擇您的存取方法，並依照下列步驟移除原生支援的 AWS 服務 Security Lake 來源。您可以移除一或多個區域的來源。當您移除來源時，Security Lake 會停止從指定區域和帳戶中的來源收集資料，訂閱者無法再從來源取用新資料。不過，訂閱者仍然可以使用 Security Lake 在移除之前從來源收集的資料。您只能使用這些指示來移除原生支援的 AWS 服務 來源。如需移除自訂來源的相關資訊，請參閱 [從 Security Lake 中的自訂來源收集資料](#)。

## Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 從導覽窗格中選擇來源。
3. 選取來源，然後選擇停用。
4. 選取您要停止從此來源收集資料的區域。Security Lake 將停止從來源收集來自所選區域中所有帳戶的資料。

## API

若要以程式設計方式移除 AWS 服務 做為來源，請使用 Security Lake API 的 [DeleteAwsLogSource](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [delete-aws-log-source](#) 命令。sourceName 和 regions 是必要參數。或者，您可以將移除的範圍限制為特定 accounts 或特定 sourceVersion。

### Important

當您未在命令中提供參數時，Security Lake 會假設缺少的參數會參照整個集。例如，如果您不提供 accounts 參數，則命令會套用至組織中的整個帳戶集。

下列範例會移除 VPC 流程日誌，做為指定帳戶和區域中的來源。

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

下列範例會移除 Route 53 做為指定帳戶和區域中的來源。

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

上述範例已針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 換行字元來改善可讀性。

## Security Lake 中的 CloudTrail 事件日誌

AWS CloudTrail 提供您帳戶的 AWS API 呼叫歷史記錄，包括使用 AWS Management Console、AWS SDKs、命令列工具和特定 AWS 服務的 API 呼叫。CloudTrail 也可讓您識別哪些使用者和帳戶針對支援 CloudTrail 的服務稱為 AWS APIs、呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》<https://docs.aws.amazon.com/awsccloudtrail/latest/userguide/>。

Security Lake 可以收集與 S3 和 Lambda 的 CloudTrail 管理事件和 CloudTrail 資料事件相關聯的日誌。CloudTrail 管理事件、S3 資料事件和 Lambda 資料事件是 Security Lake 中的三個不同來源。因此，當您將其中一個值新增為擷取的日誌來源 [sourceName](#) 時，它們具有不同的值。管理事件也稱為控制平面事件，可讓您深入了解在資源上執行的管理操作 AWS 帳戶。CloudTrail 資料事件，也稱為資料平面操作，會顯示在您中資源上執行的資源操作 AWS 帳戶。這些操作通常是大量活動。

若要在 Security Lake 中收集 CloudTrail 管理事件，您必須至少有一個 CloudTrail 多區域組織線索，可收集讀取和寫入 CloudTrail 管理事件。必須針對追蹤啟用記錄。如果您在其他服務中已設定記錄，則不需要變更記錄組態，即可在 Security Lake 中將其新增為記錄來源。Security Lake 透過獨立且重複的事件串流，直接從這些服務提取資料。

多區域追蹤會將日誌檔案從多個區域交付到單一 Amazon Simple Storage Service (Amazon S3) 儲存貯體 AWS 帳戶。如果您已透過 CloudTrail 主控台或管理多區域追蹤 AWS Control Tower，則不需要進一步的動作。

- 如需有關透過 CloudTrail 建立和管理追蹤的資訊，請參閱 AWS CloudTrail 《使用者指南》中的 [為組織建立追蹤](#)。
- 如需有關透過建立和管理追蹤的資訊 AWS Control Tower，請參閱 AWS Control Tower 《使用者指南》中的 [使用記錄 AWS Control Tower 動作 AWS CloudTrail](#)。

當您新增 CloudTrail 事件做為來源時，Security Lake 會立即開始收集 CloudTrail 事件日誌。它透過獨立且重複的事件串流，直接從 CloudTrail 取用 CloudTrail 管理和資料事件。

Security Lake 不會管理您的 CloudTrail 事件，也不會影響現有的 CloudTrail 組態。若要直接管理 CloudTrail 事件的存取和保留，您必須使用 CloudTrail 服務主控台或 API。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南中的 [使用 CloudTrail 事件歷史記錄檢視事件](#)。

下列清單提供 GitHub 儲存庫連結，以連結至對應參考，了解 Security Lake 如何將 CloudTrail 事件標準化為 OCSF。

適用於 CloudTrail 事件的 GitHub OCSF 儲存庫

- 來源版本 1 ([v1.0.0-rc.2](#))

- 來源版本 2 ([1.1.0 版](#))

## Security Lake 中的 Amazon EKS 稽核日誌

當您新增 Amazon EKS 稽核日誌做為來源時，Security Lake 會開始收集在 Elastic Kubernetes Service (EKS) 叢集中執行之 Kubernetes 資源上執行活動的深入資訊。EKS 稽核日誌可協助您在 Amazon Elastic Kubernetes Service 中偵測 EKS 叢集中潛在的可疑活動。

Security Lake 透過獨立且重複的稽核日誌串流，直接從 Amazon EKS 控制平面記錄功能取用 EKS 稽核日誌事件。此程序的設計不需要額外的設定，也不會影響現有的 Amazon EKS 控制平面記錄組態。如需詳細資訊，請參閱 [《Amazon EKS 使用者指南》中的 Amazon EKS 控制平面記錄](#)。

Amazon EKS 稽核日誌僅支援 OCSF 1.1.0 版。如需有關 Security Lake 如何將 EKS 稽核日誌事件標準化為 OCSF 的資訊，請參閱 [GitHub OCSF 儲存庫中的對應參考](#)，其中適用於 Amazon EKS 稽核日誌事件 (1.1.0 版)。

## Security Lake 中的 Route 53 解析程式查詢日誌

Route 53 解析程式查詢日誌會追蹤 Amazon Virtual Private Cloud (Amazon VPC) 內資源所做的 DNS 查詢。這可協助您了解應用程式的運作方式，並找出安全威脅。

當您在 Security Lake 中新增 Route 53 解析程式查詢日誌做為來源時，Security Lake 會立即開始透過獨立且重複的事件串流，直接從 Route 53 收集您的解析程式查詢日誌。

Security Lake 不會管理您的 Route 53 日誌，也不會影響現有的解析程式查詢記錄組態。若要管理解析程式查詢日誌，您必須使用 Route 53 服務主控台。如需詳細資訊，請參閱 [《Amazon Route 53 開發人員指南》中的管理解析程式查詢記錄組態](#)。

下列清單提供 GitHub 儲存庫連結，以連結至對應參考，了解 Security Lake 如何將 Route 53 日誌標準化為 OCSF。

Route 53 日誌的 GitHub OCSF 儲存庫

- 來源版本 1 ([v1.0.0-rc.2](#))
- 來源版本 2 ([1.1.0 版](#))

## Security Lake 中的 Security Hub 調查結果

Security Hub 調查結果可協助您了解 中的安全狀態，AWS 並可讓您根據安全產業標準和最佳實務來檢查環境。Security Hub 從各種來源收集調查結果，包括與其他 AWS 服務第三方產品整合的整合，以

及針對 Security Hub 控制項的檢查。Security Hub 會以稱為 AWS Security Finding Format (ASFF) 的標準格式處理問題清單。

當您在 Security Lake 中新增 Security Hub 調查結果做為來源時，Security Lake 會立即開始透過獨立且重複的事件串流，直接從 Security Hub 收集調查結果。Security Lake 也會將調查結果從 ASFF 轉換為 [Security Lake 中的開放式網路安全結構描述架構 \(OCSF\)](#)(OCSF)。

Security Lake 不會管理您的 Security Hub 調查結果，也不會影響 Security Hub 設定。若要管理 Security Hub 調查結果，您必須使用 Security Hub 服務主控台、API 或 AWS CLI。如需詳細資訊，請參閱AWS Security Hub 《使用者指南》中的[調查結果 AWS Security Hub](#)。

下列清單提供 GitHub 儲存庫連結，以連結至對應參考，了解 Security Lake 如何將 Security Hub 調查結果標準化為 OCSF。

Security Hub 調查結果的 GitHub OCSF 儲存庫

- 來源版本 1 ([v1.0.0-rc.2](#))
- 來源版本 2 ([1.1.0 版](#))

## Security Lake 中的 VPC 流程日誌

Amazon VPC 的 VPC 流程日誌功能會擷取往返您環境中網路介面的 IP 流量相關資訊。

當您在 Security Lake 中新增 VPC 流程日誌做為來源時，Security Lake 會立即開始收集 VPC 流程日誌。它透過獨立且重複的流量日誌串流，直接從 Amazon VPC 使用 VPC 流量日誌。

Security Lake 不會管理您的 VPC 流程日誌或影響您的 Amazon VPC 組態。若要管理您的流程日誌，您必須使用 Amazon VPC 服務主控台。如需詳細資訊，請參閱《Amazon VPC 開發人員指南》中的[使用流程日誌](#)。

下列清單提供 GitHub 儲存庫連結，以連結至對應參考，了解 Security Lake 如何將 VPC 流程日誌標準化為 OCSF。

VPC 流程日誌的 GitHub OCSF 儲存庫

- 來源版本 1 ([v1.0.0-rc.2](#))
- 來源版本 2 ([1.1.0 版](#))

## AWS WAF Security Lake 中的日誌

當您在 Security Lake 中新增 AWS WAF 做為日誌來源時，Security Lake 會立即開始收集日誌。AWS WAF 是 Web 應用程式防火牆，可用來監控最終使用者傳送到您應用程式的 Web 請求，以及控制對內容的存取。記錄的資訊包括從您的 AWS 資源 AWS WAF 接收 Web 請求的時間、請求的詳細資訊，以及請求相符規則的詳細資訊。

Security Lake AWS WAF 透過獨立且重複的 AWS WAF 日誌串流，直接從取用日誌。此程序設計為不需要額外的設定或影響現有的 AWS WAF 組態。Security Lake 日誌只會擷取 [Web 存取控制清單 \(Web ACL\)](#) 組態允許 AWS WAF 的資料。如果在 Security Lake 帳戶中為 Web ACL 啟用 [資料保護](#)，產生的資料將根據您的 Web ACL 設定進行修訂或雜湊處理。如需有關使用 AWS WAF 來保護應用程式資源的資訊，請參閱《AWS WAF 開發人員指南》中的 [如何 AWS WAF 運作](#)。

### Important

如果您使用 Amazon CloudFront 分佈做為中的資源類型 AWS WAF，則必須選取美國東部（維吉尼亞北部）以擷取 Security Lake 中的全域日誌。

AWS WAF 日誌僅在 OCSF v1.1.0 中受支援。如需有關 Security Lake 如何將 AWS WAF 日誌事件標準化為 OCSF 的資訊，請參閱 [GitHub OCSF AWS WAF 日誌儲存庫中的映射參考 \(1.1.0 版\)](#)。

## 移除 AWS 服務 做為來源

選擇您的存取方法，並依照下列步驟移除原生支援的 AWS 服務 Security Lake 來源。您可以移除一或多個區域的來源。當您移除來源時，Security Lake 會停止從指定區域和帳戶中的來源收集資料，訂閱者無法再從來源取用新資料。不過，訂閱者仍然可以使用 Security Lake 在移除之前從來源收集的資料。您只能使用這些指示來移除原生支援的 AWS 服務 來源。如需移除自訂來源的相關資訊，請參閱 [從 Security Lake 中的自訂來源收集資料](#)。

### Console

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。
2. 從導覽窗格中選擇來源。
3. 選取來源，然後選擇停用。
4. 選取您要停止從此來源收集資料的區域。Security Lake 將停止從來源收集來自所選區域中所有帳戶的資料。

## API

若要以程式設計方式移除 AWS 服務 做為來源，請使用 Security Lake API 的 [DeleteAwsLogSource](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [delete-aws-log-source](#) 命令。sourceName 和 regions 是必要參數。或者，您可以將移除的範圍限制為特定 accounts 或特定 sourceVersion。

### Important

當您未在命令中提供參數時，Security Lake 會假設缺少的參數會參照整個集。例如，如果您不提供 accounts 參數，則命令會套用至組織中的整個帳戶集。

下列範例會移除 VPC 流程日誌，做為指定帳戶和區域中的來源。

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

下列範例會移除 Route 53 做為指定帳戶和區域中的來源。

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

上述範例已針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 換行字元來改善可讀性。

## 從 Security Lake 中的自訂來源收集資料

Amazon Security Lake 可以從第三方自訂來源收集日誌和事件。Security Lake 自訂來源是一種第三方服務，可將安全日誌和事件傳送至 Amazon Security Lake。傳送資料之前，自訂來源必須將日誌和事件轉換為開放網路安全結構描述架構 (OCSF)，並符合 Security Lake 的來源需求，包括分割區、parquet 檔案格式和物件大小和速率需求。

針對每個自訂來源，Security Lake 會處理下列項目：

- 為 Amazon S3 儲存貯體中的來源提供唯一的字首。

- 在 AWS Identity and Access Management (IAM) 中建立角色，允許自訂來源將資料寫入資料湖。此角色的許可界限是由名為 [AWS 受管政策](#) 所設定 [AmazonSecurityLakePermissionsBoundary](#)。
- 建立 AWS Lake Formation 資料表來組織來源寫入 Security Lake 的物件。
- 設定 AWS Glue 爬蟲程式來分割來源資料。爬蟲程式 AWS Glue Data Catalog 會將資料表填入。它也會自動探索新的來源資料並擷取結構描述定義。

#### Note

您最多可以在 帳戶中新增 50 個自訂日誌來源。

若要將自訂來源新增至 Security Lake，必須符合下列要求。未能滿足這些要求可能會影響效能，並可能影響 分析使用案例，例如查詢。

- 目的地 – 自訂來源必須能夠將資料寫入 Security Lake，做為指派給來源的字首下方的一組 S3 物件。對於包含多個資料類別的來源，您應該將每個唯一的 [開放網路安全結構描述架構 \(OCSF\) 事件類別](#) 交付為單獨的來源。Security Lake 會建立 IAM 角色，允許自訂來源寫入 S3 儲存貯體中的指定位置。
- 格式 – 從自訂來源收集的每個 S3 物件都應格式化為 Apache Parquet 檔案。
- 結構描述 – 相同的 OCSF 事件類別應套用至 Parquet 格式物件中的每個記錄。Security Lake 支援 Parquet 1.x 和 2.x 版。資料頁面大小應限制為 1 MB（未壓縮）。資料列群組大小不應大於 256 MB（壓縮）。對於 Parquet 物件內的壓縮，建議使用 zstandard。
- 分割 – 物件必須依區域、AWS 帳戶、eventDay 進行分割。物件應以為字首 `source location/region=region/accountId=accountID/eventDay=yyyyMMdd/`。
- 物件大小和速率 – 傳送至 Security Lake 的檔案應遞增，介於 5 分鐘到 1 個事件日之間。如果檔案的大小超過 256MB 分鐘。物件和大小需求是最佳化 Security Lake for Query Performance。未遵循自訂來源要求可能會影響 Security Lake 效能。
- 排序 – 在每個 Parquet 格式物件中，記錄應按時間排序，以減少查詢資料的成本。

#### Note

使用 [OCSF 驗證工具](#) 來驗證自訂來源是否與 相容 OCSF Schema。對於自訂來源，Security Lake 支援 OCSF 1.3 版和更早版本。

## 在 Security Lake 中擷取自訂來源的分割區需求

為了促進高效率的資料處理和查詢，在將自訂來源新增至 Security Lake 時，我們需要符合分割和物件和大小要求：

### 分割

物件應依來源位置 AWS 區域、AWS 帳戶、和日期進行分割。

- 分割區資料路徑的格式為

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

具有範例儲存貯體名稱的範例分割區為 `aws-security-data-lake-us-west-2-lake-uid/ext/custom-source-name/region=us-west-2/accountId=123456789012/eventDay=20230428/`。

下列清單說明 S3 路徑分割區中使用的參數：

- Security Lake 存放自訂來源資料的 Amazon S3 儲存貯體名稱。
- `source-location` – S3 儲存貯體中自訂來源的字首。Security Lake 會將指定來源的所有 S3 物件存放在此字首下，而該字首對於指定來源是唯一的。
- `region` – 資料上傳 AWS 區域 到其中。例如，您必須使用 US East (N. Virginia) 將資料上傳至美國東部（維吉尼亞北部）區域的 Security Lake 儲存貯體。
- `accountId` – 來源分割區中的記錄所相關的 AWS 帳戶 ID。對於與 外部帳戶相關的記錄 AWS，我們建議您使用字串，例如 `external` 或 `external_externalAccountId`。透過採用此命名對流，您可以避免在命名外部帳戶 IDs 時模稜兩可，以免與其他身分管理系統維護 AWS 的帳戶 IDs 或外部帳戶 IDs 衝突。
- `eventDay` – 記錄的 UTC 時間戳記，截斷為小時，格式為八個字元字串 (YYYYMMDD)。如果記錄在事件時間戳記中指定不同的時區，您必須將此分割區金鑰的時間戳記轉換為 UTC。

## 在 Security Lake 中新增自訂來源的先決條件

新增自訂來源時，Security Lake 會建立 IAM 角色，允許來源將資料寫入資料湖中的正確位置。角色的名稱遵循格式 `AmazonSecurityLake-Provider-{name of the custom source}-{region}`，其中 `region` 是 AWS 區域 您要新增自訂來源的。Security Lake 會將政策連接至允許存取資料湖的角色。如果您已使用客戶受管 AWS KMS 金鑰加密資料湖，Security Lake 也會將政策與

`kms:Decrypt`和 `kms:GenerateDataKey` 許可連接至角色。此角色的許可界限是由名為 `AWS` 受管政策所設定 [AmazonSecurityLakePermissionsBoundary](#)。

## 主題

- [驗證許可](#)
- [建立 IAM 角色以允許對 Security Lake 儲存貯體位置的寫入存取權 \(API AWS CLI和僅限步驟\)](#)

## 驗證許可

新增自訂來源之前，請確認您具有執行下列動作的許可。

若要驗證您的許可，請使用 IAM 來檢閱連接至 IAM 身分的 IAM 政策。然後，將這些政策中的資訊與下列必須允許您執行的動作清單進行比較，以新增自訂來源。

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

這些動作可讓您從自訂來源收集日誌和事件、將其傳送至正確的 AWS Glue 資料庫和資料表，並將它們存放在 Amazon S3 中。

如果您使用 AWS KMS 金鑰進行資料湖的伺服器端加密，您也需要 `kms:CreateGrant`、`kms:DescribeKey`和 `kms:GenerateDataKey`的許可。

**⚠ Important**

如果您計劃使用 Security Lake 主控台來新增自訂來源，您可以略過下一個步驟並繼續 [在 Security Lake 中新增自訂來源](#)。Security Lake 主控台提供簡化的入門程序，並建立所有必要的 IAM 角色，或代表您使用現有的角色。

如果您打算使用 Security Lake API AWS CLI 或新增自訂來源，請繼續下一個步驟以建立 IAM 角色，以允許對 Security Lake 儲存貯體位置進行寫入存取。

## 建立 IAM 角色以允許對 Security Lake 儲存貯體位置的寫入存取權 (API AWS CLI 和僅限步驟)

如果您使用 Security Lake API 或 AWS CLI 來新增自訂來源，請新增此 IAM 角色，以授予 AWS Glue 許可來擷取自訂來源資料，並識別資料中的分割區。這些分割區是組織資料以及在 Data Catalog 中建立和更新資料表的必要分割區。

建立此 IAM 角色之後，您需要角色的 Amazon Resource Name (ARN) 才能新增自訂來源。

您必須連接 `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS 受管政策。

若要授予必要的許可，您還必須在角色中建立和內嵌下列內嵌政策，AWS Glue 編目程式 以允許 從自訂來源讀取資料檔案，並在 AWS Glue Data Catalog 中建立/更新資料表。

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

連接下列信任政策，AWS 帳戶 以允許 使用 ，它可以根據外部 ID 擔任角色：

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

如果您新增自訂來源的區域中的 S3 儲存貯體使用客戶管理加密 AWS KMS key，您還必須將下列政策連接至角色和 KMS 金鑰政策：

```
{
  "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 中新增自訂來源

建立 IAM 角色以叫用 AWS Glue 爬蟲程式之後，請依照下列步驟在 Security Lake 中新增自訂來源。

## Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要建立自訂來源的區域。
3. 在導覽窗格中選擇自訂來源，然後選擇建立自訂來源。
4. 在自訂來源詳細資訊區段中，輸入自訂來源的全域唯一名稱。然後，選取描述自訂來源將傳送至 Security Lake 的資料類型的 OCSF 事件類別。
5. 對於 AWS 帳戶 具有寫入資料許可的，輸入將寫入日誌和事件到資料湖的自訂來源 AWS 帳戶的 ID 和外部 ID。
6. 對於服務存取，請建立並使用新的服務角色，或使用現有的服務角色，以授予 Security Lake 調用許可 AWS Glue。
7. 選擇 Create (建立)。

## API

若要以程式設計方式新增自訂來源，請使用 Security Lake API 的 [CreateCustomLogSource](#) 操作。在 AWS 區域 您要建立自訂來源的 中使用 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [create-custom-log-source](#) 命令。

在您的請求中，使用支援的參數來指定自訂來源的組態設定：

- `sourceName` – 指定來源的名稱。名稱必須是區域唯一值。
- `eventClasses` – 指定一或多個 OCSF 事件類別，描述來源將傳送至 Security Lake 的資料類型。如需 Security Lake 中支援做為來源的 OCSF 事件類別清單，請參閱 [開放式網路安全結構描述架構 \(OCSF\)](#)。
- `sourceVersion` – 或者，指定一個值，將日誌收集限制為自訂來源資料的特定版本。
- `crawlerConfiguration` – 指定您建立用來叫用爬蟲程式之 IAM 角色的 AWS Glue Amazon Resource Name (ARN)。如需建立 IAM 角色的詳細步驟，請參閱 [新增自訂來源的先決條件](#)
- `providerIdentity` – 指定來源將用來將日誌和事件寫入資料湖的 AWS 身分和外部 ID。

下列範例會在指定區域的指定日誌提供者帳戶中，將自訂來源新增為日誌來源。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ 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"]
```

## 在 中保持自訂來源資料更新 AWS Glue

在 Security Lake 中新增自訂來源後，Security Lake 會建立 AWS Glue 爬蟲程式。爬蟲程式會連接至您的自訂來源、決定資料結構，並使用資料表填入 AWS Glue Data Catalog。

我們建議手動執行爬蟲程式，讓您的自訂來源結構描述保持在最新狀態，並維護 Athena 和其他查詢服務的查詢功能。具體而言，如果自訂來源的輸入資料集發生下列任一變更，您應該執行爬蟲程式：

- 資料集有一或多個新的最上層資料欄。
- 資料集在具有 struct 資料類型的欄中有一或多個新欄位。

如需執行爬蟲程式的說明，請參閱《AWS Glue 開發人員指南》中的[排程 AWS Glue 爬蟲程式](#)。

Security Lake 無法刪除或更新您帳戶中現有的爬蟲程式。如果您刪除自訂來源，如果您計劃在未來建立具有相同名稱的自訂來源，建議您刪除相關聯的爬蟲程式。

## 支援的 OCSF 事件類別

Open Cybersecurity Schema Framework (OCSF) 事件類別說明自訂來源將傳送至 Security Lake 的資料類型。支援的事件類別清單如下：

```
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,  
REMIEDIATION_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  
}
```

## 從 Security Lake 刪除自訂來源

刪除自訂來源，以停止將資料從來源傳送至 Security Lake。當您移除來源時，Security Lake 會停止從指定區域和帳戶中的來源收集資料，訂閱者無法再從來源取用新資料。不過，訂閱者仍然可以使用 Security Lake 在移除之前從來源收集的資料。您只能使用這些指示來移除自訂來源。如需移除原生支援的資訊 AWS 服務，請參閱 [在 Security Lake AWS 服務 中從 收集資料](#)。

在 Security Lake 中刪除自訂來源時，您必須使用來源停用 Security Lake 主控台外部的每個來源。未停用整合可能會導致來源整合繼續將日誌傳送至 Amazon S3。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選取要從中移除自訂來源的區域。
3. 在導覽窗格中，選擇自訂來源。
4. 選取您要移除的自訂來源。
5. 選擇取消註冊自訂來源，然後選擇刪除以確認動作。

### API

若要以程式設計方式刪除自訂來源，請使用 Security Lake API 的 [DeleteCustomLogSource](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [delete-custom-log-source](#) 命令。使用 AWS 區域 您要刪除自訂來源的 中的 操作。

在您的請求中，使用 `sourceName` 參數來指定要刪除的自訂來源名稱。或指定自訂來源的名稱，並使用 `sourceVersion` 參數，將刪除的範圍限制為僅來自自訂來源的特定資料版本。

下列範例會從 Security Lake 刪除自訂日誌來源。

此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

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

# Security Lake 中的訂閱者管理

Amazon Security Lake 訂閱者會使用來自 Security Lake 的日誌和事件。為了控制成本並遵循最低權限存取最佳實務，您可以為每個來源提供訂閱者對資料的存取權。如需來源的詳細資訊，請參閱 [Security Lake 中的來源管理](#)。

Security Lake 支援兩種類型的訂閱者存取：

- 當資料寫入 S3 儲存貯體時，系統會通知具有 Amazon Security Lake 中來源資料之資料存取權的資料存取訂閱者來源的新物件。S3 根據預設，訂閱者會透過他們提供的 HTTPS 端點收到新物件的通知。或者，訂閱者可以透過輪詢 Amazon Simple Queue Service (Amazon SQS) 佇列，收到新物件的通知。
- 查詢存取 – 具有查詢存取的訂閱者可以查詢 Security Lake 收集的資料。這些訂閱者會使用 Amazon Athena 等服務，直接查詢 S3 儲存貯體中的 AWS Lake Formation 資料表。

訂閱者只能存取 AWS 區域您在建立訂閱者時選取的 中的來源資料。若要讓訂閱者存取來自多個區域的資料，您可以指定將訂閱者建立為彙總區域的區域，並讓其他區域為其貢獻資料。如需彙總區域和貢獻區域的詳細資訊，請參閱 [管理 Security Lake 中的區域](#)。

## Important

Security Lake 允許為每個訂閱者新增的來源數量上限為 10。這可能是 AWS 來源和自訂來源的組合。

## 主題

- [管理 Security Lake 訂閱者的資料存取](#)
- [管理 Security Lake 訂閱者的查詢存取權](#)

## 管理 Security Lake 訂閱者的資料存取

當資料寫入 S3 儲存貯體時，對 Amazon Security Lake 中來源資料具有資料存取權的訂閱者會收到來源新物件的通知。根據預設，訂閱者會透過他們提供的 HTTPS 端點收到新物件的通知。或者，訂閱者可以透過輪詢 Amazon Simple Queue Service (Amazon SQS) 佇列，收到新物件的通知。

當物件寫入 Security Lake 資料湖時，訂閱者會收到來源的新 Amazon S3 物件通知。訂閱者可以透過訂閱端點或輪詢 Amazon Simple Queue Service (Amazon SQS) 佇列，直接存取 S3 物件並接收新物件的通知。此訂閱類型在 [CreateSubscriber](#) API 的 `accessTypes` 參數中識別為 S3。

## 主題

- [在 Security Lake 中建立具有資料存取權的訂閱者的先決條件](#)
- [在 Security Lake 中建立具有資料存取權的訂閱者](#)
- [在 Security Lake 中更新資料訂閱者](#)
- [從 Security Lake 移除資料訂閱者](#)

## 在 Security Lake 中建立具有資料存取權的訂閱者的先決條件

您必須先完成下列先決條件，才能在 Security Lake 中建立具有資料存取權的訂閱者。

### 驗證許可

若要驗證您的許可，請使用 IAM 來檢閱連接至 IAM 身分的 IAM 政策。然後，將這些政策中的資訊與下列（許可）動作清單進行比較，您必須在將新資料寫入資料湖時通知訂閱者。

您需要許可才能執行下列動作：

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

除了上述清單之外，您也需要執行下列動作的許可：

- `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`

## 取得訂閱者的外部 ID

若要建立訂閱者，除了訂閱者的 AWS 帳戶 ID 之外，您也需要取得其外部 ID。外部 ID 是訂閱者提供給您的唯一識別符。Security Lake 會將外部 ID 新增至其建立的訂閱者 IAM 角色。當您在 Security Lake 主控台中、透過 API 或建立訂閱者時，您可以使用外部 ID AWS CLI。

如需外部 IDs 的詳細資訊，請參閱《IAM 使用者指南》中的 [如何在將 AWS 資源的存取權授予第三方時使用外部 ID](#)。

### Important

如果您計劃使用 Security Lake 主控台來新增訂閱者，您可以略過下一個步驟並繼續 [在 Security Lake 中建立具有資料存取權的訂閱者](#)。Security Lake 主控台提供簡化的入門程序，並建立所有必要的 IAM 角色，或代表您使用現有的角色。

如果您打算使用 Security Lake API AWS CLI 或新增訂閱者，請繼續下一個步驟來建立 IAM 角色以叫用 EventBridge API 目的地。

## 建立 IAM 角色以叫用 EventBridge API 目的地 (API AWS CLI和僅限步驟 )

如果您透過 API 或 使用 Security Lake AWS CLI，請在 AWS Identity and Access Management (IAM) 中建立角色，授予 Amazon EventBridge 呼叫 API 目的地的許可，並將物件通知傳送至正確的 HTTPS 端點。

建立此 IAM 角色之後，您需要角色的 Amazon Resource Name (ARN) 才能建立訂閱者。如果訂閱者從 Amazon Simple Queue Service (Amazon SQS) 佇列輪詢資料或直接從 查詢資料，則不需要此 IAM 角色 AWS Lake Formation。如需此類型資料存取方法（存取類型）的詳細資訊，請參閱[管理 Security Lake 訂閱者的查詢存取權](#)。

將下列政策連接至您的 IAM 角色：

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

將下列信任政策連接至您的 IAM 角色，以允許 EventBridge 擔任該角色：

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

```
}  
  ]  
}
```

Security Lake 會自動建立 IAM 角色，允許訂閱者從資料湖讀取資料（如果這是偏好的通知方法，則從 Amazon SQS 佇列輪詢事件）。此角色受到名為的 AWS 受管政策保護 [AmazonSecurityLakePermissionsBoundary](#)。

## 在 Security Lake 中建立具有資料存取權的訂閱者

選擇下列其中一種存取方法，以建立可存取目前中資料的訂閱者 AWS 區域。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要建立訂閱者的 區域。
3. 在導覽窗格中，選擇訂閱者。
4. 在訂閱者頁面上，選擇建立訂閱者。
5. 如需訂閱者詳細資訊，請輸入訂閱者名稱和選用的描述。

區域會自動填入為您目前選取的區域 AWS 區域，且無法修改。

6. 針對日誌和事件來源，選擇訂閱者有權使用的來源。
7. 針對資料存取方法，選擇 S3 為訂閱者設定資料存取。
8. 對於訂閱者憑證，請提供訂閱者的 AWS 帳戶 ID 和 [外部 ID](#)。
9. （選用）如需通知詳細資訊，如果您希望 Security Lake 建立訂閱者可以輪詢物件通知的 Amazon SQS 佇列，請選取 SQS 佇列。如果您希望 Security Lake 透過 EventBridge 將通知傳送至 HTTPS 端點，請選取訂閱端點。

如果您選取訂閱端點，也請執行下列動作：

- a. 輸入訂閱端點。有效端點格式的範例包括 <http://example.com>。您也可以選擇性地提供 HTTPS 金鑰名稱和 HTTPS 金鑰值。
- b. 針對服務存取，建立新的 IAM 角色或使用現有的 IAM 角色，提供 EventBridge 呼叫 API 目的地的許可，並將物件通知傳送至正確的端點。

如需建立新的 IAM 角色的資訊，請參閱 [建立 IAM 角色以叫用 EventBridge API 目的地](#)。

10. （選用）針對標籤，輸入最多 50 個標籤來指派給訂閱者。

標籤是您可以定義並指派給特定類型 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。標籤可協助您以不同的方式識別、分類和管理資源。如需進一步了解，請參閱 [標記 Security Lake 資源](#)。

## 11. 選擇 Create (建立)。

### API

若要以程式設計方式建立具有資料存取權的訂閱者，請使用 Security Lake API 的 [CreateSubscriber](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [create-subscriber](#) 命令。

在您的請求中，使用這些參數為訂閱者指定下列設定：

- 針對 `sources`，指定您希望訂閱者存取的每個來源。
- 針對 `subscriberIdentity`，指定訂閱者用來存取來源資料的 AWS 帳戶 ID 和外部 ID。
- 針對 `subscriber-name`，指定訂閱者的名稱。
- 對於 `accessTypes`，請指定 S3。

### 範例 1

下列範例會建立具有目前 AWS 區域中資料存取權的 AWS 訂閱者，以取得來源的指定訂閱者身分。

```
$ 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
```

### 範例 2

下列範例會建立可存取目前 AWS 區域中資料的訂閱者，以取得自訂來源的指定訂閱者身分。

```
$ 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
```

上述範例已針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 換行字元來改善可讀性。

(選用) 建立訂閱者之後，請使用 [CreateSubscriberNotification](#) 操作，指定如何在將新資料寫入資料湖時通知訂閱者，以取得您希望訂閱者存取的來源。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [create-subscriber-notification](#) 命令。

- 若要覆寫預設通知方法 (HTTPS 端點) 並建立 Amazon SQS 佇列，請指定 `sqsNotificationConfiguration` 參數的值。
- 如果您偏好使用 HTTPS 端點的通知，請指定 `httpsNotificationConfiguration` 參數的值。
- 針對 `targetRoleArn` 欄位，指定您建立用來叫用 EventBridge API 目的地之 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"}
```

若要取得 `subscriberID`，請使用 Security Lake API 的 [ListSubscribers](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [list-subscriber](#) 命令。

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

若要後續變更訂閱者的通知方法 (Amazon SQS 佇列或 HTTPS 端點)，請使用 [UpdateSubscriberNotification](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [update-subscriber-notification](#) 命令。您也可以使用 Security Lake 主控台變更通知方法：在訂閱者頁面上選取訂閱者，然後選擇編輯。

## 物件通知訊息範例

下列範例顯示 `CreateSubscriberNotification` 操作的 JSON 結構格式事件通知。

```
{
```

```
"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"
}
}
```

## 在 Security Lake 中更新資料訂閱者

您可以透過變更訂閱者使用的來源來更新訂閱者。您也可以為訂閱者指派或編輯標籤。標籤是您可以定義和指派給特定類型 AWS 資源的標籤，包括訂閱者。如需進一步了解，請參閱 [標記 Security Lake 資源](#)。

選擇其中一種存取方法，並依照下列步驟定義現有訂閱的新來源。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 在導覽窗格中，選擇訂閱者。
3. 選取訂閱者。
4. 選擇編輯，然後執行下列任一動作：
  - 若要更新訂閱者的來源，請在日誌和事件來源區段中輸入新設定。
  - 若要為訂閱者指派或編輯標籤，請在標籤區段中視需要變更標籤。
5. 完成後，請選擇儲存。

## API

若要以程式設計方式更新訂閱者的資料存取來源，請使用 Security Lake API 的 [UpdateSubscriber](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [update-subscriber](#) 命令。在您的請求中，使用 `sources` 參數來指定您希望訂閱者存取的每個來源。

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

如需與特定 AWS 帳戶 或組織相關聯的訂閱者清單，請使用 [ListSubscribers](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [list-subscribers](#) 命令。

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

若要檢閱特定訂閱者的目前設定，請使用 [GetSubscriber](#) 操作。執行 [get-subscriber](#) 命令。然後，Security Lake 會傳回訂閱者的名稱和描述、外部 ID 和其他資訊。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [get-subscriber](#) 命令。

若要更新訂閱者的通知方法，請使用 [UpdateSubscriberNotification](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [update-subscriber-notification](#) 命令。例如，您可以為訂閱者指定新的 HTTPS 端點，或從 HTTPS 端點切換到 Amazon SQS 佇列。

## 從 Security Lake 移除資料訂閱者

如果您不希望訂閱者從 Security Lake 取用資料，您可以依照下列步驟移除訂閱者。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 在導覽窗格中，選擇訂閱者。
3. 選取您要移除的訂閱者。
4. 選擇刪除，然後確認動作。這將刪除訂閱者和所有相關聯的通知設定。

### API

根據您的案例，執行下列其中一項：

- 若要刪除訂閱者和所有相關通知設定，請使用 Security Lake API 的 [DeleteSubscriber](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [delete-subscriber](#) 命令。

- 若要保留訂閱者，但停止未來通知訂閱者，請使用 Security Lake API 的 [DeleteSubscriberNotification](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [delete-subscriber-notification](#) 命令。

## 管理 Security Lake 訂閱者的查詢存取權

具有查詢存取權的訂閱者可以查詢 Security Lake 收集的資料。這些訂閱者會使用 Amazon Athena 等服務直接查詢 S3 儲存貯體中的 AWS Lake Formation 資料表。雖然 Security Lake 的主要查詢引擎是 Athena，但您也可以使用與整合的其他服務，例如 [Amazon Redshift Spectrum](#) 和 Spark SQL AWS Glue Data Catalog。

訂閱者會使用 Amazon Athena 等服務查詢 S3 儲存貯體中 AWS Lake Formation 資料表的來源資料。此訂閱類型在 [CreateSubscriber](#) API 的 `accessTypes` 參數 LAKEFORMATION 中識別為。

### Note

本節說明如何將查詢存取權授予第三方訂閱者。如需針對您自己的資料湖執行查詢的資訊，請參閱 [步驟 4：檢視和查詢您自己的資料](#)。

### 主題

- [在 Security Lake 中建立具有查詢存取權的訂閱者的先決條件](#)
- [在 Security Lake 中建立具有查詢存取權的訂閱者](#)
- [在 Security Lake 中編輯具有查詢存取權的訂閱者](#)

## 在 Security Lake 中建立具有查詢存取權的訂閱者的先決條件

您必須先完成下列先決條件，才能在 Security Lake 中建立具有資料存取權的訂閱者。

### 驗證許可

建立具有查詢存取權的訂閱者之前，請確認您具有執行下列動作清單的許可。

若要驗證您的許可，請使用 IAM 來檢閱連接至 IAM 身分的 IAM 政策。然後，將這些政策中的資訊與下列必須允許您執行的動作清單進行比較，以建立具有查詢存取權的訂閱者。

- `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

驗證許可之後：

- 如果您計劃使用 Security Lake 主控台新增具有查詢存取權的訂閱者，您可以略過下一個步驟並繼續 [授予 Lake Formation 管理員許可](#)。Security Lake 會建立所有必要的 IAM 角色，或代表您使用現有的角色。
- 如果您計劃使用 Security Lake API 或 CLI 來新增具有查詢存取權的訂閱者，請繼續下一個步驟，建立 IAM 角色來查詢 Security Lake 資料。

## 建立 IAM 角色以查詢 Security Lake 資料 (API AWS CLI和僅限步驟 )

使用 Security Lake API 或 AWS CLI 將查詢存取權授予訂閱者時，您需要建立名為的角色 `AmazonSecurityLakeMetaStoreManager`。Security Lake 使用此角色來註冊 AWS Glue 分割區和更新 AWS Glue 資料表。您可能已在建立 [必要的 IAM 角色時建立此角色](#)。

## 授予 Lake Formation 管理員許可

您也需要將 Lake Formation 管理員許可新增至您用來存取 Security Lake 主控台和新增訂閱者的 IAM 角色。

您可以依照下列步驟，將 Lake Formation 管理員許可授予您的角色：

1. 開啟 Lake Formation 主控台，網址為 <https://console.aws.amazon.com/lakeformation/>。
2. 以管理使用者身分登入。
3. 如果出現歡迎使用 Lake Formation 視窗，請選擇您在步驟 1 中建立或選取的使用者，然後選擇開始使用。
4. 如果您沒有看到歡迎使用 Lake Formation 視窗，請執行下列步驟來設定 Lake Formation 管理員。
  1. 在導覽窗格中的許可下，選擇管理角色和任務。在資料湖管理員區段中，選擇選擇管理員。
  2. 在管理資料湖管理員對話方塊中，針對 IAM 使用者和角色，選擇存取 Security Lake 主控台時使用的管理員角色，然後選擇儲存。

如需變更資料湖管理員許可的詳細資訊，請參閱《AWS Lake Formation 開發人員指南》中的[建立資料湖管理員](#)。

IAM 角色必須具有您要授予訂閱者存取權之資料庫和資料表 SELECT 的權限。如需如何執行此操作的說明，請參閱《AWS Lake Formation 開發人員指南》中的[使用具名資源方法授予資料目錄許可](#)。

## 在 Security Lake 中建立具有查詢存取權的訂閱者

選擇您偏好的方法，以建立目前具有查詢存取權的訂閱者 AWS 區域。訂閱者只能從 AWS 區域 建立資料的中查詢資料。若要建立訂閱者，您需要擁有訂閱者的 AWS 帳戶 ID 和外部 ID。外部 ID 是訂閱者提供給您的唯一識別符。如需外部 IDs 的詳細資訊，請參閱《IAM 使用者指南》中的[如何在將 AWS 資源的存取權授予第三方時使用外部 ID](#)。

### Note

Security Lake 不支援 Lake Formation 跨帳戶資料共用第 1 版。您必須將 Lake Formation 跨帳戶資料共用更新為第 2 版或第 3 版。如需透過 AWS Lake Formation 主控台或 CLI AWS 更新跨帳戶版本設定的步驟，請參閱《AWS Lake Formation 開發人員指南》中的[如何啟用新版本](#)。

### Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。  
登入委派的管理員帳戶。

2. 使用頁面右上角的 AWS 區域 選取器，選取您要建立訂閱者的 區域。
3. 在導覽窗格中，選擇訂閱者。
4. 在訂閱者頁面上，選擇建立訂閱者。
5. 如需訂閱者詳細資訊，請輸入訂閱者名稱和選用的描述。

區域會自動填入為您目前選取的區域 AWS 區域，且無法修改。

6. 針對日誌和事件來源，選擇您希望 Security Lake 在傳回查詢結果時包含的來源。
7. 針對資料存取方法，選擇 Lake Formation 為訂閱者建立查詢存取。
8. 對於訂閱者憑證，請提供訂閱者的 AWS 帳戶 ID 和 [外部 ID](#)。
9. (選用) 針對標籤，輸入最多 50 個標籤來指派給訂閱者。

標籤是您可以定義並指派給特定類型 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。標籤可協助您以不同的方式識別、分類和管理資源。如需進一步了解，請參閱 [標記 Security Lake 資源](#)。

10. 選擇 Create (建立)。

## API

若要以程式設計方式建立具有查詢存取權的訂閱者，請使用 Security Lake API 的 [CreateSubscriber](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [create-subscriber](#) 命令。

在您的請求中，使用這些參數為訂閱者指定下列設定：

- 對於 `accessTypes`，請指定 LAKEFORMATION。
- 針對 `sources`，指定您希望 Security Lake 在傳回查詢結果時包含的每個來源。
- 針對 `subscriberIdentity`，指定訂閱者用來查詢來源資料的 AWS 身分和外部 ID。

下列範例會建立具有目前 AWS 區域中指定訂閱者身分之查詢存取權的訂閱者。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ 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
```

## 設定跨帳戶資料表共用（訂閱者步驟）

Security Lake 使用 Lake Formation 跨帳戶資料表共用來支援訂閱者查詢存取。當您在 Security Lake 主控台、API 或中建立具有查詢存取權的訂閱者 AWS CLI 時，Security Lake 會透過在 AWS Resource Access Manager () 中建立 [資源共享](#)，與訂閱者共享有關相關 Lake Formation 資料表的資訊 AWS RAM。

當您對具有查詢存取權的訂閱者進行特定類型的編輯時，Security Lake 會建立新的資源共享。如需詳細資訊，請參閱 [在 Security Lake 中編輯具有查詢存取權的訂閱者](#)。

訂閱者應遵循下列步驟，以取用 Lake Formation 資料表中的資料：

1. 接受資源共享 – 訂閱者必須接受資源共享，而 resourceShareName 該資源共享具有在您建立或編輯訂閱者時所產生的 resourceShareArn 和 。選擇下列其中一種存取方法：
  - 如需主控台和 AWS CLI，請參閱 [接受來自的資源共用邀請 AWS RAM](#)。
  - 對於 API，請叫用 [GetResourceShareInvitations](#) API。依 resourceShareArn 和 篩選 resourceShareName，以尋找正確的資源共享。使用 [AcceptResourceShareInvitation](#) API 接受邀請。

資源共享邀請會在 12 小時內過期，因此您必須在 12 小時內驗證並接受邀請。如果邀請過期，您會繼續在 PENDING 狀態中看到，但接受邀請不會讓您存取共用資源。超過 12 小時後，請刪除 Lake Formation 訂閱者，並重新建立訂閱者以取得新的資源共享邀請。
2. 建立共用資料庫的資源連結 – 訂閱者必須在 AWS Lake Formation（如果使用主控台）或 AWS Glue（如果使用 API/AWS CLI）中建立共用 Lake Formation 資料庫的資源連結。此資源連結會將訂閱者的帳戶指向共用資料庫。選擇下列其中一種存取方法：
  - 如需主控台和 AWS CLI，請參閱《[開發人員指南](#)》中的 [建立共用 Data Catalog 資料庫的資源連結](#)。AWS Lake Formation
  - 我們建議訂閱者也使用 [CreateDatabase](#) API 建立唯一的資料庫，以存放資源連結資料表。
3. 查詢共用資料表 – Amazon Athena 之類的服務可以直接參考資料表，而且 Security Lake 收集的新資料會自動可供查詢。查詢會在訂閱者的中執行 AWS 帳戶，而查詢產生的成本會向訂閱者收費。您可以控制自己 Security Lake 帳戶中資源的讀取存取權。

如需授予跨帳戶許可的詳細資訊，請參閱《[AWS Lake Formation 開發人員指南](#)》中的 [Lake Formation 中的跨帳戶資料共用](#)。

## 在 Security Lake 中編輯具有查詢存取權的訂閱者

Security Lake 支援對具有查詢存取權的訂閱者進行編輯。您可以編輯訂閱者的名稱、描述、外部 ID、委託人 (AWS 帳戶 ID)，以及訂閱者能夠使用的日誌來源。選擇您偏好的方法，並依照步驟編輯目前具有查詢存取權的訂閱者 AWS 區域。

### Note

Security Lake 不支援 Lake Formation 跨帳戶資料共用第 1 版。您必須將 Lake Formation 跨帳戶資料共用更新為第 2 版或第 3 版。如需透過 AWS Lake Formation 主控台或 CLI AWS 更新跨帳戶版本設定的步驟，請參閱《AWS Lake Formation 開發人員指南》中的[如何啟用新版本](#)。

## Console

根據您要編輯的詳細資訊，僅遵循針對該動作提供的步驟。

### 編輯訂閱者名稱

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。  
登入委派的管理員帳戶。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要編輯訂閱者詳細資訊的區域。
3. 在導覽窗格中，選擇訂閱者。
4. 在訂閱者頁面上，使用選項按鈕選取要編輯的訂閱者。所選訂閱者的資料存取方法必須為 LAKEFORMATION。
5. 選擇編輯。
6. 輸入新的訂閱者名稱，然後選擇儲存。

### 編輯訂閱者描述

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。  
登入委派的管理員帳戶。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要編輯訂閱者的 區域。
3. 在導覽窗格中，選擇訂閱者。

4. 在訂閱者頁面上，使用選項按鈕選取要編輯的訂閱者。所選訂閱者的資料存取方法必須為 LAKEFORMATION。
5. 選擇編輯。
6. 輸入訂閱者的新描述，然後選擇儲存。

### 編輯外部 ID

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。  
登入委派的管理員帳戶。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要編輯訂閱者詳細資訊的區域。
3. 在導覽窗格中，選擇訂閱者。
4. 在訂閱者頁面上，使用選項按鈕選取要編輯的訂閱者。所選訂閱者的資料存取方法必須為 LAKEFORMATION。
5. 選擇編輯。
6. 輸入訂閱者提供的新外部 ID，然後選擇儲存。

儲存新的外部 ID 會自動移除先前的 AWS RAM 資源共享，並為訂閱者建立新的資源共享。

7. 訂閱者必須依照中的步驟 1 接受新的資源共享 [設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。請確定訂閱者詳細資訊中顯示的 Amazon Resource Name (ARN) 與 Lake Formation 主控台 中的 Amazon Resource Name (ARN) 相同。共用資料表的資源連結保持不變，因此訂閱者 不需要建立新的資源連結。

### 編輯主體 (AWS 帳戶 ID)

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。  
登入委派的管理員帳戶。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要編輯訂閱者詳細資訊的區域。
3. 在導覽窗格中，選擇訂閱者。
4. 在訂閱者頁面上，使用選項按鈕選取要編輯的訂閱者。所選訂閱者的資料存取方法必須為 LAKEFORMATION。
5. 選擇編輯。
6. 輸入訂閱者的新 AWS 帳戶 ID，然後選擇儲存。

儲存新帳戶 ID 會自動移除先前的 AWS RAM 資源共用，因此先前的主體無法使用日誌和事件來源。Security Lake 會建立新的資源共享。

7. 使用新主體的登入資料，訂閱者必須接受新的資源共用，並建立共用資料表的資源連結。這可讓新的主體存取共用資源。如需說明，請參閱 [中的步驟 1 和 2 設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。請確定訂閱者詳細資訊中顯示的 ARN 與 Lake Formation 主控台中的 ARN 相同。

## 編輯日誌和事件來源

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。  
登入委派的管理員帳戶。
2. 使用頁面右上角的 AWS 區域 選擇器，選取您要編輯訂閱者詳細資訊的區域。
3. 在導覽窗格中，選擇訂閱者。
4. 在訂閱者頁面上，使用選項按鈕選取要編輯的訂閱者。所選訂閱者的資料存取方法必須為 LAKEFORMATION。
5. 選擇編輯。
6. 取消選取現有的來源，或選取要新增的來源。如果您取消選取來源，則不需要再採取任何動作。如果您選擇新增來源，則不會建立新的資源共享邀請。不過，Security Lake 會根據新增的來源更新共用的 Lake Formation 資料表。訂閱者必須建立更新共用資料表的資源連結，才能查詢來源資料。如需說明，請參閱 [中的步驟 2 設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。
7. 選擇 Save (儲存)。

## API

若要以程式設計方式編輯具有查詢存取權的訂閱者，請使用 Security Lake API 的 [UpdateSubscriber](#) 操作。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [update-subscriber](#) 命令。在您的請求中，使用支援的參數為訂閱者指定下列設定：

- 針對 `subscriberName`，指定新的訂閱者名稱。
- 針對 `subscriberDescription`，指定新的描述。
- 針對 `subscriberIdentity`，指定訂閱者用來查詢來源資料的主體 (AWS 帳戶 ID) 和外部 ID。您必須同時提供委託人和外部 ID。如果您想要保持其中一個值相同，請傳遞目前的值。

- 僅更新外部 ID – 此動作會移除先前的 AWS RAM 資源共用，並為訂閱者建立新的資源共用。訂閱者必須依照中的步驟 1 接受新的資源共享[設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。共用資料表的資源連結保持不變，因此訂閱者不需要建立新的資源連結。
- 僅更新委託人 – 此動作會移除先前的 AWS RAM 資源共用，因此先前的委託人無法使用日誌和事件來源。Security Lake 會建立新的資源共享。使用新主體的登入資料，訂閱者必須接受新的資源共用，並建立共用資料表的資源連結。這可讓新的主體存取共用資源。如需說明，請參閱中的步驟 1 和 2[設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。

若要更新外部 ID 和主體，請遵循 中的步驟 1 和 2[設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。

- 針對 sources，移除現有的來源或指定您要新增的來源。如果您移除來源，則不需要進一步的動作。如果您新增來源，則不會建立新的資源共享邀請。不過，Security Lake 會根據新增的來源更新共用的 Lake Formation 資料表。訂閱者必須建立更新共用資料表的資源連結，才能查詢來源資料。如需說明，請參閱 中的步驟 2[設定跨帳戶資料表共用 \(訂閱者步驟\)](#)。

# Security Lake 查詢

您可以查詢 Security Lake 存放在 AWS Lake Formation 資料庫和資料表中的資料。您也可以直接在 Security Lake 主控台、API 或中建立第三方訂閱者 AWS CLI。第三方訂閱者也可以從您指定的來源查詢 Lake Formation 資料。

Lake Formation 資料湖管理員必須將相關資料庫和資料表的 SELECT 許可授予查詢資料的 IAM 身分。訂閱者也必須在 Security Lake 中建立，才能查詢資料。如需如何建立具有查詢存取權的訂閱者的詳細資訊，請參閱 [管理 Security Lake 訂閱者的查詢存取權](#)。

## 使用保留設定查詢資料

[Amazon S3 生命週期設定](#)會影響資料保留的時間，進而影響您可以查詢的時間。如果您在 Security Lake 中設定了保留設定，則必須在查詢中包含以時間為基礎的篩選條件，以確保結果集的範圍限定為尚未過期的資料檔案。如需 Security Lake 中資料保留的詳細資訊，請參閱 [生命週期管理](#)。

下列各節中的查詢範例包含時間型篩選條件，例如 eventDay 或 time\_dt，以示範此最佳實務。

## 主題

- [AWS 來源版本 1 \(OCSF 1.0.0-rc.2\) 的 Security Lake 查詢](#)
- [AWS 來源版本 2 \(OCSF 1.1.0\) 的 Security Lake 查詢](#)

## AWS 來源版本 1 (OCSF 1.0.0-rc.2) 的 Security Lake 查詢

下一節提供從 Security Lake 查詢資料的指引，並包含 AWS 一些來源版本 1 原生支援 AWS 來源的查詢範例。這些查詢旨在擷取特定中的資料 AWS 區域。這些範例使用 us-east-1（美國東部（維吉尼亞北部））。此外，範例查詢使用 LIMIT 25 參數，最多可傳回 25 筆記錄。您可以省略此參數，或根據您的偏好設定進行調整。如需更多範例，請參閱 [Amazon Security Lake OCSF 查詢 GitHub 目錄](#)。

下列查詢包含使用的時間型篩選條件 eventDay，以確保您的查詢位於設定的保留設定內。如需詳細資訊，請參閱 [Querying data with retention settings](#)。

例如，如果超過 60 天的資料已過期，您的查詢應包含時間限制，以防止存取過期的資料。對於 60 天的保留期，請在查詢中包含下列子句：

```
...  
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)
```

```
...
```

此子句使用 59 天（而不是 60 天），以避免 Amazon S3 和 Apache Iceberg 之間的任何資料或時間重疊。

## 日誌來源資料表

當您查詢 Security Lake 資料時，必須包含資料所在的 Lake Formation 資料表名稱。

```
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
```

日誌來源資料表的常見值包括下列項目：

- cloud\_trail\_mgmt\_1\_0 – AWS CloudTrail 管理事件
- lambda\_execution\_1\_0 – Lambda 的 CloudTrail 資料事件
- s3\_data\_1\_0 – S3 的 CloudTrail 資料事件
- route53\_1\_0 – Amazon Route 53 解析程式查詢日誌
- sh\_findings\_1\_0 – AWS Security Hub 尋找
- vpc\_flow\_1\_0 – Amazon Virtual Private Cloud (Amazon VPC) 流程日誌

範例：**sh\_findings\_1\_0**us-east-1 區域資料表中的所有 Security Hub 問題清單

```
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
```

## 資料庫區域

查詢 Security Lake 資料時，您必須包含要從中查詢資料的資料庫區域名稱。如需目前可使用 Security Lake 的資料庫區域完整清單，請參閱 [Amazon Security Lake 端點](#)。

範例：列出來源 IP AWS CloudTrail 的活動

下列範例列出來源 IP `192.0.2.1` 的所有 CloudTrail 活動，這些活動是在 `20230301` (2023 年 3 月 1 日) 之後記錄在 `us-east-1` 的資料表 `cloud_trail_mgmt_1_0` 中 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
```

## 分割區日期

透過分割資料，您可以限制每個查詢掃描的資料量，從而改善效能並降低成本。Security Lake 透過 `eventDay`、`region` 和 `accountid` 參數實作分割。`eventDay` 分割區使用格式 `YYYYMMDD`。

這是使用 `eventDay` 分割區的範例查詢：

```
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
```

的常見值 `eventDay` 包括下列項目：

## 過去 1 年發生的事件

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

## 過去 1 個月內發生的事件

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

## 過去 30 天內發生的事件

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

## 過去 12 小時內發生的事件

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

## 過去 5 分鐘內發生的事件

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

## 7-14 天前發生的事件

```
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)
```

## 在特定日期或之後發生的事件

```
>= '20230301'
```

範例：資料表中 **192.0.2.1** 2023 年 3 月 1 日或之後來源 IP 的所有 CloudTrail 活動清單

## **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_0
WHERE eventDay >= '20230301'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
```

```
LIMIT 25
```

範例：資料表 **192.0.2.1** 中過去 30 天內來自來源 IP 的所有 CloudTrail 活動清單

### 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_0
  WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
  AND src_endpoint.ip = '192.0.2.1'
  ORDER BY time desc
  LIMIT 25
```

## CloudTrail 資料的範例 Security Lake 查詢

AWS CloudTrail 會追蹤 中的使用者活動和 API 用量 AWS 服務。訂閱者可以查詢 CloudTrail 資料，以了解下列類型的資訊：

以下是 AWS 來源版本 1 CloudTrail 資料的一些查詢範例：

過去 7 天內對 AWS 服務 進行未經授權的嘗試

```
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_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 api.response.error in (
```

```

        'Client.UnauthorizedOperation',
        'Client.InvalidPermission.NotFound',
        'Client.OperationNotPermitted',
        'AccessDenied')
ORDER BY time desc
LIMIT 25

```

### 192.0.2.1 過去 7 天內來自來源 IP 的所有 CloudTrail 活動清單

```

SELECT
    api.request.uid,
    time,
    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_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

```

### 過去 7 天內所有 IAM 活動的清單

```

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

```

### 過去 7 天內 AIDACKCEVSQ6C2EXAMPLE 使用登入資料的執行個體

```

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
```

### 過去 7 天內失敗的 CloudTrail 記錄清單

```
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 解析程式查詢日誌的範例 Security Lake 查詢

Amazon Route 53 解析程式查詢日誌會追蹤 Amazon VPC 內資源所做的 DNS 查詢。訂閱者可以查詢 Route 53 解析程式查詢日誌，以了解下列類型的資訊：

以下是 AWS 來源版本 1 的 Route 53 解析程式查詢日誌的一些範例查詢：

### 過去 7 天內來自 CloudTrail 的 DNS 查詢清單

```
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
```

### s3.amazonaws.com 過去 7 天內相符的 DNS 查詢清單

```
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
```

### 過去 7 天內未解析的 DNS 查詢清單

```
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
```

## 過去 7 天內解析為 的 DNS 查詢清單 192.0.2.1

```

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 查詢 Security Hub 問題清單的範例

Security Hub 為您提供 中安全狀態的完整檢視，AWS 並協助您根據安全產業標準和最佳實務檢查環境。Security Hub 會產生安全檢查的問題清單，並接收第三方服務的問題清單。

以下是一些 Security Hub 問題清單的範例查詢：

### **MEDIUM**在過去 7 天內，嚴重性大於或等於 的新問題清單

```

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

```

### 過去 7 天內重複的問題清單

```

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

```

### 過去 7 天內的所有非資訊性問題清單

```

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

```

### 資源是 Amazon S3 儲存貯體的調查結果 ( 無時間限制 )

```

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

```

### 常見漏洞評分系統 (CVSS) 分數大於 1 ( 無時間限制 ) 的問題清單

```

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
```

符合常見漏洞與暴露 (CVE) 的調查結果 **CVE-0000-0000** (無時間限制)

```
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
```

過去 7 天內從 Security Hub 傳送問題清單的產品計數

```
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
```

過去 7 天內調查結果中的資源類型計數

```
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
```

來自過去 7 天內調查結果的易受攻擊套件

```
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

```

## 在過去 7 天內變更的問題清單

```

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 流程日誌的範例 Security Lake 查詢

Amazon Virtual Private Cloud (Amazon VPC) 提供往返 VPC 中網路介面之 IP 流量的詳細資訊。

以下是 AWS 來源版本 1 的 Amazon VPC 流程日誌的一些範例查詢：

### 過去 7 天內特定 AWS 區域 中的流量

```

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 region in ('us-east-1','us-east-2','us-west-2')
LIMIT 25

```

### 22 過去 7 天內來源 IP 192.0.2.1 和來源連接埠的活動清單

```
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
```

### 過去 7 天內不同目的地 IP 地址的計數

```
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
```

### 過去 7 天內源自 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
```

### 過去 7 天內的所有 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

```

#### 443過去 7 天內目的地為連接埠之連線的封包計數排序

```

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

```

#### 192.0.2.2過去 7 天內 IP 192.0.2.1與 之間的所有流量

```

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

```

### 過去 7 天內的所有傳入流量

```

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

```

### 過去 7 天內的所有傳出流量

```

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

```

### 過去 7 天內所有被拒絕的流量

```

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 來源版本 2 (OCSF 1.1.0) 的 Security Lake 查詢

下節提供從 Security Lake 查詢資料的指引，並包含 AWS 一些來源版本 2 原生支援 AWS 來源的查詢範例。這些查詢旨在擷取特定中的資料 AWS 區域。這些範例使用 us-east-1（美國東部（維吉尼亞北部））。此外，範例查詢使用 LIMIT 25 參數，最多可傳回 25 筆記錄。您可以省略此參數，或根據您的偏好設定進行調整。如需更多範例，請參閱 [Amazon Security Lake OCSF 查詢 GitHub 目錄](#)。

您可以查詢 Security Lake 存放在 AWS Lake Formation 資料庫和資料表中的資料。您也可以 Security Lake 主控台、API 或中建立第三方訂閱者 AWS CLI。第三方訂閱者也可以從您指定的來源查詢 Lake Formation 資料。

Lake Formation 資料湖管理員必須將相關資料庫和資料表的 SELECT 許可授予查詢資料的 IAM 身分。訂閱者也必須在 Security Lake 中建立，才能查詢資料。如需如何建立具有查詢存取權的訂閱者的詳細資訊，請參閱 [管理 Security Lake 訂閱者的查詢存取權](#)。

下列查詢包含使用的時間型篩選條件 eventDay，以確保您的查詢位於設定的保留設定內。如需詳細資訊，請參閱 [Querying data with retention settings](#)。

例如，如果超過 60 天的資料已過期，您的查詢應包含時間限制，以防止存取過期的資料。對於 60 天的保留期，請在查詢中包含下列子句：

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

此子句使用 59 天（而不是 60 天）來避免 Amazon S3 和 Apache Iceberg 之間的任何資料或時間重疊。

## 日誌來源資料表

當您查詢 Security Lake 資料時，必須包含資料所在的 Lake Formation 資料表名稱。

```
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
```

日誌來源資料表的常見值包括下列項目：

- `cloud_trail_mgmt_2_0` – AWS CloudTrail 管理事件
- `lambda_execution_2_0` – Lambda 的 CloudTrail 資料事件
- `s3_data_2_0` – S3 的 CloudTrail 資料事件
- `route53_2_0` – Amazon Route 53 解析程式查詢日誌
- `sh_findings_2_0` – AWS Security Hub 尋找
- `vpc_flow_2_0` – Amazon Virtual Private Cloud (Amazon VPC) 流程日誌
- `eks_audit_2_0` – Amazon Elastic Kubernetes Service (Amazon EKS) 稽核日誌
- `waf_2_0` – AWS WAF v2 日誌

範例：`sh_findings_2_0`us-east-1 區域資料表中的所有 Security Hub 問題清單

```
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
```

## 資料庫區域

查詢 Security Lake 資料時，您必須包含要從中查詢資料的資料庫區域名稱。如需目前可使用 Security Lake 的資料庫區域完整清單，請參閱 [Amazon Security Lake 端點](#)。

範例：從來源 IP 列出 Amazon Virtual Private Cloud 活動

下列範例列出來源 IP `192.0.2.1` 的所有 Amazon VPC 活動，這些活動是在 `20230301` (2023 年 3 月 1 日) 之後記錄在 `us-west-2` 的資料表 `vpc_flow_2_0` 中 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
```

## 分割區日期

透過分割資料，您可以限制每個查詢掃描的資料量，從而改善效能並降低成本。與 Security Lake 1.0 相比，Security Lake 2.0 中的分割區運作方式略有不同。Security Lake 現在會透過 `time_dt`、`region` 和 `實作分割accountid`。不過，Security Lake 1.0 透過 `eventDay`、`region` 和 `accountid` 參數實作分割。

查詢 `time_dt` 會自動從 S3 產生日期分割區，並且可以像 Athena 中的任何時間型欄位一樣進行查詢。

這是使用分割區在 `time_dt` 2023 年 3 月 1 日之後查詢日誌的範例查詢：

```
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
```

的常見值 `time_dt` 包括下列項目：

過去 1 年發生的事件

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

過去 1 個月內發生的事件

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

過去 30 天內發生的事件

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

過去 12 小時內發生的事件

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

過去 5 分鐘內發生的事件

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

## 7-14 天前發生的事件

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

在特定日期或之後發生的事件

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

範例：資料表中 **192.0.2.1** 2023 年 3 月 1 日或之後來源 IP 的所有 CloudTrail 活動清單

### 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_0
WHERE eventDay >= '20230301'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

範例：資料表 **192.0.2.1** 中過去 30 天來自來源 IP 的所有 CloudTrail 活動清單

### 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_0
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
```

## 查詢 Security Lake 可觀測項目

可觀測功能是 Security Lake 2.0 現提供的新功能。可觀察物件是一種樞紐元素，其中包含事件中許多位置中找到的相關資訊。查詢可觀測項目可讓使用者從其資料集中衍生高階安全洞見。

透過查詢可觀察項目中的特定元素，您可以將資料集限制為特定使用者名稱、資源 UUIDs、IPs、雜湊和其他 IOC 類型資訊

這是使用可觀測陣列來查詢 VPC Flow 和 Route53 資料表日誌的範例查詢，其中包含 IP 值 '172.01.02.03'

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

## CloudTrail 資料的範例 Security Lake 查詢

AWS CloudTrail 會追蹤 中的使用者活動和 API 用量 AWS 服務。訂閱者可以查詢 CloudTrail 資料，以了解下列類型的資訊：

以下是 AWS 來源版本 2 CloudTrail 資料的一些查詢範例：

過去 7 天內對 AWS 服務 進行未經授權的嘗試

```
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

```

### 192.0.2.1 過去 7 天內來自來源 IP 的所有 CloudTrail 活動清單

```

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

```

### 過去 7 天內所有 IAM 活動的清單

```

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

```

## 過去 7 天內 AIDACKCEVSQ6C2EXAMPLE 使用登入資料的執行個體

```
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
```

## 過去 7 天內失敗的 CloudTrail 記錄清單

```
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 解析程式查詢日誌的範例查詢

Amazon Route 53 解析程式查詢日誌會追蹤 Amazon VPC 內資源所做的 DNS 查詢。訂閱者可以查詢 Route 53 解析程式查詢日誌，以了解下列類型的資訊：

以下是 AWS 來源版本 2 的 Route 53 reresolver 查詢日誌的一些範例查詢：

## 過去 7 天內來自 CloudTrail 的 DNS 查詢清單

```
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

```

### s3.amazonaws.com 過去 7 天內相符的 DNS 查詢清單

```

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

```

### 過去 7 天內未解析的 DNS 查詢清單

```

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

```

### 過去 7 天內解析為 的 DNS 查詢清單 192.0.2.1

```

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 查詢 Security Hub 問題清單的範例

Security Hub 為您提供 中安全狀態的完整檢視，AWS 並協助您根據安全產業標準和最佳實務檢查環境。Security Hub 會產生安全檢查的問題清單，並接收第三方服務的問題清單。

以下是 AWS 來源版本 2 的 Security Hub 問題清單的一些範例查詢：

### **MEDIUM**在過去 7 天內，嚴重性大於或等於 的新問題清單

```

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

```

### 過去 7 天內的重複問題清單

```

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

```

### 過去 7 天內的所有非資訊性問題清單

```

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

```

### 資源是 Amazon S3 儲存貯體的調查結果 ( 無時間限制 )

```

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

```

### 常見漏洞評分系統 (CVSS) 分數大於 1 ( 無時間限制 ) 的問題清單

```

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(cvss)
WHERE cvs.base_score > 1.0
AND vulnerabilities is NOT NULL
LIMIT 25
```

符合常見漏洞與暴露 (CVE) 的調查結果 **CVE-0000-0000** (無時間限制)

```
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
```

過去 7 天內從 Security Hub 傳送問題清單的產品計數

```
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
```

過去 7 天內調查結果中的資源類型計數

```
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
```

來自過去 7 天內調查結果的易受攻擊套件

```
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

```

### 在過去 7 天內變更的問題清單

```

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 流程日誌的範例 Security Lake 查詢

Amazon Virtual Private Cloud (Amazon VPC) 提供往返 VPC 中網路介面的 IP 流量詳細資訊。

以下是 AWS 來源版本 2 的 Amazon VPC 流程日誌的一些範例查詢：

### 過去 7 天內特定 AWS 區域 中的流量

```

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 region in ('us-east-1', 'us-east-2', 'us-west-2')
LIMIT 25

```

### 22 過去 7 天內來源 IP 192.0.2.1 和來源連接埠的活動清單

```

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
```

### 過去 7 天內不同目的地 IP 地址的計數

```
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
```

### 過去 7 天內源自 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
```

### 過去 7 天內的所有 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
```

#### 443 過去 7 天內目的地為連接埠之連線的封包計數排序

```
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
```

#### 192.0.2.2 過去 7 天內 IP 192.0.2.1 與 之間的所有流量

```
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
```

#### 過去 7 天內的所有傳入流量

```
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
```

### 過去 7 天內的所有傳出流量

```
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
```

### 過去 7 天內所有被拒絕的流量

```
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 稽核日誌的範例 Security Lake 查詢

Amazon EKS 日誌會追蹤控制平面活動，將稽核和診斷日誌直接從 Amazon EKS 控制平面提供給帳戶中的 CloudWatch Logs。這些日誌可讓您輕鬆執行叢集並確保叢集的安全。訂閱者可以查詢 EKS 日誌，以了解下列類型的資訊。

以下是 AWS 來源版本 2 的 Amazon EKS 稽核日誌的一些範例查詢：

### 過去 7 天內對特定 URL 的請求

```
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
```

更新過去 7 天內來自 '10.0.97.167' 的請求

```
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
```

過去 7 天內與資源 'kube-controller-manager' 相關聯的請求和回應

```
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 日誌的範例 Security Lake 查詢

AWS WAF 是一種 Web 應用程式防火牆，可用來監控最終使用者傳送到應用程式的 Web 請求，以及控制對內容的存取。

以下是 AWS 來源第 2 版 AWS WAF v2 日誌的一些查詢範例：

## 在過去 7 天內，張貼來自特定來源 IP 的請求

```
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
```

## 過去 7 天內符合防火牆類型的請求 MANAGED\_RULE\_GROUP

```
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
```

## 過去 7 天內符合防火牆規則中 REGEX 的請求

```
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
```

### 拒絕取得過去 7 天內觸發 AWS WAF 規則之 AWS 登入資料的請求

```
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
```

### 取得 AWS 登入資料請求，在過去 7 天內依國家/地區分組

```
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 中的生命週期管理

您可以自訂 Security Lake，將資料存放在您偏好的時間 AWS 區域 長度。生命週期管理可協助您遵守不同的合規要求。

## 保留管理

若要管理資料，使其以經濟實惠的方式存放，您可以使用 Security Lake 中的生命週期設定來設定資料的保留。這些保留設定可協助您指定偏好的 [Amazon S3 儲存體方案](#)，以及 Amazon S3 物件在轉換至不同的儲存體方案以過期之前，保留在該儲存體方案中的期間。

### Warning

我們建議您透過 Security Lake 主控台、API 或 CLI 管理保留設定。這是因為直接在 Amazon S3 服務中修改 Amazon S3 生命週期設定可能會刪除中繼資料，並阻止您存取資料。

## Security Lake 中保留設定的重要考量事項

在 Security Lake 中管理資料保留時，請檢閱下列考量事項：

- Security Lake 不支援 [Amazon S3 物件鎖定](#)。建立資料湖儲存貯體時，預設會停用 S3 物件鎖定。使用預設保留模式啟用 S3 物件鎖定會中斷將標準化日誌資料交付至資料湖。
- 預設 Amazon S3 儲存類別為 S3 Standard。如果您未設定保留設定，Security Lake 會使用 Amazon S3 生命週期組態的預設設定，使用 S3 標準儲存類別無限期儲存資料。
- 在 Security Lake 中，您可以在區域層級指定保留設定。例如，您可以在特定 中設定所有 S3 物件 AWS 區域，以便在寫入資料湖 30 天後轉換為 S3 Standard-IA 儲存類別。
- 雖然保留設定只會套用至存放在 S3 儲存貯體中的資料，但保留政策會排除 Apache Iceberg 中繼資料。

## 啟用 Security Lake 時設定保留設定

當您加入 Security Lake 時，請遵循這些指示來設定一或多個區域的保留設定。

### Console

1. 開啟 Security Lake 主控台，網址為 <https://console.aws.amazon.com/securitylake/>。

2. 當您達到步驟 2：定義加入工作流程的目標時，請選擇選取儲存類別下的新增轉換。然後選擇您要轉換 Amazon S3 S3 儲存體方案。（未列出的預設儲存類別為 S3 Standard。）同時指定該儲存體方案的保留期間（以天為單位）。若要在該時間之後將物件轉換為另一個儲存體方案，請選擇新增轉換，然後輸入後續儲存體方案和保留期的設定。
3. 若要指定您希望 S3 物件何時過期，請選擇新增轉換。然後，對於儲存體方案，選擇過期。針對保留期間，輸入建立物件後，您要使用任何儲存類別將物件存放在 Amazon S3 中的總天數。當此期間結束時，物件會過期，Amazon S3 會將其刪除。
4. 完成後，請選擇下一步。

您的變更將套用至您在先前加入步驟期間在 中啟用 Security Lake 的所有區域。

## API

若要在加入 Security Lake 時以程式設計方式設定保留設定，請使用 Security Lake API [CreateDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [create-data-lake](#) 命令。在 `lifecycleConfiguration` 參數中指定您想要的保留設定，如下所示：

- 針對 `transitions`，指定您要在特定 Amazon S3 儲存類別 (`days`) 中存放 S3 物件的總天數 (`storageClass`)。Amazon S3
- 針對 `expiration`，指定建立物件後，使用任何儲存類別，在 Amazon S3 中儲存物件的總天數。當此期間結束時，物件會過期，Amazon S3 會將其刪除。

Security Lake 會將設定套用至您在 `configurations` 物件的 `region` 欄位中指定的區域。

例如，下列命令會在 `us-east-1` 區域中啟用 Security Lake。在此區域中，物件會在 365 天後過期，而物件會在 60 天後轉換為 `ONEZONE_IA` S3 儲存類別。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (`\`) 行接續字元來改善可讀性。

```
$ 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"
```

## 更新保留設定

啟用 Security Lake 後，請依照這些指示更新一或多個區域的保留設定。

### Console

1. 開啟 Security Lake 主控台，網址為 <https://console.aws.amazon.com/securitylake/>。
2. 在導覽窗格中，選擇區域
3. 選取區域，然後選擇編輯。
4. 在選取儲存類別區段中，輸入您想要的設定。針對儲存體方案，選擇您要轉換 Amazon S3 S3 儲存體方案。（未列出的預設儲存類別為 S3 Standard。）針對保留期間，輸入您要在該儲存類別中存放物件的天數。您可以指定多個轉換。

若要指定您希望 S3 物件過期的時間，請選擇儲存體方案的過期時間。然後，針對保留期間，在建立物件之後，使用任何儲存類別，輸入您要在 Amazon S3 中儲存物件的天數總計。當此期間結束時，物件會過期，Amazon S3 會將其刪除。

5. 完成後，請選擇儲存。

### API

若要以程式設計方式更新保留設定，請使用 Security Lake API [UpdateDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [update-data-lake](#) 命令。在您的請求中，使用 `lifecycleConfiguration` 參數來指定新設定：

- 若要變更轉換設定，請使用 `transitions` 參數來指定您要將 S3 物件存放在特定 Amazon S3 儲存類別 (`days`) 中的每個新期間，以天 () 為單位 `storageClass`。
- 若要變更整體保留期，請使用 `expiration` 參數指定建立物件後，您要使用任何儲存類別來存放 S3 物件的總天數。當此保留期結束時，物件會過期，Amazon S3 會將其刪除。

Security Lake 會將設定套用至您在 `configurations` 物件的 `region` 欄位中指定的區域。

Security Lake API `UpdateDataLake` 的操作可做為「upsert」操作，在指定的項目或記錄不存在時執行插入，或在已存在時執行更新。Security Lake 使用 AWS 加密解決方案安全地存放靜態資料。

`encryptionConfiguration` 從目前使用 KMS 的更新呼叫中包含的區域省略金鑰，會保留該區域的 KMS 金鑰，但指定金鑰會重設相同區域中的金鑰。

例如，下列 AWS CLI 命令會更新 `us-east-1` 區域的資料過期設定和儲存轉換設定。在此區域中，物件會在 500 天後過期，而物件會在 30 天後轉換為 `ONEZONE_IA` S3 儲存類別。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (`\`) 行接續字元來改善可讀性。

```
$ 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"
```

## 彙總區域

彙總區域會合併一或多個貢獻區域的資料。這可協助您遵守區域資料合規要求。

如需設定彙總區域的說明，請參閱 [在 Security Lake 中設定彙總區域](#)。

# Security Lake 中的開放式網路安全結構描述架構 (OCSF)

## 什麼是 OCSF ?

[Open Cybersecurity 結構描述架構 \(OCSF\)](#) 是由網路安全產業的 AWS 領導合作夥伴所共同努力的開放原始碼工作。OCSF 為常見安全事件提供標準結構描述、定義版本控制條件以促進結構描述演變，並包含安全日誌生產者和消費者的自我監督程序。OCSF 的公有原始碼託管於 [GitHub](#)。

Security Lake 會自動 AWS 服務 將來自原生支援的日誌和事件轉換為 OCSF 結構描述。轉換為 OCSF 後，Security Lake 會將資料存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中（每個儲存貯體一個 AWS 區域）AWS 帳戶。從自訂來源寫入 Security Lake 的日誌和事件必須遵循 OCSF 結構描述和 Apache Parquet 格式。訂閱者可以將日誌和事件視為一般 Parquet 記錄，或套用 OCSF 結構描述事件類別，以更準確地解譯記錄中包含的資訊。

## OCSF 事件類別

來自指定 Security Lake [來源](#) 的日誌和事件符合 OCSF 中定義的特定事件類別。DNS 活動、SSH 活動和身分驗證是 [OCSF 中事件類別](#) 的範例。您可以指定特定來源相符的事件類別。

## OCSF 來源識別

OCSF 使用各種欄位來協助您判斷一組特定日誌或事件的來源。這些是 Security Lake AWS 服務 中原生支援做為來源的相關欄位值。

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

來源	metadata. product.name	metadata. product.v endor_name	metadata. product.f eature.name	class_name	metadata. version
CloudTrail Lambda 資料 事件	CloudTrai l	AWS	Data	API Activity	1.0.0-rc. 2

來源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
CloudTrail 管理事件	CloudTrail	AWS	Management	API Activity、Authentication 或 Account Change	1.0.0-rc.2
CloudTrail S3 資料事件	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
安全中樞	Security Hub	AWS	符合 <a href="#">Security Hub ProductName</a> 值	Security Finding	1.0.0-rc.2
VPC 流量日誌	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.

來源	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
CloudTrail Lambda 資料事件	CloudTrail	AWS	Data	API Activity	1.1.0
CloudTrail 管理事件	CloudTrail	AWS	Management	API Activity、Au	1.1.0

來源	metadata. product.name	metadata. product.v endor_name	metadata. product.f eature.name	class_name	metadata. version
				ation 或 Account Change	
CloudTrail S3 資料事件	CloudTrai l	AWS	Data	API Activity	1.1.0
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
安全中樞	符合 AWS 安 全調查結果 格式 (ASFF) <a href="#">ProductNa me</a> 值	符合 AWS 安 全調查結果 格式 (ASFF) <a href="#">CompanyNa me</a> 值	從 ASFF 比 對 <a href="#">featureNa me</a> 值 ProductFi elds	Vulnerabi lity Finding, Complianc e Finding, or Detection Finding	1.1.0
VPC 流量日 誌	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0
EKS 稽核日 誌	Amazon EKS	AWS	Elastic Kubernet es Service	API Activity	1.1.0
AWS WAF v2 日誌	AWS WAF	AWS	–	HTTP Activity	1.1.0

## 與 Security Lake 的整合

Amazon Security Lake 與其他 AWS 服務 和第三方產品整合。整合可以將資料作為來源傳送至 Security Lake，或以訂閱者身分使用 Security Lake 中的資料。下列主題說明哪些 AWS 服務 和第三方產品與 Security Lake 整合。

### 主題

- [AWS 服務 與 Security Lake 整合](#)
- [與 Security Lake 的第三方整合](#)

## AWS 服務 與 Security Lake 整合

Amazon Security Lake 與其他 整合 AWS 服務。服務可以做為來源整合、訂閱者整合或兩者。

來源整合具有下列屬性：

- 將資料傳送至 Security Lake
- 資料抵達[Security Lake 中的開放式網路安全結構描述架構 \(OCSF\)結構描述](#)
- 資料以 Apache Parquet 格式送達

訂閱者整合可以透過下列其中一種方式存取 Security Lake 資料：

- 透過 HTTPS 端點從 Security Lake 讀取來源資料
- 透過 Amazon Simple Queue Service (Amazon SQS) 從 Security Lake 讀取來源資料
- 透過使用 直接查詢來源資料 AWS Lake Formation

下表提供 Security Lake 支援的 AWS 服務 整合清單。

AWS 服務	整合類型	描述	整合的運作方式
<a href="#">Amazon Bedrock</a>	Subscriber	產生 AI 支援的洞見，以分析 Security Lake 資料。	<a href="#">Amazon Bedrock 整合</a>
<a href="#">Amazon Detective</a>	Subscriber	透過查詢 Security Lake 來分析、調查和	<a href="#">Amazon Detective 整合</a>

AWS 服務	整合類型	描述	整合的運作方式
		快速識別安全調查結果或可疑活動的根本原因。	
<a href="#">Amazon OpenSearch Service</a>	Subscriber	使用 OpenSearch Service 擷取，從 Security Lake 資料產生安全洞見。	<a href="#">Amazon OpenSearch Service 整合</a>
<a href="#">Amazon OpenSearch Service 擷取管道</a>	訂閱者、來源	將日誌、指標和追蹤資料串流至 OpenSearch Service 和 Security Lake。	<a href="#">Amazon OpenSearch Service Ingestion 管道整合</a>
<a href="#">Amazon OpenSearch Service 零 ETL</a>	訂閱者 (查詢)	使用零 ETL 查詢 Security Lake 中的資料。	<a href="#">Amazon OpenSearch Service 零 ETL 直接查詢整合</a>
<a href="#">QuickSight</a>	Subscriber	使用 QuickSight 視覺化、探索和解釋 Security Lake 中的日誌。	<a href="#">QuickSight 整合</a>
<a href="#">Amazon SageMaker AI</a>	Subscriber	產生 AI 支援的洞見，以分析 Security Lake 資料。	<a href="#">Amazon SageMaker AI 整合</a>
<a href="#">AWS AppFabric</a>	來源	將軟體即服務 (SaaS) 應用程式日誌擷取並標準化為 Security Lake 標準格式。	<a href="#">AWS AppFabric 整合</a>
<a href="#">AWS Security Hub</a>	來源	以 Security Lake 標準格式集中和存放來自 Security Hub 的安全調查結果。	<a href="#">AWS Security Hub 整合</a>

## 與 Amazon Bedrock 整合

[Amazon Bedrock](#) 是一項全受管服務，可讓您透過統一 API 使用來自領導 AI 新創公司的高效能基礎模型 (FMs) 和 Amazon。藉助 Amazon Bedrock 的無伺服器體驗，您可以快速入門，使用您自己的資料私下自訂基礎模型，並使用 AWS 工具輕鬆安全地整合和部署到您的應用程式中，而無需管理任何基礎設施。

### 生成式 AI

您可以使用 SageMaker AI Studio 中 Amazon Bedrock 的生成式 AI 功能和自然語言輸入來分析 Security Lake 中的資料，並努力降低組織的風險並提高安全狀態。您可以透過自動識別適當的資料來源、產生和叫用 SQL 查詢，以及視覺化調查中的資料，來減少執行調查所需的時間。如需詳細資訊，請參閱[使用 Amazon SageMaker AI Studio 和 Amazon Bedrock 為 Amazon Security Lake 產生 AI 支援的洞見](#)。

## 與 Amazon Detective 整合

整合類型：訂閱者

[Amazon Detective](#) 會協助您分析、調查並快速識別安全調查結果或可疑活動的根本原因。Detective 會自動從您的 AWS 資源收集日誌資料。Detective 接著會使用機器學習、統計分析和圖論來產生視覺化內容，協助您更快地進行有效率的安全調查。Detective 提供預先建置的資料彙總、摘要和內容，可協助您快速分析並判斷潛在安全問題的本質和範圍。

當您整合 Security Lake 和 Detective 時，您可以從 Detective 查詢 Security Lake 存放的原始日誌資料。如需詳細資訊，請參閱[與 Amazon Security Lake 整合](#)。

## 與 Amazon OpenSearch Service 整合

整合類型：訂閱者

[Amazon OpenSearch Service](#) 是一種受管服務，可讓您在 中輕鬆部署、操作和擴展 OpenSearch Service 叢集 AWS 雲端。使用 OpenSearch Service Ingestion 將資料擷取至 OpenSearch Service 叢集，您可以更快速地衍生洞見，以進行時間敏感的安全調查。您可以快速回應安全事件，協助您保護業務關鍵資料和系統。

### OpenSearch Service 儀表板

將 OpenSearch Service 與 Security Lake 整合之後，您可以設定 Security Lake，透過無伺服器 OpenSearch Service Ingestion，將不同來源的安全資料傳送至 OpenSearch Service。如需如何設

定 OpenSearch Service 擷取以處理安全資料的詳細資訊，請參閱[使用 Amazon OpenSearch Service Ingestion 從 Amazon Security Lake 資料產生安全洞見](#)。

OpenSearch Service Ingestion 開始將資料寫入 OpenSearch Service 網域後。若要使用預先建置的儀表板視覺化資料，請導覽至儀表板，然後選擇任何一個已安裝的儀表板。

## 與 Amazon OpenSearch Service Ingestion 管道整合

整合類型：訂閱者、來源

Amazon OpenSearch Service Ingestion 是全受管、無伺服器資料收集器，可將日誌、指標和追蹤資料串流至 OpenSearch Service 和 Security Lake。

使用 OpenSearch Ingestion 管道將資料傳送至 Security Lake

您可以使用 OpenSearch Ingestion 中的 Amazon Simple Storage Service (Amazon S3) 接收器外掛程式，將資料從任何支援的來源傳送至 Security Lake。Security Lake 會自動將來自 AWS 環境、內部部署環境和 SaaS 供應商的安全資料集中到專用資料湖中。如需詳細資訊，請參閱[使用 OpenSearch 擷取管道搭配 Amazon Security Lake 做為接收器](#)。

使用 OpenSearch 擷取管道將資料從 Security Lake 傳送至 OpenSearch

您可以使用 Amazon S3 來源外掛程式，將資料擷取至 OpenSearch 擷取管道。如需詳細資訊，請參閱[使用 OpenSearch 擷取管道搭配 Amazon Security Lake 做為來源](#)。

## 與 Amazon OpenSearch Service 零 ETL 直接查詢整合

整合類型：訂閱者（查詢）

您可以使用 OpenSearch Service 直接查詢來分析 Amazon Security Lake 中的資料。OpenSearch Service 提供零 ETL 整合，以使用 OpenSearch SQL 或 OpenSearch Piped Processing Language (PPL) 直接查詢 Security Lake 中的資料，而不會產生建置擷取管道或在分析工具之間切換的摩擦。這種方法不需要資料移動或複製，可讓您使用 OpenSearch Service Dashboards 中的探索體驗來分析資料靜態的位置。當您想要從靜態查詢資料切換到使用儀表板主動監控時，您可以建立查詢結果的索引檢視，並將其擷取到 OpenSearch Service 索引。如需直接查詢的詳細資訊，請參閱《Amazon OpenSearch Service 開發人員指南》中的[使用直接查詢](#)。

OpenSearch Service 使用 OpenSearch Serverless 集合直接查詢 Security Lake 中的資料，並儲存您的索引檢視。若要這樣做，您可以建立資料來源，讓您能夠在 Security Lake 資料上使用 OpenSearch 零 ETL 功能。建立資料來源時，您可以直接搜尋、從 Security Lake 中取得洞見和分析存放在 Security

Lake 中的資料。您可以加速查詢效能，並在使用隨需索引的特定 Security Lake 資料集上使用進階 OpenSearch 分析。

- 如需建立 OpenSearch Service 資料來源整合的詳細資訊，請參閱 [《Amazon OpenSearch Service 開發人員指南》](#) 中的 [建立 Amazon Security Lake 資料來源整合](#)。 OpenSearch
- 如需在 OpenSearch Service 中設定 Security Lake 資料來源的詳細資訊，請參閱 [《Amazon OpenSearch Service 開發人員指南》](#) 中的 [在 OpenSearch Service Dashboards 中設定 Security Lake 資料來源](#)。 OpenSearch

如需搭配 Security Lake 使用 OpenSearch Service 的詳細資訊，請使用下列資源。

- [Amazon OpenSearch Service 和 Amazon Security Lake 整合簡介，以簡化安全分析](#)
- Amazon Security Lake OpenSearch Service 上的零 ETL 簡介

[Amazon Security Lake OpenSearch Service 上的零 ETL 簡介](#)

## 與 Amazon QuickSight 整合

整合類型：訂閱者

[Amazon QuickSight](#) 是一項雲端規模的商業智慧 (BI) 服務，可讓您隨時隨地為您工作的人員提供 easy-to-understand 的洞見。QuickSight 會連線至雲端中的資料，並結合來自許多不同來源的資料。QuickSight 讓決策者有機會在互動式視覺環境中探索和解讀資訊。他們可以從網路上的任何裝置以及從行動裝置安全地存取儀表板。

### QuickSight 儀表板

若要在 QuickSight 中視覺化您的 Amazon Security Lake 資料，請建立必要的 AWS 物件，並將基本資料來源、資料集、分析、儀表板和使用群組部署到 QuickSight 中與 Security Lake 相關。如需詳細說明，請參閱 [與 Amazon QuickSight 整合](#)。

如需使用 QuickSight 視覺化 Security Lake 資料的詳細資訊，請參閱下列資源。

[使用 QuickSight 視覺化 Security Lake 資料：2024 QuickSight 學習系列](#)

[使用 Security Lake 操作 AWS WAF Web ACL 日誌](#)

## 與 Amazon SageMaker AI 整合

整合類型：訂閱者

[Amazon SageMaker AI](#) 是一種全受管機器學習 (ML) 服務。有了 Security Lake，資料科學家和開發人員可以快速且自信地在生產就緒的託管環境中建置、訓練和部署 ML 模型。它提供執行 ML 工作流程的 UI 體驗，讓 SageMaker AI ML 工具可在多個整合開發環境 (IDEs) 中使用。

### SageMaker AI 洞察

您可以使用 SageMaker AI Studio 為 Security Lake 產生機器學習洞見。此 Studio 是適用於機器學習的 Web 整合開發環境 (IDE)，可為資料科學家提供工具，以準備、建置、訓練和部署機器學習模型。透過此解決方案，您可以快速部署一組 Python 筆記本，專注於 Security Lake 中的 [AWS Security Hub](#) 問題清單，也可以將其擴展為在 Security Lake 中整合其他 AWS 來源或自訂資料來源。如需詳細資訊，請參閱 [使用 Amazon SageMaker AI 產生 Amazon Security Lake 資料的機器學習洞察](#)。

## 與 整合 AWS AppFabric

整合類型：來源

[AWS AppFabric](#) 是一種無程式碼服務，可連接整個組織的軟體即服務 (SaaS) 應用程式，因此 IT 和安全應用程式會使用標準結構描述和中央儲存庫。

### Security Lake 如何接收 AppFabric 調查結果

您可以透過選取 Amazon Kinesis Data Firehose 做為目的地，並設定 Kinesis Data Firehose 以 OCSF 結構描述和 Apache Parquet 格式將資料交付至 Security Lake，將 AppFabric 稽核日誌資料傳送至 Security Lake。

### 先決條件

您必須先將 OCSF 標準化稽核日誌輸出至 Kinesis Data Firehose 串流，才能將 AppFabric 稽核日誌傳送至 Security Lake。然後，您可以設定 Kinesis Data Firehose 將輸出傳送到 Security Lake Amazon S3 儲存貯體。如需詳細資訊，請參閱 [《Amazon Kinesis 開發人員指南》](#) 中的 [為您的目的地選擇 Amazon S3](#)。Amazon Kinesis

### 將您的 AppFabric 調查結果傳送至 Security Lake

若要在完成上述先決條件後將 AppFabric 稽核日誌傳送至 Security Lake，您必須啟用這兩個服務，並在 Security Lake 中新增 AppFabric 做為自訂來源。如需新增自訂來源的說明，請參閱 [從 Security Lake 中的自訂來源收集資料](#)。

## 在 Security Lake 中停止接收 AppFabric 日誌

若要停止接收 AppFabric 稽核日誌，您可以使用 Security Lake 主控台、Security Lake API 或刪除 AWS CLI AppFabric 做為自訂來源。如需說明，請參閱[從 Security Lake 刪除自訂來源](#)。

## 與 整合 AWS Security Hub

整合類型：來源

[AWS Security Hub](#) 為您提供 中安全狀態的完整檢視 AWS，並協助您的環境符合安全產業標準和最佳實務。Security Hub 會從跨 AWS 帳戶、服務和支援的第三方合作夥伴產品收集安全資料，並協助您分析安全趨勢並識別最高優先順序的安全問題。

當您啟用 Security Hub 並將 Security Hub 調查結果新增為 Security Lake 中的來源時，Security Hub 會開始將新的調查結果和更新傳送至 Security Lake。

### Security Lake 如何接收 Security Hub 調查結果

在 Security Hub 中，將安全問題作為問題清單進行追蹤。有些問題清單來自其他 AWS 服務 或第三方合作夥伴偵測到的問題。Security Hub 也會針對規則執行自動化和持續安全檢查，以產生自己的調查結果。規則由安全控制表示。

所有 Security Hub 中的問題清單都使用稱為 [AWS 安全問題清單格式 \(ASFF\)](#) 的標準 JSON 格式。

Security Lake 會收到 Security Hub 調查結果並將其轉換為 [Security Lake 中的開放式網路安全結構描述架構 \(OCSF\)](#)。

### 將您的 Security Hub 調查結果傳送至 Security Lake

若要將 Security Hub 調查結果傳送至 Security Lake，您必須啟用這兩個服務，並將 Security Hub 調查結果新增為 Security Lake 中的來源。如需新增 AWS 來源的說明，請參閱 [新增 AWS 服務 做為來源](#)。

如果您希望 Security Hub 產生 [控制調查結果](#) 並將其傳送至 Security Lake，則必須啟用相關安全標準，並在其中以區域為基礎開啟資源記錄 AWS Config。如需詳細資訊，請參閱 AWS Security Hub 《使用者指南》中的 [啟用和設定 AWS Config](#)。

### 在 Security Lake 中停止接收 Security Hub 問題清單

若要停止接收 Security Hub 問題清單，您可以使用 Security Hub 主控台、Security Hub API，或 AWS Security Hub 使用者指南 AWS CLI 中的下列主題：

- [停用和啟用從整合接收問題清單的流程 \(主控台\)](#)
- [從 整合停用問題清單流程 \(Security Hub API、AWS CLI\)](#)

## 與 Security Lake 的第三方整合

Amazon Security Lake 與多個第三方供應商整合。供應商可以提供來源整合、訂閱者整合或服務整合。供應商可能會提供一或多個整合類型。

來源整合具有下列屬性：

- 將資料傳送至 Security Lake
- 資料以 Apache Parquet 格式送達
- 資料抵達 [Security Lake 中的開放式網路安全結構描述架構 \(OCSF\) 結構描述](#)

訂閱者整合具有下列屬性：

- 從 HTTPS 端點或 Amazon Simple Queue Service (Amazon SQS) 佇列的 Security Lake 讀取來源資料，或直接從 查詢來源資料 AWS Lake Formation
- 能夠讀取 Apache Parquet 格式的資料
- 能夠在 OCSF 結構描述中讀取資料

服務整合可協助您 AWS 服務 在組織中實作 Security Lake 和其他。他們也可以提供報告、分析和其他使用案例的協助。

若要搜尋特定的合作夥伴供應商，請參閱 [合作夥伴解決方案搜尋工具](#)。若要購買第三方產品，請參閱 [AWS Marketplace](#)。

若要請求新增為合作夥伴整合或成為 Security Lake 合作夥伴，請傳送電子郵件至 <securitylake-partners@amazon.com>。

如果您使用將調查結果傳送到 的第三方整合 AWS Security Hub，如果 Security Lake 的 Security Hub 整合已啟用，您也可以 Security Lake 中檢閱這些調查結果。如需啟用整合的指示，請參閱 [與整合 AWS Security Hub](#)。如需將調查結果傳送至 Security Hub 的第三方整合清單，請參閱 AWS Security Hub 《使用者指南》中的 [可用的第三方合作夥伴產品整合](#)。

設定訂閱者之前，請先驗證訂閱者的 OCSF 日誌支援。如需最新詳細資訊，請檢閱訂閱者的文件。

## 查詢整合

您可以查詢 Security Lake 存放在 AWS Lake Formation 資料庫和資料表中的資料。您也可以直接在 Security Lake 主控台、API 或 中建立第三方訂閱者 AWS Command Line Interface。

Lake Formation 資料湖管理員必須將相關資料庫和資料表的 SELECT 許可授予查詢資料的 IAM 身分。您必須先在 Security Lake 中建立訂閱者，才能查詢資料。如需如何建立具有查詢存取權的訂閱者的詳細資訊，請參閱 [管理 Security Lake 訂閱者的查詢存取權](#)。

您可以為下列第三方合作夥伴設定與 Security Lake 的查詢整合。

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

## Accenture – MxDR

整合類型：訂閱者、服務

Accenture's 與 Security Lake 的 MxDR 整合提供日誌和事件的即時資料擷取、受管異常偵測、威脅追蹤和安全操作。這有助於分析和受管偵測與回應 (MDR)。

作為服務整合，Accenture 也可以協助您在組織中實作 Security Lake。

[整合文件](#)

## Aqua Security

整合類型：來源

Aqua Security 可以新增為自訂來源，以將稽核事件傳送至 Security Lake。稽核事件會轉換為 OCSF 結構描述和 Parquet 格式。

[整合文件](#)

## Barracuda – Email Protection

整合類型：來源

Barracuda Email Protection 可以在偵測到新的網路釣魚電子郵件攻擊時，將事件傳送至 Security Lake。您可以在資料湖中接收這些事件和其他安全資料。

[整合文件](#)

## Booz Allen Hamilton

整合類型：Service

作為服務整合，透過將資料和分析與 Security Lake 服務融合，Booz Allen Hamilton使用資料驅動型網路安全方法。

[合作夥伴連結](#)

## Bosch Software and Digital Solutions – AIShield

整合類型：來源

AIShield 採用 技術，透過與 Security Lake 的整合，為 AI 資產 Bosch 提供自動化漏洞分析和端點保護。

[整合文件](#)

## ChaosSearch

整合類型：訂閱者

ChaosSearch 透過 Elasticsearch 和 SQL 等開放式 APIs，或原生包含的 Kibana 和 Superset UIs，為使用者提供多模型資料存取。您可以在 中使用 Security Lake 資料，ChaosSearch 沒有監控、警示和威脅追蹤的保留限制。這可協助您面對現今複雜的安全環境和持久性威脅。

[整合文件](#)

## Cisco Security – Secure Firewall

整合類型：來源

透過 Cisco Secure Firewall 與 Security Lake 整合，您可以以結構化且可擴展的方式存放防火牆日誌。Cisco 的 eNcore 用戶端會從 Firewall Management Center 串流防火牆日誌，執行結構描述轉換為 OCSF 結構描述，並將它們存放在 Security Lake 中。

### [整合文件](#)

## Claroty – xDome

整合類型：來源

Claroty xDome 會以最少的組態，將網路內偵測到的警示傳送至 Security Lake。彈性且快速的部署選項有助於 xDome 保護網路內延伸的物聯網 (XIoT) 資產，包括 IoT、IIoT 和 BMS 資產，同時自動偵測威脅的早期指標。

### [整合文件](#)

## CMD Solutions

整合類型：Service

CMD Solutions 透過設計、自動化和持續保證程序，及早且持續地整合安全性，協助企業提高敏捷性。作為服務整合，CMD Solutions 可協助您在組織中實作 Security Lake。

### [合作夥伴連結](#)

## Confluent – Amazon S3 Sink Connector

整合類型：來源

Confluent 會自動使用全受管、預先建置的連接器來連接、設定和協調資料整合。Confluent S3 Sink Connector 可讓您擷取原始資料，並以原生 parquet 格式大規模傳入 Security Lake。

### [整合文件](#)

## Contrast Security

整合類型：來源

整合的合作夥伴產品：對比度評估

Contrast Security Assess 是一種 IAST 工具，可在 Web 應用程式、APIs 和微服務中提供即時漏洞偵測。評估與 Security Lake 整合，以協助為所有工作負載提供集中可見性。

[整合文件](#)

## Cribl – Search

整合類型：訂閱者

您可以使用 Cribl Search 來搜尋 Security Lake 資料。

[整合文件](#)

## Cribl – Stream

整合類型：來源

您可以使用 Cribl Stream 將資料從任何Cribl支援的第三方來源傳送至 OCSF 結構描述中的 Security Lake。

[整合文件](#)

## CrowdStrike – Falcon Data Replicator

整合類型：來源

此整合CrowdStrike Falcon Data Replicator會以持續串流為基礎從 提取資料、將資料轉換為 OCSF 結構描述，並將其傳送至 Security Lake。

[整合文件](#)

## CrowdStrike – Next Gen SIEM

整合類型：訂閱者

使用具有原生 OCSF 結構描述剖析器CrowdStrike Falcon Next-Gen SIEM的資料連接器來簡化 Security Lake 資料的擷取。透過在一個統一平台中結合無可匹敵的安全深度和廣度來阻止違規，Falcon NG SIEM徹底改變威脅偵測、調查和回應。

[整合文件](#)

## CyberArk – Unified Identify Security Platform

整合類型：來源

CyberArk Audit Adapter 函數 AWS Lambda 會從 收集安全事件，CyberArk Identity Security Platform 並將資料傳送至 OCSF 結構描述中的 Security Lake。

[整合文件](#)

## Cyber Security Cloud – Cloud Fastener

整合類型：訂閱者

CloudFastener 利用 Security Lake，讓您更輕鬆地整合雲端環境的安全資料。

[整合文件](#)

## DataBahn

整合類型：來源

使用 Security Data Fabric 在 Security Lake 中集中您的DataBahn's安全資料。

[整合文件 \( 登入DataBahn入口網站以檢閱文件 \)](#)

## Darktrace – Cyber AI Loop

整合類型：來源

Darktrace 和 Security Lake 整合將Darktrace自我學習的力量帶入 Security Lake。的洞見Cyber AI Loop可以與您組織安全堆疊的其他資料串流和元素建立關聯。整合會將Darktrace模型違規記錄為安全調查結果。

[整合文件 \( 登入Darktrace入口網站以檢閱文件 \)](#)

## Datadog

整合類型：訂閱者

Datadog Cloud SIEM 會偵測您雲端環境的即時威脅，包括 Security Lake 中的資料，並在單一平台上整合 DevOps 和安全團隊。

[整合文件](#)

## Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

整合類型：訂閱者、服務

Deloitte MXDR CAE 可協助您快速儲存、分析和視覺化標準化的安全資料。CAE 套件的自訂分析、AI 和 ML 功能會根據針對 Security Lake 中的 OCSF 格式資料執行的模型，自動提供可行的洞見。

作為服務整合，Deloitte 也可以協助您在組織中實作 Security Lake。

### [整合文件](#)

## Devo

**整合類型：**訂閱者

的Devo收集器 AWS 支援從 Security Lake 擷取。此整合可協助您分析和解決各種安全使用案例，例如威脅偵測、調查和事件回應。

### [整合文件](#)

## DXC – SecMon

**整合類型：**訂閱者、服務

DXC SecMon 從 Security Lake 收集安全事件並監控它們，以偵測和提醒潛在的安全威脅。這有助於組織更好地了解其安全狀態，並主動識別和回應威脅。

作為服務整合，DXC 也可以協助您在組織中實作 Security Lake。

### [整合文件](#)

## Eviden – Alsaac ( 先前為 Atos)

**整合類型：**訂閱者

Alsaac MDR 平台使用擷取至 Security Lake 中 OCSF 結構描述的 VPC 流程日誌，並使用 AI 模型來偵測威脅。

### [整合文件](#)

## ExtraHop – Reveal(x) 360

**整合類型：**來源

您可以透過整合網路資料來增強工作負載和應用程式安全性，包括從 ExtraHop Reveal(x) 360到 OCSF 結構描述中 Security Lake IOCs 偵測

[整合文件](#)

## Falcosidekick

整合類型：來源

Falcosidekick 收集 Falco 事件並將其傳送至 Security Lake。此整合會使用 OCSF 結構描述匯出安全事件。

[整合文件](#)

## Fortinet - Cloud Native Firewall

整合類型：來源

在中建立 FortiGate CNF 執行個體時 AWS，您可以將 Amazon Security Lake 指定為日誌輸出目的地。

[整合文件](#)

## Gigamon – Application Metadata Intelligence

整合類型：來源

Gigamon Application Metadata Intelligence (AMI) 為您的可觀測性、SIEM 和網路效能監控工具提供關鍵中繼資料屬性。這有助於提供更深入的應用程式可見性，讓您可以找出效能瓶頸、品質問題和潛在的網路安全風險。

[整合文件](#)

## Hoop Cyber

整合類型：服務

Hoop Cyber FastStart 包括資料來源評估、優先順序、資料來源加入，並協助客戶使用 Security Lake 提供的現有工具和整合來查詢其資料。

[合作夥伴連結](#)

## HTCD – AI-First Cloud Security Platform

整合類型：訂閱者

取得即時合規自動化、安全調查結果的優先順序，以及量身打造的修補程式。HTCD 可以查詢 Security Lake，以協助您透過自然語言查詢和 AI 驅動的洞察來發現威脅。

## [整合文件](#)

### IBM – QRadar

整合類型：訂閱者

IBM Security QRadar SIEM with UAX 將 Security Lake 與分析平台整合，以識別和防止混合雲端的威脅。此整合支援資料存取和查詢存取。

#### [使用 AWS CloudTrail 日誌的整合文件](#)

#### [使用 Amazon Athena 進行查詢的整合文件](#)

### Infosys

整合類型：服務

Infosys 可協助您針對組織需求自訂 Security Lake 實作，並提供自訂洞見。

#### [合作夥伴連結](#)

### Insbuilt

整合類型：服務

Insbuilt 專精於雲端諮詢服務，可協助您了解如何在組織中實作 Security Lake。

#### [合作夥伴連結](#)

### Kyndryl – AIOps

整合類型：訂閱者、服務

Kyndryl 與 Security Lake 整合，以提供網路資料、威脅情報和 AI 驅動分析的互通性。身為資料存取訂閱者，會從 Security Lake Kyndryl 擷取 AWS CloudTrail 管理事件以進行分析。

作為服務整合，Kyndryl 也可以協助您在組織中實作 Security Lake。

## [整合文件](#)

## Lacework – Polygraph

整合類型：來源

Lacework Polygraph® Data Platform 將與 Security Lake 整合為資料來源，並在您的 AWS 環境中提供有關漏洞、設定錯誤以及已知和未知威脅的安全調查結果。

[整合文件](#)

## Laminar

整合類型：來源

Laminar 會將資料安全事件傳送至 OCSF 結構描述中的 Security Lake，使其可用於其他分析使用案例，例如事件回應和調查。

[整合文件](#)

## MegazoneCloud

整合類型：服務

MegazoneCloud 專精於雲端諮詢服務，可協助您了解如何在組織中實作 Security Lake。我們將 Security Lake 與整合式 ISV 解決方案連線，以建置自訂任務，並建置與客戶需求相關的自訂洞見。

[整合文件](#)

## Monad

整合類型：來源

Monad 會自動將您的資料轉換為 OCSF 結構描述，並將其傳送至 Security Lake 資料湖。

[整合文件](#)

## NETSCOUT – Omnis Cyber Intelligence

整合類型：來源

透過與 Security Lake 整合，NETSCOUT 成為安全調查結果的自訂來源，並詳細了解企業中發生的情況，例如網路威脅、安全風險和攻擊面變更。這些調查結果是由 NETSCOUT CyberStreams和 在客戶

帳戶中產生Omnis Cyber Intelligence，然後傳送到 OCSF 結構描述中的 Security Lake。擷取的資料也符合 Security Lake 來源的其他要求和最佳實務，包括格式、結構描述、分割和效能相關方面。

### [整合文件](#)

## Netskope – CloudExchange

整合類型：來源

Netskope 透過與 Security Lake 共用安全相關日誌和威脅資訊，協助您加強安全狀態。Netskope問題清單會使用CloudExchange外掛程式傳送至 Security Lake，該外掛程式可在本機資料中心內 AWS 或內部以 Docker 為基礎的環境啟動。

### [整合文件](#)

## New Relic ONE

整合類型：訂閱者

New Relic ONE 是以 Lambda 為基礎的訂閱者應用程式。它部署在您的帳戶中，由 Amazon SQS 觸發，並使用New RelicNew Relic授權金鑰將資料傳送至

### [整合文件](#)

## Okta – Workforce Identity Cloud

整合類型：來源

Okta 透過 Amazon EventBridge 整合將身分日誌傳送至 OCSF 結構描述中的 Security Lake。在 OCSF 結構描述Okta System Logs中，將協助安全與資料科學家團隊透過開放原始碼標準查詢安全事件。從 Okta 產生標準化 OCSF 日誌可協助您執行稽核活動，並在一致的結構描述下產生與身分驗證、授權、帳戶變更和實體變更相關的報告。

### [整合文件](#)

[AWS CloudFormation 在 Security Lake 中新增Okta為自訂來源的 範本](#)

## Orca – Cloud Security Platform

整合類型：來源

的無Orca代理程式雲端安全平台透過在 OCSF 結構描述中傳送雲端偵測和回應 (CDR) 事件，與 Security Lake AWS 整合。

[整合文件 \( 登入Orca入口網站以檢閱文件 \)](#)

## Palo Alto Networks – Prisma Cloud

整合類型：來源

Palo Alto Networks Prisma Cloud 會彙總雲端原生環境中跨 VMs漏洞偵測資料，並將其傳送至 Security Lake。

[整合文件](#)

## Palo Alto Networks – XSOAR

整合類型：Subscriber

Palo Alto Networks XSOAR 已建立與 XSOAR 和 Security Lake 的訂閱者整合。

[整合文件](#)

## Panther

整合類型：訂閱者

Panther 支援擷取 Security Lake 日誌以用於搜尋和偵測。

[整合文件](#)

## Ping Identity – PingOne

整合類型：來源

PingOne 會以 OCSF 結構描述和 Parquet 格式將帳戶修改提醒傳送至 Security Lake，讓您探索帳戶變更並採取行動。

[整合文件](#)

## PwC – Fusion center

整合類型：訂閱者、服務

PwC 帶來知識和專業知識，協助用戶端實作融合中心以滿足其個別需求。融合中心以 Amazon Security Lake 為基礎，提供結合各種來源資料的能力，以建立集中式、近乎即時的檢視。

### [整合文件](#)

## Query.AI – Query Federated Search

整合類型：訂閱者

Query Federated Search 可以透過 Amazon Athena 直接查詢任何 Security Lake 資料表，以支援 OCSF 結構描述中各種可觀測項目、事件和物件的事件回應、調查、威脅追蹤和一般搜尋。

### [整合文件](#)

## Rapid7 – InsightIDR

整合類型：訂閱者

InsightIDRSIEM/XDR Rapid7 解決方案可以在 Security Lake 中擷取日誌，以偵測威脅並調查可疑活動。

### [整合文件](#)

## RipJar – Labyrinth for Threat Investigations

整合類型：訂閱者

Labyrinth for Threat Investigations 提供企業級方法，根據資料融合大規模探索威脅，並具有精細的安全性、可調適的工作流程和報告。

### [整合文件](#)

## Sailpoint

整合類型：來源

整合的合作夥伴產品：SailPoint IdentityNow

此整合可讓客戶從 轉換事件資料SailPoint IdentityNow。整合旨在提供自動化程序，將IdentityNow使用者活動和管理事件帶入 Security Lake，以改善安全事件和事件監控產品的洞察。

### [整合文件](#)

## Securonix

整合類型：訂閱者

Securonix Next-Gen SIEM 與 Security Lake 整合，讓安全團隊能夠更快速地擷取資料，並擴展其偵測和回應功能。

[整合文件](#)

## SentinelOne

整合類型：訂閱者

SentinelOne Singularity™ XDR 平台會將即時偵測和回應延伸至在內部部署和公有雲端基礎設施上執行的端點、身分和雲端工作負載，包括 Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Container Service (Amazon ECS) 和 Amazon Elastic Kubernetes Service (Amazon EKS)。

[整合文件 \( 登入SentinelOne入口網站以檢閱文件 \)](#)

## Sentra – Data Lifecycle Security Platform

整合類型：來源

在帳戶中部署Sentra掃描基礎設施之後，Sentra 會擷取問題清單並將其擷取到您的 SaaS。這些調查結果是中繼資料，會將 和更新串流Sentra存放在 OCSF 結構描述中的 Security Lake 進行查詢。

[整合文件](#)

## SOC Prime

整合類型：訂閱者

SOC Prime 透過 Amazon OpenSearch Service 和 Amazon Athena 與 Security Lake 整合，以根據零信任里程碑促進智慧資料協同運作和威脅追捕。SOC Prime可讓安全團隊提高威脅可見性，並調查事件，而不會產生大量警示。您可以使用可在 OCSF 結構描述中自動轉換為 Athena 和 OpenSearch Service 的可重複使用規則和查詢來節省開發時間。

[整合文件](#)

## Splunk

整合類型：訂閱者

適用於 Amazon Web Services 的 Splunk AWS 附加元件 (AWS) 支援從 Security Lake 擷取。此整合透過從 Security Lake 訂閱 OCSF 結構描述中的資料，協助您加速威脅偵測、調查和回應。

### [整合文件](#)

## Stellar Cyber

整合類型：訂閱者

Stellar Cyber 會使用來自 Security Lake 的日誌，並將記錄新增至 Stellar Cyber 資料湖。此連接器使用 OCSF 結構描述。

### [整合文件](#)

## Sumo Logic

整合類型：訂閱者

Sumo Logic 使用來自 Security Lake 的資料，並提供跨 AWS、內部部署和混合雲端環境的廣泛可見性。Sumo Logic 為安全團隊提供其所有安全工具的全方位可見性、自動化和威脅監控。

### [整合文件](#)

## Swimlane – Turbine

整合類型：訂閱者

Swimlane 從 OCSF 結構描述中的 Security Lake 擷取資料，並透過低程式碼手冊和案例管理來傳送資料，以加速威脅偵測、調查和事件回應。

### [整合文件 \( 登入 Swimlane 入口網站以檢閱文件 \)](#)

## Sysdig Secure

整合類型：來源

Sysdig Secure's 雲端原生應用程式保護平台 (CNAPP) 會將安全事件傳送至 Security Lake，以最大化監督、簡化調查並簡化合規。

### [整合文件](#)

## Talon

整合類型：來源

整合的合作夥伴產品：Talon Enterprise Browser

Talon's Enterprise Browser是安全且隔離的瀏覽器型端點環境，可將Talon存取、資料保護、SaaS 動作和安全事件傳送至 Security Lake，提供可見性和選項，以跨關聯事件進行偵測、鑑識和調查。

[整合文件（登入Talon入口網站以檢閱文件）](#)

## Tanium

整合類型：來源

Tanium Unified Cloud Endpoint Detection, Management, and Security 平台提供庫存資料給 OCSF 結構描述中的 Security Lake。

[整合文件](#)

## TCS

整合類型：服務

TCS AWS Business Unit 提供創新、經驗和才能。此整合由十年的共同價值建立、深厚的產業知識、技術專業知識和交付智慧提供支援。作為服務整合，TCS可協助您在組織中實作 Security Lake。

[整合文件](#)

## Tego Cyber

整合類型：訂閱者

Tego Cyber 與 Security Lake 整合，協助您快速偵測和調查潛在的安全威脅。透過將各種威脅指標與廣泛的時間範圍和日誌來源相互關聯，Tego Cyber 會發現隱藏的威脅。平台充實了高度情境式威脅情報，提供威脅偵測和調查的精確度和洞見。

[整合文件](#)

## Tines – No-code security automation

整合類型：訂閱者

Tines No-code security automation 利用集中在 Security Lake 中的安全資料，協助您做出更準確的決策。

### [整合文件](#)

## Torq – Enterprise Security Automation Platform

整合類型：來源、訂閱者

Torq 可無縫整合 Security Lake 做為自訂來源和訂閱者。Torq 可協助您使用簡單的無程式碼平台實作企業規模自動化和協同運作。

### [整合文件](#)

## Trellix – XDR

整合類型：來源、訂閱者

作為一個開放式的 DevOps 平台，Trellix XDR 支援 Security Lake 整合。Trellix XDR 可以利用 OCSF 結構描述中的資料進行安全分析使用案例。您也可以在中使用超過 1,000 個安全事件來源來擴增 Security Lake 資料湖Trellix XDR。這可協助您擴展 AWS 環境的偵測和回應功能。擷取的資料與其他安全風險相關聯，為您提供必要的手冊，以及時回應風險。

### [整合文件](#)

## Trend Micro – CloudOne

整合類型：來源

Trend Micro CloudOne Workload Security 會將下列資訊從您的 Amazon Elastic Compute Cloud (EC2) 執行個體傳送至 Security Lake：

- DNS 查詢活動
- 檔案活動
- 網路活動
- 程序活動
- 登錄值活動
- 使用者帳戶活動

[整合文件](#)

## Uptycs – Uptycs XDR

整合類型：來源

Uptycs 會將 OCSF 結構描述中的大量資料從內部部署和雲端資產傳送至 Security Lake。資料包括來自端點和雲端工作負載的行為威脅偵測、異常偵測、政策違規、風險政策、設定錯誤和漏洞。

[整合文件](#)

## Vectra AI – Vectra Detect for AWS

整合類型：來源

透過使用 Vectra Detect for AWS，您可以使用專用 AWS CloudFormation 範本，將高保真度警示傳送至 Security Lake 做為自訂來源。

[整合文件](#)

## VMware Aria Automation for Secure Clouds

整合類型：來源

透過此整合，您可以偵測雲端設定錯誤，並將其傳送至 Security Lake 進行進階分析。

[整合文件](#)

## Wazuh

整合類型：訂閱者

Wazuh 旨在安全地處理使用者資料、為每個來源提供查詢存取，以及最佳化查詢成本。

[整合文件](#)

## Wipro

整合類型：來源、服務

此整合可讓您從 Wipro Cloud Application Risk Governance (CARG) 平台收集資料，以統一檢視整個企業的雲端應用程式和合規狀態。

作為服務整合，Wipro 也可以協助您在組織中實作 Security Lake。

### [整合文件](#)

## Wiz – CNAPP

整合類型：來源

Wiz 與 Security Lake 之間的整合透過利用 OCSF 結構描述，在單一安全資料湖中促進雲端安全資料收集，這是一種開放原始碼標準，專為可擴展和標準化的安全資料交換而設計。

[整合文件 \( 登入Wiz入口網站以檢閱文件 \)](#)

## Zscaler – Zscaler Posture Control

整合類型：來源

Zscaler Posture Control™ 是雲端原生應用程式保護平台，會將安全調查結果傳送至 OCSF 結構描述中的 Security Lake。

[整合文件](#)

# Security Lake 中的安全

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 和 之間的共同責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。第三方稽核人員會定期測試和驗證我們的安全有效性，做為[AWS 合規計畫](#)的一部分。若要了解適用於 Amazon Security Lake 的合規計畫，請參閱[AWS 合規計畫範圍內的服務](#)。
- 雲端安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Security Lake 時套用共同責任模型。下列主題說明如何設定 Security Lake 以符合您的安全和合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Security Lake 資源。

## 主題

- [Security Lake 的身分和存取管理](#)
- [Amazon Security Lake 中的資料保護](#)
- [Amazon Security Lake 的合規驗證](#)
- [Security Lake 的安全最佳實務](#)
- [Amazon Security Lake 中的彈性](#)
- [Amazon Security Lake 中的基礎設施安全](#)
- [Security Lake 中的組態和漏洞分析](#)
- [Amazon Security Lake 和介面 VPC 端點 \(AWS PrivateLink\)](#)
- [監控 Amazon Security Lake](#)

## Security Lake 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可），以使用 Security Lake 資源。IAM 是 AWS 服務 您可以免費使用的。

## 主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [Security Lake 如何與 IAM 搭配使用](#)
- [Security Lake 的身分型政策範例](#)
- [AWS Security Lake 的 受管政策](#)
- [使用 Security Lake 的服務連結角色](#)

## 目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Security Lake 中執行的工作。

**服務使用者** – 如果您使用 Security Lake 服務來執行您的任務，則您的管理員會為您提供所需的登入資料和許可。當您使用更多 Security Lake 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Security Lake 中的功能，請參閱 [對 Amazon Security Lake 身分和存取進行故障診斷](#)。

**服務管理員** – 如果您在公司負責 Security Lake 資源，您可能可以完整存取 Security Lake。您的任務是判斷服務使用者應存取哪些 Security Lake 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Security Lake 使用 IAM，請參閱 [Security Lake 如何與 IAM 搭配使用](#)。

**IAM 管理員** – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Security Lake 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Security Lake 身分型政策範例，請參閱 [Security Lake 的身分型政策範例](#)。

## 使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 (登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入。AWS IAM Identity Center (IAM Identity Center) 使用者、您的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取時，您會間接擔任角色。

視您身分的使用者類型而定，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 AWS 登入 《使用者指南》中的[如何登入您的 AWS 帳戶](#)。

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的[適用於 API 請求的 AWS Signature 第 4 版](#)。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如，AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的[多重要素驗證](#)和《IAM 使用者指南》中的[IAM 中的 AWS 多重要素驗證](#)。

## AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的[需要根使用者憑證的任務](#)。

## 聯合身分

最佳實務是，要求人類使用者，包括需要管理員存取權的使用者，使用臨時登入資料 AWS 服務來使用與身分提供者的聯合來存取。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、AWS Directory Service、身分中心目錄，或是使用透過身分來源提供的憑證 AWS 服務存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶和群組，以便在所有和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center ?](#)。

## IAM 使用者和群組

[IAM 使用者](#)是 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 [IAM 使用者指南](#)中的為需要長期憑證的使用案例定期輪換存取金鑰。

[IAM 群組](#)是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 [IAM 使用者的使用案例](#)。

## IAM 角色

[IAM 角色](#)是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從[使用者切換至 IAM 角色（主控台）](#)。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《[IAM 使用者指南](#)》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的[許可集](#)。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源 (而不是使用角色做為代理)。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的[IAM 中的跨帳戶資源存取](#)。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
- 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱 [《轉發存取工作階段》](#)。

- 服務角色 – 服務角色是服務擔任的 [IAM 角色](#)，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[建立角色以委派許可權給 AWS 服務](#)。
- 服務連結角色 – 服務連結角色是一種連結至的服務角色。AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 `中 AWS 帳戶`，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式](#)。

## 使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 `中的物件`，AWS 當與身分或資源相關聯時，會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時，會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 `中`。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的[JSON 政策概觀](#)。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、AWS CLI 或 API AWS 取得角色資訊。

### 身分型政策

身分型政策是可以附加到身分（例如 IAM 使用者、使用者群組或角色）的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的[在受管政策和內嵌政策間選擇](#)。

## 資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者，或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

## 存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF 和 Amazon VPC 是支援 ACLs 的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的[存取控制清單 \(ACL\) 概觀](#)。

## 其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 Principal 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCPs) – SCPs 是 JSON 政策，可指定 in. 中組織或組織單位 (OU) 的最大許可 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶的多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的

許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs 的詳細資訊，包括 AWS 服務支援 RCPs 的清單，請參閱 AWS Organizations 《使用者指南》中的[資源控制政策 RCPs](#)。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的[工作階段政策](#)。

## 多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

## Security Lake 如何與 IAM 搭配使用

在您使用 IAM 管理 Security Lake 的存取權之前，請先了解哪些 IAM 功能可與 Security Lake 搭配使用。

您可以搭配 Amazon Security Lake 使用的 IAM 功能

IAM 功能	Security Lake 支援
<a href="#">身分型政策</a>	是
<a href="#">資源型政策</a>	是
<a href="#">政策動作</a>	是
<a href="#">政策資源</a>	是
<a href="#">政策條件索引鍵</a>	是
<a href="#">ACL</a>	否
<a href="#">ABAC (政策中的標籤)</a>	是
<a href="#">暫時性憑證</a>	是
<a href="#">主體許可</a>	是

IAM 功能	Security Lake 支援
<a href="#">服務角色</a>	否
<a href="#">服務連結角色</a>	是

若要深入了解 Security Lake 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的[AWS 與 IAM 搭配使用的服務](#)。

## Security Lake 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的[IAM JSON 政策元素參考](#)。

Security Lake 支援以身分為基礎的政策。如需詳細資訊，請參閱[Security Lake 的身分型政策範例](#)。

## Security Lake 中的資源型政策

支援資源型政策：是

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包括帳戶、使用者、角色、聯合身分使用者，或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當委託人和資源位於不同的位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體 (使用者或角色) 存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

Security Lake 服務會為存放資料的 Amazon S3 儲存貯體建立以資源為基礎的政策。您不會將這些資源型政策連接至 S3 儲存貯體。Security Lake 會自動代表您建立這些政策。

範例資源是 Amazon Resource Name (ARN) 為的 S3 儲存貯體 `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`。在此範例中，`region` 是您啟用 Security Lake 的特定 AWS 區域，而 Security Lake `bucket-identifier` 是指派給儲存貯體的區域唯一英數字串。Security Lake 會建立 S3 儲存貯體來存放該區域的資料。資源政策會定義哪些主體可以對儲存貯體執行動作。以下是 Security Lake 連接到儲存貯體的範例資源型政策（儲存貯體政策）：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
        "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    },
    {
      "Sid": "PutSecurityLakeObject",
      "Effect": "Allow",
      "Principal": {
        "Service": "securitylake.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
        "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{DA-AccountID}",
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

```
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:securitylake:us-east-1:{DA-AccountID}:*"
    }
  }
]
}
```

若要進一步了解以資源為基礎的政策，請參閱《IAM 使用者指南》中的以[身分為基礎的政策和資源為基礎的政策](#)。

## Security Lake 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

如需 Security Lake 動作的清單，請參閱服務授權參考中的 [Amazon Security Lake 定義的動作](#)。

Security Lake 中的政策動作在動作之前使用下列字首：

```
securitylake
```

例如，若要授予使用者存取特定訂閱者相關資訊的許可，請在指派給該使用者的政策中包含 securitylake:GetSubscriber 動作。政策陳述式必須包含 Action 或 NotAction 元素。Security Lake 會定義自己的動作集，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 Security Lake 身分型政策的範例，請參閱 [Security Lake 的身分型政策範例](#)。

## Security Lake 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (\*) 來表示陳述式適用於所有資源。

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

Security Lake 定義下列資源類型：訂閱者，以及 AWS 帳戶 特定的資料湖組態 AWS 區域。您可以使用 ARNs 在政策中指定這些類型的資源。

如需每個類型的 Security Lake 資源類型和 ARN 語法清單，請參閱服務授權參考中的 [Amazon Security Lake 定義的資源類型](#)。若要了解您可以為每種類型的資源指定哪些動作，請參閱服務授權參考中的 [Amazon Security Lake 定義的動作](#)。

若要檢視 Security Lake 身分型政策的範例，請參閱 [Security Lake 的身分型政策範例](#)。

## Security Lake 的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵，AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，會使用邏輯 OR 操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 [IAM 政策元素：變數和標籤](#)。

AWS 支援全域條件金鑰和服務特定的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

如需 Security Lake 條件金鑰的清單，請參閱服務授權參考中的 [Amazon Security Lake 條件金鑰](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱服務授權參考中的 [Amazon Security Lake 定義的動作](#)。如需使用條件索引鍵的政策範例，請參閱 [Security Lake 的身分型政策範例](#)。

## Security Lake 中的存取控制清單 (ACLs)

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Security Lake 不支援 ACLs，這表示您無法將 ACL 連接至 Security Lake 資源。

## 使用 Security Lake 的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤連接至 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的 [使用屬性型存取控制 \(ABAC\)](#)。

您可以將標籤連接至 Security Lake 資源 - 訂閱者，以及 AWS 帳戶 個別的資料湖組態 AWS 區域。您也可以在政策的 Condition 元素中提供標籤資訊，以控制對這些資源類型的存取。如需標記 Security Lake 資源的詳細資訊，請參閱 [標記 Security Lake 資源](#)。如需根據該資源的標籤控制資源存取的身分型政策範例，請參閱 [Security Lake 的身分型政策範例](#)。

## 搭配 Security Lake 使用臨時憑證

支援臨時憑證：是

當您使用臨時登入資料登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱 [《AWS 服務 IAM 使用者指南》](#) 中的使用 IAM 的。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 [《IAM 使用者指南》](#) 中的 [從使用者切換至 IAM 角色 \(主控台\)](#)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [IAM 中的暫時性安全憑證](#)。

Security Lake 支援使用臨時登入資料。

## 轉送 Security Lake 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的策略詳細資訊，請參閱 [轉發存取工作階段](#)。

有些 Security Lake 動作需要其他 中其他相依動作的許可 AWS 服務。如需這些動作的清單，請參閱服務授權參考中的 [Amazon Security Lake 定義的動作](#)。

## Security Lake 的服務角色

支援服務角色：否

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 [《IAM 使用者指南》](#) 中的 [建立角色以委派許可權給 AWS 服務](#)。

Security Lake 不會擔任或使用服務角色。不過，當您使用 Security Lake 時 AWS Lambda，Amazon EventBridge 和 Amazon S3 等相關服務會擔任服務角色。若要代表您執行動作，Security Lake 會使用服務連結角色。

### ⚠ Warning

變更服務角色的許可可能會在您使用 Security Lake 時產生操作問題。只有在 Security Lake 提供指引時，才能編輯服務角色。

## Security Lake 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Security Lake 使用名為的 IAM 服務連結角

色AWSServiceRoleForAmazonSecurityLake。Security Lake 服務連結角色會授予許可，以代表客戶操作安全資料湖服務。此服務連結角色是直接連結至 Security Lake 的 IAM 角色。它由 Security Lake 預先定義，並包含 Security Lake AWS 服務代表您呼叫其他所需的所有許可。Security Lake 會在提供 AWS 區域 Security Lake 的所有中使用此服務連結角色。

如需建立或管理 Security Lake 服務連結角色的詳細資訊，請參閱 [使用 Security Lake 的服務連結角色](#)。

## Security Lake 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Security Lake 資源的許可。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的 [建立 IAM 政策 \(主控台\)](#)。

如需 Security Lake 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的 [Amazon Security Lake 的動作、資源和條件索引鍵](#)。

主題

- [政策最佳實務](#)
- [使用 Security Lake 主控台](#)

- [範例：允許使用者檢視他們自己的許可](#)
- [範例：允許組織管理帳戶指定和移除委派管理員](#)
- [範例：允許使用者根據標籤檢閱訂閱者](#)

## 政策最佳實務

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Security Lake 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA)：如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》 [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_mfa\\_configure-api-require.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html) 中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 [IAM 安全最佳實務](#)。

## 使用 Security Lake 主控台

若要存取 Amazon Security Lake 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中 Security Lake 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 AWS API 進行呼叫的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色可以使用 Security Lake 主控台，請建立 IAM 政策來為其提供主控台存取權。如需詳細資訊，請參閱 [《IAM 使用者指南》中的 IAM 身分](#)。

如果您建立的政策允許使用者或角色使用 Security Lake 主控台，請確定政策包含這些使用者或角色在主控台上存取所需的資源的適當動作。否則，他們將無法在主控台上導覽或顯示這些資源的詳細資訊。

例如，若要使用主控台新增自訂來源，必須允許使用者執行這些動作：

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

### 範例：允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台上完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

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

```

### 範例：允許組織管理帳戶指定和移除委派管理員

此範例說明如何建立政策，允許 AWS Organizations 管理帳戶的使用者為其組織指定和移除委派的 Security Lake 管理員。

```

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

```

```
}
```

## 範例：允許使用者根據標籤檢閱訂閱者

在以身分為基礎的政策中，您可以使用條件來根據標籤控制對 Security Lake 資源的存取。此範例示範如何建立政策，允許使用者使用 Security Lake 主控台或 Security Lake API 來檢閱訂閱者。不過，只有在訂閱者的 Owner 標籤值為使用者的使用者名稱時，才會授予許可。

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

在此範例中，如果擁有使用者名稱的使用者 richard-roe 嘗試檢閱個別訂閱者的詳細資訊，則訂閱者必須加上標籤 Owner=richard-roe 或 owner=richard-roe。否則，便會拒絕該使用者存取。條件標籤金鑰 Owner 符合 Owner 和 owner，因為條件金鑰名稱不區分大小寫。如需使用條件索引鍵的詳細資訊，請參閱 [《IAM 使用者指南》中的 IAM JSON 政策元素：條件](#)。如需標記 Security Lake 資源的相關資訊，請參閱 [標記 Security Lake 資源](#)。

## AWS Security Lake 的 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新受 AWS 管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的[AWS 受管政策](#)。

## AWS 受管政策：AmazonSecurityLakeMetastoreManager

Amazon Security Lake 使用 AWS Lambda 函數來管理資料湖中的中繼資料。透過使用此函數，Security Lake 可以將包含您的資料和資料檔案的 Amazon Simple Storage Service (Amazon S3) 分割區索引至 AWS Glue Data Catalog 資料表。此受管政策包含 Lambda 函數將 S3 分割區和資料檔案索引到 AWS Glue 資料表的所有許可。

### 許可詳細資訊

此政策包含以下許可：

- logs – 允許主體將 Lambda 函數的輸出記錄到 Amazon CloudWatch Logs。
- glue – 允許主體執行 AWS Glue Data Catalog 資料表的特定寫入動作。這也允許 AWS Glue 爬蟲程式識別資料中的分割區。
- sqs – 允許主體為 Amazon SQS 佇列執行特定的讀取和寫入動作，這些佇列會在資料湖中新增或更新物件時傳送事件通知。
- s3 – 允許主體為包含您資料的 Amazon S3 儲存貯體執行特定的讀取和寫入動作。

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

```

    "logs:CreateLogStream",
    "logs:PutLogEvents",
    "logs:CreateLogGroup"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
    "arn:aws:logs:*:*/aws/lambda/AmazonSecurityLake*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "AllowGlueManage",
  "Effect": "Allow",
  "Action": [
    "glue:CreatePartition",
    "glue:BatchCreatePartition",
    "glue:GetTable",
    "glue:UpdateTable"
  ],
  "Resource": [
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "AllowToReadFromSqs",
  "Effect": "Allow",
  "Action": [
    "sqs:ReceiveMessage",
    "sqs:DeleteMessage",
    "sqs:GetQueueAttributes"
  ],
  "Resource": [
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ]
}

```

```
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "AllowMetaDataReadWrite",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::aws-security-data-lake*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  }
},
{
  "Sid": "AllowMetaDataCleanup",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteObject"
  ],
  "Resource": [
    "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
    "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
}
]
}
```

## AWS 受管政策 : AmazonSecurityLakePermissionsBoundary

Amazon Security Lake 會為第三方自訂來源建立 IAM 角色，以將資料寫入資料湖，並為第三方自訂訂閱者建立來自資料湖的資料，並在建立這些角色時使用此政策來定義其許可界限。您不需要採取動作即可使用此政策。如果使用客戶受管 AWS KMS 金鑰加密資料湖，`kms:Decrypt`則會新增 `kms:GenerateDataKey` 許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsForSecurityLake",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs>DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsForSecurityLake",
      "Effect": "Deny",
      "NotAction": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",

```

```

    "kms:GenerateDataKey",
    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "Resource": "*"
},
{
  "Sid": "DenyActionsNotOnSecurityLakeBucket",
  "Effect": "Deny",
  "Action": [
    "s3:GetObject",
    "s3:GetObjectVersion",
    "s3:ListBucket",
    "s3:ListBucketVersions",
    "s3:PutObject",
    "s3:GetBucketLocation"
  ],
  "NotResource": [
    "arn:aws:s3:::aws-security-data-lake*"
  ]
},
{
  "Sid": "DenyActionsNotOnSecurityLakeSQS",
  "Effect": "Deny",
  "Action": [
    "sqs:ReceiveMessage",
    "sqs:ChangeMessageVisibility",
    "sqs>DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues"
  ],
  "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
},
{
  "Sid": "DenyActionsNotOnSecurityLakeKMSS3SQS",
  "Effect": "Deny",
  "Action": [

```

```

    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotLike": {
      "kms:ViaService": [
        "s3.*.amazonaws.com",
        "sqs.*.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "DenyActionsNotOnSecurityLakeKMSForS3",
  "Effect": "Deny",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:s3:arn": "false"
    },
    "StringNotLikeIfExists": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    }
  }
},
{
  "Sid": "DenyActionsNotOnSecurityLakeKMSForS3SQS",
  "Effect": "Deny",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:sqs:arn": "false"
    }
  },

```

```
    "StringNotLikeIfExists": {
      "kms:EncryptionContext:aws:sqs:arn": [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ]
    }
  }
}
```

## AWS 受管政策：AmazonSecurityLakeAdministrator

您可以在主體為其帳戶啟用 Amazon Security Lake 之前，將 AmazonSecurityLakeAdministrator 政策連接至主體。此政策授予管理許可，允許主體完整存取所有 Security Lake 動作。然後，委託人可以加入 Security Lake，然後在 Security Lake 中設定來源和訂閱者。

此政策包含 Security Lake 管理員可以透過 Security Lake 在其他 AWS 服務上執行的動作。

此 AmazonSecurityLakeAdministrator 政策不支援建立 Security Lake 所需的公用程式角色，以管理 Amazon S3 跨區域複寫、在中註冊新資料分割區 AWS Glue、對新增至自訂來源的資料執行 Glue 爬蟲程式，或通知 HTTPS 端點訂閱者新資料。您可以事先建立這些角色，如中所述 [Amazon Security Lake 入門](#)。

除了 AmazonSecurityLakeAdministrator 受管政策之外，Security Lake 需要加入和組態函數的 lakeformation:PutDataLakeSettings 許可。PutDataLakeSettings 允許將 IAM 主體設定為帳戶中所有區域 Lake Formation 資源的管理員。此角色必須具有 iam:CreateRole permission 和 AmazonSecurityLakeAdministrator 政策。

Lake Formation 管理員可以完整存取 Lake Formation 主控台，並控制初始資料組態和存取許可。Security Lake 會將啟用 Security Lake 和 AmazonSecurityLakeMetaStoreManager 角色（或其他指定角色）的主體指派為 Lake Formation 管理員，以便他們可以建立資料表、更新資料表結構描述、註冊新的分割區，以及設定資料表的許可。您必須在 Security Lake 管理員使用者或角色的政策中包含下列許可：

### Note

為了提供足夠的許可來授予 Lake Formation 型訂閱者存取權，Security Lake 建議新增下列 glue:PutResourcePolicy 許可。

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

## 許可詳細資訊

此政策包含以下許可。

- securitylake – 允許主體完整存取所有 Security Lake 動作。
- organizations – 允許主體從 AWS Organizations 擷取有關組織中帳戶的資訊。如果帳戶屬於組織，則這些許可允許 Security Lake 主控台顯示帳戶名稱和帳戶號碼。

- iam – 允許主體為 Security Lake、AWS Lake Formation 和 建立服務連結角色 Amazon EventBridge，做為啟用這些服務的必要步驟。也允許建立和編輯訂閱者和自訂來源角色的政策，這些角色的許可僅限於 AmazonSecurityLakePermissionsBoundary 政策允許的許可。
- ram – 允許主體設定訂閱者對 Security Lake 來源的 Lake Formation 查詢存取。
- s3 – 允許主體建立和管理 Security Lake 儲存貯體，並讀取這些儲存貯體的內容。
- lambda – 允許主體管理 Lambda 用於在 AWS 來源交付和跨區域複寫之後更新 AWS Glue 資料表分割區的。
- glue – 允許主體建立和管理 Security Lake 資料庫和資料表。
- lakeformation – 允許主體管理 Security Lake 資料表的 Lake Formation 許可。
- events – 允許主體管理用來通知訂閱者 Security Lake 來源中新資料的規則。
- sqs – 允許主體建立和管理用於通知訂閱者 Security Lake 來源中新資料的 Amazon SQS 佇列。
- kms – 允許主體授予 Security Lake 使用客戶受管金鑰寫入資料的存取權。
- secretsmanager – 允許主體管理用來透過 HTTPS 端點通知訂閱者 Security Lake 來源中新資料的秘密。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsWithAnyResource",
      "Effect": "Allow",
      "Action": [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect": "Allow",
      "Action": [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",

```

```
    "lambda:CreateEventSourceMapping",
    "lakeformation:GrantPermissions",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "lakeformation:GetDataLakeSettings",
    "events:ListConnections",
    "events:ListApiDestinations",
    "iam:GetRole",
    "iam:ListAttachedRolePolicies",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowManagingSecurityLakeS3Buckets",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketNotification",
    "s3:PutBucketTagging",
    "s3:PutEncryptionConfiguration",
    "s3:PutBucketVersioning",
    "s3:PutReplicationConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetBucketNotification"
  ],
  "Resource": "arn:aws:s3::aws-security-data-lake*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
```

```
"Sid": "AllowLambdaCreateFunction",
"Effect": "Allow",
"Action": [
  "lambda:CreateFunction"
],
"Resource": [
  "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
  "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
],
"Condition": {
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": "securitylake.amazonaws.com"
  }
}
},
{
  "Sid": "AllowLambdaAddPermission",
  "Effect": "Allow",
  "Action": [
    "lambda:AddPermission"
  ],
  "Resource": [
    "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
    "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    },
    "StringEquals": {
      "lambda:Principal": "securitylake.amazonaws.com"
    }
  }
}
},
{
  "Sid": "AllowGlueActions",
  "Effect": "Allow",
  "Action": [
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "glue:CreateTable",
    "glue:GetTable"
  ],
  "Resource": [
```

```

    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowEventBridgeActions",
  "Effect": "Allow",
  "Action": [
    "events:PutTargets",
    "events:PutRule",
    "events:DescribeRule",
    "events:CreateApiDestination",
    "events:CreateConnection",
    "events:UpdateConnection",
    "events:UpdateApiDestination",
    "events>DeleteConnection",
    "events>DeleteApiDestination",
    "events:ListTargetsByRule",
    "events:RemoveTargets",
    "events>DeleteRule"
  ],
  "Resource": [
    "arn:aws:events:*:*:rule/AmazonSecurityLake*",
    "arn:aws:events:*:*:rule/SecurityLake*",
    "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
    "arn:aws:events:*:*:connection/AmazonSecurityLake*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowSQSActions",
  "Effect": "Allow",
  "Action": [
    "sqs:CreateQueue",

```

```

    "sqs:SetQueueAttributes",
    "sqs:GetQueueURL",
    "sqs:AddPermission",
    "sqs:GetQueueAttributes",
    "sqs>DeleteQueue"
  ],
  "Resource": [
    "arn:aws:sqs:*:*:SecurityLake*",
    "arn:aws:sqs:*:*:AmazonSecurityLake*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowKmsCmkGrantForSecurityLake",
  "Effect": "Allow",
  "Action": "kms:CreateGrant",
  "Resource": "arn:aws:kms:*:*:key/*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::aws-security-data-lake*"
    },
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "GenerateDataKey",
        "RetireGrant",
        "Decrypt"
      ]
    }
  }
},
{
  "Sid": "AllowEnablingQueryBasedSubscribers",
  "Effect": "Allow",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ]
},

```

```

"Resource": "*",
"Condition": {
  "StringLikeIfExists": {
    "ram:ResourceArn": [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ]
  },
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": "securitylake.amazonaws.com"
  }
},
{
  "Sid": "AllowConfiguringQueryBasedSubscribers",
  "Effect": "Allow",
  "Action": [
    "ram:UpdateResourceShare",
    "ram:GetResourceShares",
    "ram:DisassociateResourceShare",
    "ram>DeleteResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "ram:ResourceShareName": "LakeFormation*"
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowConfiguringCredentialsForSubscriberNotification",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:CreateSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:PutSecretValue"
  ],
  "Resource": "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
  "Condition": {

```

```

    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": [
          "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
          "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
      }
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
}

```

```

},
{
  "Sid": "AllowPassRoleForCrossRegionReplicationSecLakeArn",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "s3.amazonaws.com"
    },
    "StringLike": {
      "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
    }
  }
},
{
  "Sid": "AllowPassRoleForCrossRegionReplicationS3Arn",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "s3.amazonaws.com"
    },
    "StringLike": {
      "iam:AssociatedResourceARN": "arn:aws:s3:::aws-security-data-lake*"
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeCustomDataGlueCrawler*",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "glue.amazonaws.com"
    },
    "StringLike": {
      "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
    }
  }
}

```

```
    }
  }
},
{
  "Sid": "AllowPassRoleForCustomSourceCrawlerGlueArn",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "glue.amazonaws.com"
    },
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "securitylake.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowPassRoleForSubscriberNotificationSecLakeArn",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "events.amazonaws.com"
    },
    "StringLike": {
      "iam:AssociatedResourceARN": "arn:aws:securitylake::*:subscriber/*"
    }
  }
},
{
  "Sid": "AllowPassRoleForSubscriberNotificationEventsArn",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "events.amazonaws.com"
    },
    "StringLike": {
```

```

    "iam:AssociatedResourceARN": "arn:aws:events:*:*:rule/AmazonSecurityLake*"
  },
  "ForAnyValue:StringEquals": {
    "aws:CalledVia": "securitylake.amazonaws.com"
  }
},
{
  "Sid": "AllowOnboardingToSecurityLakeDependencies",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": [
    "arn:aws:iam:*:*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
    "arn:aws:iam:*:*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "arn:aws:iam:*:*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
  ],
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": [
        "securitylake.amazonaws.com",
        "lakeformation.amazonaws.com",
        "apidestinations.events.amazonaws.com"
      ]
    }
  }
},
{
  "Sid": "AllowRolePolicyActionsforSubscribersandSources",
  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam:*:*:role/AmazonSecurityLake*",
  "Condition": {
    "StringEquals": {
      "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
    }
  },
  "ForAnyValue:StringEquals": {

```

```

        "aws:CalledVia": "securitylake.amazonaws.com"
    }
}
},
{
    "Sid": "AllowRegisterS3LocationInLakeFormation",
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "securitylake.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowIAMActionsByResource",
    "Effect": "Allow",
    "Action": [
        "iam:ListRolePolicies",
        "iam>DeleteRole"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "securitylake.amazonaws.com"
        }
    }
},
{
    "Sid": "S3ReadAccessToSecurityLakes",
    "Effect": "Allow",
    "Action": [
        "s3:Get*",
        "s3:List*"
    ],
    "Resource": "arn:aws:s3::aws-security-data-lake-*"
},
{
    "Sid": "S3ReadAccessToSecurityLakeMetastoreObject",

```

```
"Effect": "Allow",
"Action": [
  "s3:GetObject",
  "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::security-lake-meta-store-manager-*"
},
{
  "Sid": "S3ResourcelessReadOnly",
  "Effect": "Allow",
  "Action": [
    "s3:GetAccountPublicAccessBlock",
    "s3:ListAccessPoints",
    "s3:ListAllMyBuckets"
  ],
  "Resource": "*"
}
]
```

## AWS 受管政策：SecurityLakeServiceLinkedRole

Security Lake 使用名為 `的`服務連結角色 `AWSServiceRoleForSecurityLake` 來建立和操作安全資料湖。

您無法將 `SecurityLakeServiceLinkedRole` 受管政策連接至 IAM 實體。此政策會連接到服務連結角色，允許 Security Lake 代表您執行動作。如需詳細資訊，請參閱 [Security Lake 的服務連結角色許可](#)。

## AWS 受管政策：SecurityLakeResourceManagementServiceRolePolicy

Security Lake 使用名為 `的`服務連結角色 `AWSServiceRoleForSecurityLakeResourceManagement` 來執行持續的監控和效能改善，進而降低延遲和成本。

您無法將 `SecurityLakeResourceManagementServiceRolePolicy` 受管政策連接至 IAM 實體。此政策會連接到服務連結角色，允許 Security Lake 代表您執行動作。如需詳細資訊，請參閱 [資源管理的服務連結角色許可](#)。

## AWS 受管政策：AWS GlueServiceRole

AWS GlueServiceRole 受管政策會叫用 AWS Glue 爬蟲程式，並允許 AWS Glue 爬取自訂來源資料並識別分割區中繼資料。在 Data Catalog 中建立和更新資料表時，需要此中繼資料。

如需詳細資訊，請參閱從 [Security Lake 中的自訂來源收集資料](#)。

## AWS 受管政策的安全湖更新

檢視自此服務開始追蹤這些變更以來，Security Lake AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 Security Lake 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
<a href="#">Amazon Security Lake 的服務連結角色</a> – 新的服務連結角色	我們新增了新的服務連結角色 AWSServiceRoleForSecurityLakeResourceManagement。此服務連結角色提供 Security Lake 執行持續監控和效能改善的許可，進而降低延遲和成本。	2024 年 11 月 14 日
<a href="#">Amazon Security Lake 的服務連結角色</a> – 更新至現有的服務連結角色許可	我們已將 AWS WAF 動作新增至政策的 AWS 受管 SecurityLakeServiceLinkedRole 政策。其他動作允許 Security Lake AWS WAF 在 Security Lake 中啟用日誌來源時收集日誌。	2024 年 5 月 22 日
<a href="#">AmazonSecurityLakePermissionsBoundary</a> – 更新現有政策	Security Lake 已將 SID 動作新增至政策。	2024 年 5 月 13 日
<a href="#">AmazonSecurityLakeMetastoreManager</a> – 更新現有政策	Security Lake 已更新政策，新增中繼資料清除動作，可讓您刪除資料湖中的中繼資料。	2024 年 3 月 27 日

變更	描述	日期
<a href="#">AmazonSecurityLakeAdministrator</a> – 更新現有政策	Security Lake 已更新政策，以允許新AmazonSecurityLakeMetastoreManagerV2 角色iam:PassRole，並讓 Security Lake 部署或更新資料湖元件。	2024 年 2 月 23 日
<a href="#">AmazonSecurityLakeMetastoreManager</a> – 新政策	Security Lake 新增了新的受管政策，授予 Security Lake 管理資料湖中中繼資料的許可。	2024 年 1 月 23 日
<a href="#">AmazonSecurityLakeAdministrator</a> – 新政策	Security Lake 新增了新的受管政策，授予委託人對所有 Security Lake 動作的完整存取權。	2023 年 5 月 30 日
Security Lake 開始追蹤變更	Security Lake 開始追蹤其 AWS 受管政策的變更。	2022 年 11 月 29 日

## 使用 Security Lake 的服務連結角色

Security Lake 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 Security Lake 的 IAM 角色。它由 Security Lake 預先定義，其中包含 Security Lake 代表您呼叫其他 AWS 服務並操作安全資料湖服務所需的所有許可。Security Lake 會在可使用 AWS 區域 Security Lake 的所有 中使用此服務連結角色。

服務連結角色不需要在設定 Security Lake 時手動新增必要的許可。Security Lake 定義此服務連結角色的許可，除非另有定義，否則只有 Security Lake 可以擔任該角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [服務連結角色許可](#)。只有在刪除其相關資源之後，您才能刪除服務連結角色。這可保護您的資源，避免您不小心移除資源的存取許可。

如需有關支援服務連結角色的其他服務的資訊，請參閱[AWS 使用 IAM 的服務](#)，並在服務連結角色欄中尋找具有是的服務。選擇有連結的是，以檢閱該服務的服務連結角色文件。

## 主題

- [Security Lake 的服務連結角色 \(SLR\) 許可](#)
- [資源管理的服務連結角色 \(SLR\) 許可](#)

## Security Lake 的服務連結角色 (SLR) 許可

Security Lake 使用名為的服務連結角色AWSServiceRoleForSecurityLake。此服務連結角色信任securitylake.amazonaws.com服務擔任該角色。如需 Amazon Security Lake 受 AWS 管政策的詳細資訊，請參閱 [AWS Amazon Security Lake 的管理政策](#)。

角色的許可政策是名為的 AWS 受管政策SecurityLakeServiceLinkedRole，可讓 Security Lake 建立和操作安全資料湖。它還允許 Security Lake 對指定的資源執行如下任務：

- 使用 AWS Organizations 動作來擷取關聯帳戶的相關資訊
- 使用 Amazon Elastic Compute Cloud (Amazon EC2) 擷取 Amazon VPC 流程日誌的相關資訊
- 使用 AWS CloudTrail 動作來擷取服務連結角色的相關資訊
- 在 Security Lake 中啟用 AWS WAF 日誌來源時，使用 AWS WAF 動作來收集日誌
- 使用 LogDelivery動作來建立或刪除 AWS WAF 日誌交付訂閱。

角色已設定下列許可政策：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "OrganizationsPolicies",
    "Effect": "Allow",
    "Action": [
      "organizations:ListAccounts",
      "organizations:DescribeOrganization"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Sid": "DescribeOrgAccounts",
```

```

    "Effect": "Allow",
    "Action": [
      "organizations:DescribeAccount"
    ],
    "Resource": [
      "arn:aws:organizations::*:account/o-*/*"
    ]
  },
  {
    "Sid": "AllowManagementOfServiceLinkedChannel",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:CreateServiceLinkedChannel",
      "cloudtrail>DeleteServiceLinkedChannel",
      "cloudtrail:GetServiceLinkedChannel",
      "cloudtrail:UpdateServiceLinkedChannel"
    ],
    "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
  },
  {
    "Sid": "AllowListServiceLinkedChannel",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DescribeAnyVpc",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeVpcs"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ListDelegatedAdmins",
    "Effect": "Allow",
    "Action": [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {

```

```

        "StringEquals": {
            "organizations:ServicePrincipal": "securitylake.amazonaws.com"
        }
    },
    {
        "Sid": "AllowWafLoggingConfiguration",
        "Effect": "Allow",
        "Action": [
            "wafv2:PutLoggingConfiguration",
            "wafv2:GetLoggingConfiguration",
            "wafv2:ListLoggingConfigurations",
            "wafv2>DeleteLoggingConfiguration"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "wafv2:LogScope": "SecurityLake"
            }
        }
    },
    {
        "Sid": "AllowPutLoggingConfiguration",
        "Effect": "Allow",
        "Action": [
            "wafv2:PutLoggingConfiguration"
        ],
        "Resource": "*",
        "Condition": {
            "ArnLike": {
                "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-
security-lake-*"
            }
        }
    },
    {
        "Sid": "ListWebACLs",
        "Effect": "Allow",
        "Action": [
            "wafv2:ListWebACLs"
        ],
        "Resource": "*"
    },
    {

```

```
    "Sid": "LogDelivery",
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "wafv2.amazonaws.com"
            ]
        }
    }
}
]
```

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的[服務連結角色許可](#)。

### 建立 Security Lake 服務連結角色

您不需要手動建立 Security Lake `AWSServiceRoleForSecurityLake` 的服務連結角色。當您為 啟用 Security Lake 時 AWS 帳戶，Security Lake 會自動為您建立服務連結角色。

### 編輯 Security Lake 服務連結角色

Security Lake 不允許您編輯 `AWSServiceRoleForSecurityLake` 服務連結角色。建立服務連結角色之後，您無法變更角色的名稱，因為各種實體可能會參考角色。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱「[IAM 使用者指南](#)」的編輯服務連結角色。

### 刪除 Security Lake 服務連結角色

您無法從 Security Lake 刪除服務連結角色。反之，您可以從 IAM 主控台、API 或刪除服務連結角色 AWS CLI。如需詳細資訊，請參閱「[IAM 使用者指南](#)」中的[刪除服務連結角色](#)。

您必須先確認角色沒有作用中的工作階段，並移除 `AWSServiceRoleForSecurityLake` 正在使用的任何資源，才能刪除服務連結角色。

**Note**

如果 Security Lake 在您嘗試刪除資源時正在使用 `AWSServiceRoleForSecurityLake` 角色，刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試操作。

如果您刪除 `AWSServiceRoleForSecurityLake` 服務連結角色並需要再次建立，您可以透過為您的帳戶啟用 Security Lake 來再次建立該角色。當您再次啟用 Security Lake 時，Security Lake 會自動再次為您建立服務連結角色。

## AWS 區域 支援 Security Lake 服務連結角色

Security Lake 支援在可使用 AWS 區域 Security Lake 的所有中使用 `AWSServiceRoleForSecurityLake` 服務連結角色。如需目前可使用 Security Lake 的區域清單，請參閱 [Security Lake 區域和端點](#)。

## 資源管理的服務連結角色 (SLR) 許可

Security Lake 使用名為 `AWSServiceRoleForSecurityLakeResourceManagement` 的服務連結角色來執行持續的監控和效能改善，進而降低延遲和成本。此服務連結角色信任 `resource-management.securitylake.amazonaws.com` 服務擔任該角色。啟用 `AWSServiceRoleForSecurityLakeResourceManagement` 也會授予其對 Lake Formation 的存取權，並自動向所有區域的 Lake Formation 註冊您的 Security Lake 受管 S3 儲存貯體，以提高安全性。

角色的許可政策是名為 `SecurityLakeResourceManagementServiceRolePolicy` 的 AWS 受管政策，允許存取來管理 Security Lake 建立的資源，包括管理資料湖中的中繼資料。如需 Amazon Security Lake 受 AWS 管政策的詳細資訊，請參閱 [AWS Amazon Security Lake 的受管政策](#)。

此服務連結角色可讓 Security Lake 監控 Security Lake (S3 儲存貯體、AWS Glue 資料表、Amazon SQS 佇列、中繼存放區管理員 (MSM) Lambda 函數和 EventBridge 規則) 部署的資源的運作狀態。Security Lake 可以使用此服務連結角色執行的一些操作範例如下：

- Apache Iceberg 資訊清單檔案壓縮，可改善查詢效能並降低 Lambda MSM 處理時間和成本。
- 監控 Amazon SQS 的狀態，以偵測擷取問題。
- 最佳化跨區域資料複寫以排除中繼資料檔案。

**Note**

如果您未安裝 `AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色，Security Lake 將繼續運作，但強烈建議您接受此服務連結角色，以便 Security Lake 可以監控和最佳化您帳戶中的資源。

**許可詳細資訊**

角色已設定下列許可政策：

- `events` – 允許主體管理日誌來源和日誌訂閱者所需的 EventBridge 規則。
- `lambda` – 允許主體管理用於在 AWS 來源交付和跨區域複寫之後更新 AWS Glue 資料表分割區的 `lambda`。
- `glue` – 允許主體執行 AWS Glue Data Catalog 資料表的特定寫入動作。這還允許 AWS Glue 爬蟲程式識別資料中的分割區，並允許 Security Lake 管理 Apache Iceberg 資料表的 Apache Iceberg 中繼資料。
- `s3` – 允許主體在包含日誌資料和 Glue 資料表中繼資料的 Security Lake 儲存貯體上執行特定的讀取和寫入動作。
- `logs` – 允許主體讀取存取權，將 Lambda 函數的輸出記錄到 CloudWatch Logs。
- `sqs` – 允許主體對 Amazon SQS 佇列執行特定的讀取和寫入動作，這些佇列會在資料湖中新增或更新物件時接收事件通知。
- `lakeformation` – 允許主體讀取 Lake Formation 設定，以監控組態錯誤。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadEventBridgeRules",
      "Effect": "Allow",
      "Action": [
        "events:ListRules"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```

        "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
}
},
{
    "Sid": "ManageSecurityLakeEventRules",
    "Effect": "Allow",
    "Action": [
        "events:PutRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "ManageSecurityLakeLambdaConfigurations",
    "Effect": "Allow",
    "Action": [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda>DeleteFunctionConcurrency",
        "lambda>DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
    ],
    "Resource": [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
}

```

```

    }
  },
  {
    "Sid": "AllowListLambdaEventSourceMappings",
    "Effect": "Allow",
    "Action": [
      "lambda:ListEventSourceMappings"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "AllowUpdateLambdaEventSourceMapping",
    "Effect": "Allow",
    "Action": [
      "lambda:UpdateEventSourceMapping"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      },
      "StringLike": {
        "lambda:FunctionArn":
"arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      }
    }
  },
  {
    "Sid": "AllowUpdateLambdaConfigs",
    "Effect": "Allow",
    "Action": [
      "lambda:UpdateFunctionConfiguration"
    ],
    "Resource": "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  }
}

```

```

},
{
  "Sid": "ManageSecurityLakeGlueResources",
  "Effect": "Allow",
  "Action": [
    "glue:CreatePartition",
    "glue:BatchCreatePartition",
    "glue:GetTable",
    "glue:GetTables",
    "glue:UpdateTable",
    "glue:GetDatabase"
  ],
  "Resource": [
    "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/**",
    "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
    "arn:aws:glue:*:*:catalog"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "AllowDataLakeConfigurationManagement",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:PutObject",
    "s3:GetObjectAttributes",
    "s3:GetBucketNotification",
    "s3:PutBucketNotification",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:GetEncryptionConfiguration",
    "s3:GetReplicationConfiguration"
  ],
  "Resource": [
    "arn:aws:s3:::aws-security-data-lake*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
}

```

```

    }
  },
  {
    "Sid": "AllowMetaDataCompactionAndManagement",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:DeleteObject",
      "s3:RestoreObject"
    ],
    "Resource": [
      "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
      "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "ReadSecurityLakeLambdaLogs",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogStreams",
      "logs:StartQuery",
      "logs:GetLogEvents",
      "logs:GetQueryResults",
      "logs:GetLogRecord"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  },
  {
    "Sid": "ManageSecurityLakeSQSQueue",
    "Effect": "Allow",
    "Action": [
      "sqs:StartMessageMoveTask",

```

```

    "sqs:DeleteMessage",
    "sqs:GetQueueUrl",
    "sqs:ListDeadLetterSourceQueues",
    "sqs:ChangeMessageVisibility",
    "sqs:ListMessageMoveTasks",
    "sqs:ReceiveMessage",
    "sqs:SendMessage",
    "sqs:GetQueueAttributes",
    "sqs:SetQueueAttributes"
  ],
  "Resource": [
    "arn:aws:sqs:*:*:SecurityLake_*",
    "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
},
{
  "Sid": "AllowDataLakeManagement",
  "Effect": "Allow",
  "Action": [
    "lakeformation:GetDataLakeSettings",
    "lakeformation:ListPermissions"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
  }
}
]
}

```

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [服務連結角色許可](#)。

## 建立 Security Lake 服務連結角色

您可以使用 Security Lake 主控台或 為 Security Lake 建立 `AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色 AWS CLI。

若要建立服務連結角色，您必須將下列許可授予 IAM 使用者或 IAM 角色。IAM 角色必須是所有啟用 Security Lake 的區域中的 Lake Formation 管理員。

```
{
  "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 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 在摘要頁面上的資訊列中按一下啟用服務連結角色，以接受新的服務連結角色。

啟用服務連結角色之後，就不需要重複此程序，以供日後使用 Security Lake。

## CLI

若要以程式設計方式建立 `AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色，請使用下列 CLI 命令。

```

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

```

使用 `建立AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色時 AWS CLI，您還必須將 Lake Formation 資料表層級許可 (ALTER、DESCRIBE) 授予 Security Lake Glue

資料庫上的所有資料表，以管理資料表中繼資料和存取資料。如果任何區域中的 Glue 資料表參考先前 Security Lake 啟用的 S3 儲存貯體，您必須暫時允許 DATA\_LOCATION\_ACCESS 許可給服務連結角色，以允許 Security Lake 修復這種情況。

您也必須將 Lake Formation 許可授予您帳戶的 `AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色。

下列範例顯示如何將 Lake Formation 許可授予指定區域中的服務連結角色。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws lakeformation grant-permissions --region {region} --principal
DataLakePrincipalIdentifier={AWSServiceRoleForSecurityLakeResourceManagement ARN} \
--permissions ALTER DESCRIBE --resource '{ "Table": { "DatabaseName":
"amazon_security_lake_glue_db_{region}", "TableWildcard": {} } }'
```

下列範例顯示角色 ARN 的外觀。您必須編輯角色 ARN 以符合您的區域。

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

您也可以使用 [CreateServiceLinkedRole](#) API 呼叫。在請求中，將指定 `AWSServiceName` 為 `resource-management.securitylake.amazonaws.com`。

啟用 `AWSServiceRoleForSecurityLakeResourceManagement` 角色之後，如果您使用 AWS KMS 客戶受管金鑰 (CMK) 進行加密，則必須允許服務連結角色將加密的物件寫入 CMK 存在的 AWS 區域中的 S3 儲存貯體。在 AWS KMS 主控台中，將下列政策新增至 CMK 存在的 AWS 區域中的 KMS 金鑰。如需如何變更 KMS 金鑰政策的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的 [中的金鑰政策 AWS KMS](#)。

```
{
  "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"
      }
    }
  },
},
```

## 編輯 Security Lake 服務連結角色

Security Lake 不允許您編輯 `AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色。建立服務連結角色之後，您無法變更角色的名稱，因為各種實體可能會參考角色。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 [「IAM 使用者指南」](#) 的編輯服務連結角色。

## 刪除 Security Lake 服務連結角色

您無法從 Security Lake 刪除服務連結角色。反之，您可以從 IAM 主控台、API 或刪除服務連結角色 AWS CLI。如需詳細資訊，請參閱 [「IAM 使用者指南」](#) 中的 [刪除服務連結角色](#)。

您必須先確認角色沒有作用中的工作階段，並移

除 `AWSServiceRoleForSecurityLakeResourceManagement` 正在使用的任何資源，才能刪除服務連結角色。

### Note

如果 Security Lake 在您嘗試刪除資源時正在使用 `AWSServiceRoleForSecurityLakeResourceManagement` 角色，刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試操作。

如果您刪除 `AWSServiceRoleForSecurityLakeResourceManagement` 服務連結角色並需要再次建立，您可以透過為您的帳戶啟用 Security Lake 來再次建立該角色。當您再次啟用 Security Lake 時，Security Lake 會自動再次為您建立服務連結角色。

## AWS 區域 支援 Security Lake 服務連結角色

Security Lake 支援在可使用 AWS 區域 Security Lake 的所有 中使  
用AWSServiceRoleForSecurityLakeResourceManagement服務連結角色。如需目前可使用  
Security Lake 的區域清單，請參閱 [Security Lake 區域和端點](#)。

## Amazon Security Lake 中的資料保護

AWS [共同責任模型](#)適用於 Amazon Security Lake 中的資料保護。如此模型所述，AWS 負責保護執行所有的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 [AWS 共同的責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Security Lake 或其他 AWS 服務 主控台、API AWS CLI或 AWS SDKs時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

## 靜態加密

Amazon Security Lake 使用 AWS 加密解決方案安全地存放靜態資料。原始安全日誌和事件資料存放在 Security Lake 管理的帳戶中的來源特定[多租用戶 Amazon Simple Storage Service \(Amazon S3\) 儲存貯體](#)中。每個日誌來源都有自己的多租用戶儲存貯體。Security Lake 使用來自 AWS Key

Management Service (AWS KMS) 的 [AWS 擁有金鑰](#) 來加密此原始資料。AWS 擁有的金鑰是 AWS 服務擁有和管理用於多個 AWS 帳戶的 AWS KMS 金鑰集合，在此例中為 Security Lake。

Security Lake 會在原始日誌和事件資料上執行擷取、轉換和載入 (ETL) 任務。

ETL 任務完成後，Security Lake 會在您的帳戶中建立單一租用戶 S3 儲存貯體 AWS 區域（您已啟用 Security Lake 的每個儲存貯體各一個）。資料只會暫時存放在多租用戶 S3 儲存貯體中，直到 Security Lake 能夠可靠地將資料交付至單一租用戶 S3 儲存貯體為止。單一租用戶儲存貯體包含以資源為基礎的政策，可讓 Security Lake 將日誌和事件資料寫入儲存貯體。若要加密 S3 儲存貯體中的資料，您可以選擇 [S3-managed 加密金鑰](#) 或 [客戶受管金鑰](#)（來自 AWS KMS）。這兩個選項都使用對稱加密。

## 使用 KMS 金鑰來加密您的資料

依預設，Security Lake 交付至 S3 儲存貯體的資料會由 Amazon 伺服器端加密使用 [Amazon S3-managed 加密金鑰 \(SSE-S3\) 加密](#)。若要提供您直接管理的安全層，您可以改為使用 [伺服器端加密搭配 AWS KMS 金鑰 \(SSE-KMS\)](#) 做為 Security Lake 資料。

Security Lake 主控台不支援 SSE-KMS。若要搭配 Security Lake API 或 CLI 使用 SSE-KMS，請先 [建立 KMS 金鑰](#) 或使用現有金鑰。您可以將政策連接至金鑰，以決定哪些使用者可以使用金鑰來加密和解密 Security Lake 資料。

如果您使用客戶受管金鑰來加密寫入 S3 儲存貯體的資料，則無法選擇多區域金鑰。針對客戶受管金鑰，Security Lake 會透過傳送 CreateGrant 請求至 來代表您建立 [授予](#) AWS KMS。中的授予 AWS KMS 用於授予 Security Lake 存取客戶帳戶中 KMS 金鑰的權限。

Security Lake 需要授予，才能將客戶受管金鑰用於下列內部操作：

- 將 GenerateDataKey 請求傳送至 AWS KMS，以產生由客戶受管金鑰加密的資料金鑰。
- 將 RetireGrant 請求傳送至 AWS KMS。當您更新資料湖時，此操作會讓新增至 AWS KMS 金鑰以進行 ETL 處理的授予淘汰。

Security Lake 不需要 Decrypt 許可。當金鑰的授權使用者讀取 Security Lake 資料時，S3 會管理解密，授權使用者能夠以未加密的形式讀取資料。不過，訂閱者需要 Decrypt 許可才能使用來源資料。如需訂閱者許可的詳細資訊，請參閱 [管理 Security Lake 訂閱者的資料存取](#)。

如果您想要使用現有的 KMS 金鑰來加密 Security Lake 資料，您必須修改 KMS 金鑰的金鑰政策。金鑰政策必須允許與 Lake Formation 資料湖位置相關聯的 IAM 角色使用 KMS 金鑰來解密資料。如需有關如何變更 KMS 金鑰金鑰之金鑰政策的說明，請參閱《AWS Key Management Service 開發人員指南》中的 [變更金鑰政策](#)。

當您建立金鑰政策或使用具有適當許可的現有金鑰政策時，KMS 金鑰可以接受授予請求，允許 Security Lake 存取金鑰。如需建立金鑰政策的說明，請參閱《AWS Key Management Service 開發人員指南》中的[建立金鑰政策](#)。

將下列金鑰政策連接至您的 KMS 金鑰：

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

## 使用客戶受管金鑰時所需的 IAM 許可

如需使用 Security Lake 時需要建立的 IAM 角色概觀，請參閱[入門：先決條件](#)一節。

當您新增自訂來源或訂閱者時，Security Lake 會在您的帳戶中建立 IAM 角色。這些角色旨在與其他 IAM 身分共用。它們允許自訂來源將資料寫入資料湖，並允許訂閱者使用來自資料湖的資料。名為 `AmazonSecurityLakePermissionsBoundary` 的 AWS 受管政策會設定這些角色的許可界限。

## 加密 Amazon SQS 佇列

當您建立資料湖時，Security Lake 會在委派的 Security Lake 管理員帳戶中建立兩個未加密的 Amazon Simple Queue Service (Amazon SQS) 佇列。您應該加密這些佇列來保護您的資料。Amazon Simple Queue Service 提供的預設伺服器端加密 (SSE) 不足。您必須在 AWS Key Management Service (AWS KMS) 中建立客戶受管金鑰，以加密佇列，並授予 Amazon S3 服務主體使用加密佇列的許可。如需授予這些許可的說明，請參閱 AWS 知識中心的[為什麼 Amazon S3 事件通知不會傳送到使用伺服器端加密的 Amazon SQS 佇列？](#)。

由於 Security Lake 使用 AWS Lambda 來支援擷取、傳輸和載入 (ETL) 任務，因此您還必須授予 Lambda 許可，以管理 Amazon SQS 佇列中的訊息。如需詳細資訊，請參閱《AWS Lambda 開發人員指南》中的[執行角色許可](#)。

## 傳輸中加密

Security Lake 會加密 AWS 服務之間傳輸的所有資料。Security Lake 透過使用 Transport Layer Security (TLS) 1.2 加密通訊協定自動加密所有網路間資料，保護傳輸中往返服務的資料。傳送到 Security Lake APIs 直接 HTTPS 請求，是透過使用 [AWS Signature 第 4 版演算法](#) 來建立安全連線來簽署。

## 選擇不使用您的資料以改善服務

您可以使用選擇退出政策，選擇不讓資料用於開發和改善 Security Lake AWS Organizations 和其他 AWS 安全服務。即使 Security Lake 目前未收集任何此類資料，您也可以選擇不接收。如需有關如何選擇退出的詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [AI 服務選擇退出政策](#)。

目前，Security Lake 不會收集其代表您處理的任何安全資料，或您上傳到此服務建立的安全資料湖的安全資料。為了開發和改善 Security Lake 服務和其他 AWS 安全服務的功能，Security Lake 可能會在未來收集此類資料，包括您從第三方資料來源上傳的資料。當 Security Lake 想要收集任何此類資料，並說明其運作方式時，我們將更新此頁面。您仍然有機會隨時選擇退出。

### Note

若要使用選擇退出政策，AWS 您的帳戶必須由 集中管理 AWS Organizations。如果您尚未為 AWS 帳戶建立組織，請參閱 AWS Organizations 《使用者指南》中的 [建立和管理組織](#)。

選擇退出具有以下影響：

- Security Lake 將刪除在您選擇退出之前收集和儲存的資料（如果有的話）。
- 在您選擇退出後，Security Lake 將不再收集或存放此資料。

## Amazon Security Lake 的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱 [AWS 服務 合規計劃範圍內](#) 然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱 [在中下載報告 AWS Artifact](#)。

使用時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- [安全合規與治理](#) - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- [HIPAA 合格服務參考](#) - 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- [AWS 合規資源](#) - 此工作手冊和指南的集合可能適用於您的產業和位置。
- [AWS 客戶合規指南](#) - 透過合規的角度了解共同責任模型。本指南摘要說明保護 的最佳實務，AWS 服務 並將指南映射到跨多個架構的安全控制（包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)）。
- AWS Config 開發人員指南中的 [使用規則評估資源](#) - AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#) - 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「[Security Hub 控制參考](#)」。
- [Amazon GuardDuty](#) - 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- [AWS Audit Manager](#) - 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

## Security Lake 的安全最佳實務

請參閱下列使用 Amazon Security Lake 的最佳實務。

### 授予 Security Lake 使用者最低可能許可

遵循最低權限原則，為您的 AWS Identity and Access Management (IAM) 使用者、使用者群組和角色 授予最低存取政策許可集。例如，您可能允許 IAM 使用者在 Security Lake 中檢視日誌來源清單，但不能建立來源或訂閱者。如需詳細資訊，請參閱 [Security Lake 的身分型政策範例](#)

您也可以使用 AWS CloudTrail 來追蹤 Security Lake 中的 API 用量。CloudTrail 提供使用者、群組或角色在 Security Lake 中採取的 API 動作記錄。如需詳細資訊，請參閱 [使用 CloudTrail 記錄 Security Lake API 呼叫](#)。

### 檢視摘要頁面

Security Lake 主控台的摘要頁面提供過去 14 天的問題概觀，這些問題會影響 Security Lake 服務和存放資料的 Amazon S3 儲存貯體。您可以進一步調查這些問題，以協助您減輕可能的安全相關影響。

## 與 Security Hub 整合

整合 Security Lake 和 AWS Security Hub 以接收 Security Lake 中的 Security Hub 調查結果。Security Hub 會從許多不同的 AWS 服務 第三方整合產生調查結果。接收 Security Hub 調查結果可協助您取得合規狀態的概觀，以及您是否符合 AWS 安全最佳實務。

如需詳細資訊，請參閱[與 整合 AWS Security Hub](#)。

## 刪除 AWS Lambda

刪除函數時，建議您先不要停用該 AWS Lambda 函數。在刪除之前停用 Lambda 函數可能會干擾資料查詢功能，並可能影響其他功能。最好直接刪除 Lambda 函數，而不停用它。如需刪除 Lambda 函數的詳細資訊，請參閱[AWS Lambda 開發人員指南](#)。

## 監控 Security Lake 事件

您可以使用 Amazon CloudWatch 指標來監控 Security Lake。CloudWatch 每分鐘從 Security Lake 收集原始資料，並將其處理為指標。您可以設定警示，在指標符合指定的閾值時觸發通知。

如需詳細資訊，請參閱[Amazon Security Lake 的 CloudWatch 指標](#)。

## Amazon Security Lake 中的彈性

AWS 全域基礎設施是以 AWS 區域 和 可用區域為基礎建置。AWS 區域 提供多個實體分隔和隔離的可用區域，這些區域與低延遲、高輸送量和高備援聯網連接。這些可用區域可讓您有效設計和操作應用程式與資料庫，可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

Security Lake 的可用性與區域可用性相關。跨多個可用區域分佈有助於服務容忍任何單一可用區域中的故障。

Security Lake 資料平面的可用性與任何區域可用性無關。不過，Security Lake 控制平面的可用性與美國東部（維吉尼亞北部）區域的可用性密切相關。

如需 AWS 區域 和 可用區域的詳細資訊，請參閱[AWS 全球基礎設施](#)。

除了 AWS 全球基礎設施之外，Security Lake 還支援 Amazon Simple Storage Service (Amazon S3) 的資料；提供多種功能，可協助支援您的資料彈性和備份需求。

## 生命週期組態

生命週期組態是一組規則，可定義 Amazon S3 套用至一組物件的動作。透過生命週期組態規則，您可以指示 Amazon S3 將物件轉換為較便宜的儲存體方案、進行封存或刪除。如需詳細資訊，請參閱 Simple Storage Service (Amazon S3) 使用者指南中的[管理儲存生命週期](#)。

## 版本控制

版本控制是在相同儲存貯體中保留多個物件版本的方式。您可以使用版本控制功能來保留、擷取和恢復在 Amazon S3 儲存貯體中存放的每個物件的每個版本。版本控制可協助您從意外的使用者動作和應用程式失敗中復原。如需詳細資訊，請參閱《Amazon [S3 使用者指南](#)》中的在 [S3 儲存貯體中使用版本控制](#)。Amazon S3

## 儲存類別

Amazon S3 根據您的工作負載需求，提供各種儲存類別供選擇。S3 標準 – IA 和 S3 單區域 – IA 儲存類別是針對您每月存取約一次且需要毫秒存取的資料所設計。S3 Glacier Instant Retrieval 儲存類別專為長期存在且可以毫秒存取的封存資料而設計，您可以每季度存取一次。對於不需要立即存取的封存資料，例如備份，您可以使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 儲存類別。如需詳細資訊，請參閱《[Amazon S3 使用者指南](#)》中的[使用 Amazon S3 儲存類別](#)。Amazon S3

# Amazon Security Lake 中的基礎設施安全

Amazon Security Lake 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的相關資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Security Lake。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

## Security Lake 中的組態和漏洞分析

組態和 IT 控制是 AWS 與身為我們客戶的您共同的責任。如需詳細資訊，請參閱 AWS [共同的責任模型](#)。

### Amazon Security Lake 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，在 VPC 和 Amazon Security Lake 之間建立私有連線。介面端點採用 [AWS PrivateLink](#) 技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私下存取 Security Lake APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Security Lake APIs 通訊。VPC 和 Security Lake 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

如需詳細資訊，請參閱 AWS PrivateLink 指南中的[介面 VPC 端點 \(AWS PrivateLink\)](#)。

### Security Lake VPC 端點的考量事項

設定 Security Lake 的介面 VPC 端點之前，請務必檢閱 AWS PrivateLink 指南中的[介面端點屬性和限制](#)。

Security Lake 支援從您的 VPC 呼叫其所有 API 動作。

Security Lake 僅在下列存在 FIPS 的區域支援 FIPS VPC 端點：

- 美國東部 (維吉尼亞北部)
- 美國東部 (俄亥俄)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)

### 為 Security Lake 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 Security Lake 服務建立 VPC 端點 AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[建立介面端點](#)。

使用下列服務名稱為 Security Lake 建立 VPC 端點：

- `com.amazonaws.region.securitylake`
- `com.amazonaws.region.securitylake-fips` (FIPS 端點 )

如果您為端點啟用私有 DNS，您可以使用區域的預設 DNS 名稱向 Security Lake 提出 API 請求，例如 `securitylake.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[透過介面端點存取服務](#)。

## 為 Security Lake 建立 VPC 端點政策

您可以將端點政策連接至控制 Security Lake 存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[使用 VPC 端點控制對服務的存取](#)。

範例：Security Lake 動作的 VPC 端點政策

以下是 Security Lake 端點政策的範例。連接到端點時，此政策會授予所有資源上所有主體所列出的 Security Lake 動作的存取權。

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

## 共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。如需有關 VPC 子網路共用的資訊，請參閱《Amazon VPC 使用者指南》中的[與其他帳戶共用 VPC](#)。

## 監控 Amazon Security Lake

Security Lake 與 整合 AWS CloudTrail，此服務提供使用者、角色或其他使用者在 Security Lake 中採取的動作記錄 AWS 服務。這包括來自 Security Lake 主控台的動作，以及對 Security Lake API 操作的程式設計呼叫。透過使用 CloudTrail 收集的資訊，您可以判斷向 Security Lake 提出了哪些請求。對於每個請求，您可以識別提出時間、提出請求的 IP 地址、提出請求者，以及其他詳細資料。如需詳細資訊，請參閱[使用 CloudTrail 記錄 Security Lake API 呼叫](#)。

Security Lake 和 Amazon CloudWatch 已整合，因此您可以收集、檢視和分析 Security Lake 收集之日誌的指標。Security Lake 資料湖的 CloudWatch 指標會自動收集，並每隔一分鐘推送至 CloudWatch。您也可以設定警示，在達到 Security Lake 指標的指定閾值時傳送通知給您。如需 Security Lake 傳送至 CloudWatch 的所有指標清單，請參閱[Security Lake 指標和維度](#)。

### Amazon Security Lake 的 CloudWatch 指標

您可以使用 Amazon CloudWatch 監控 Security Lake，每分鐘收集原始資料並將其處理為可讀且近乎即時的指標。這些統計資料會保留 15 個月，因此您可以存取歷史資訊，並更清楚地了解資料湖中的資料。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。

#### 主題

- [Security Lake 指標和維度](#)
- [檢視 Security Lake 的 CloudWatch 指標](#)
- [設定 Security Lake 指標的 CloudWatch 警示](#)

### Security Lake 指標和維度

AWS/SecurityLake 命名空間包含下列指標。

指標	描述
ProcessedSize	AWS 服務 目前存放在您的資料湖中，來自原生支援的資料量。  單位：位元組

下列維度適用於 Security Lake 指標。

維度	描述
Account	ProcessedSize 特定的指標 AWS 帳戶。 此維度僅在您在 CloudWatch Per-Account Source Version Metrics 上檢視時可用。
Region	ProcessedSize 特定的指標 AWS 區域。
Source	ProcessedSize 特定 AWS 日誌來源的指標。
SourceVersion	ProcessedSize AWS 日誌來源特定版本的指標。

您可以檢視 specific AWS 帳戶 (Per-Account Source Version Metrics) 或組織 () 中所有帳戶的指標 Per-Source Version Metrics。

## 檢視 Security Lake 的 CloudWatch 指標

您可以使用 CloudWatch 主控台、CloudWatch 自己的命令列界面 (CLI) 或以程式設計方式使用 CloudWatch API 監控 Security Lake 的指標。選擇您偏好的方法，然後依照步驟存取 Security Lake 指標。

### CloudWatch console

1. 透過 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇指標、所有指標。
3. 在瀏覽索引標籤上，選擇 Security Lake。
4. 選擇每個帳戶來源版本指標或每個來源版本指標。
5. 選取指標以檢視詳細資訊。您也可以選擇執行下列動作：
  - 若要排序指標，請使用欄標題。
  - 若要繪製指標圖形，請選取指標名稱，然後選擇圖形選項。
  - 若要依指標篩選，請選取指標名稱，然後選擇新增至搜尋。

## CloudWatch API

若要使用 CloudWatch API 存取 Security Lake 指標，請使用 [GetMetricStatistics](#) 動作。

## AWS CLI

若要使用 存取 Security Lake 指標 AWS CLI，請執行 [get-metric-statistics](#) 命令。

如需使用指標監控的詳細資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》中的使用 Amazon CloudWatch 指標。

## 設定 Security Lake 指標的 CloudWatch 警示

CloudWatch 亦可讓您設定到達指標的閾值時的警示。例如，您可以設定 ProcessedSize 指標的警示，以便在特定來源的資料量超過特定閾值時收到通知。

如需設定警示的指示，請參閱《[Amazon CloudWatch 使用者指南](#)》中的使用 Amazon CloudWatch [警示](#)。 Amazon CloudWatch

# 使用 CloudTrail 記錄 Security Lake API 呼叫

Amazon Security Lake 與整合 AWS CloudTrail，此服務提供使用者、角色或 Security Lake AWS 服務所採取動作的記錄。CloudTrail 會將 Security Lake 的 API 呼叫擷取為事件。擷取的呼叫包括來自 Security Lake 主控台的呼叫，以及對 Security Lake API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Security Lake 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 Security Lake 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [「AWS CloudTrail 使用者指南」](#)。

## CloudTrail 中的 Security Lake 資訊

建立帳戶 AWS 帳戶時，您的上會啟用 CloudTrail。當活動在 Security Lake 中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以在中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱 [「使用 CloudTrail 事件歷史記錄檢視事件」](#)。

若要持續記錄中的事件 AWS 帳戶，包括 Security Lake 的事件，請建立追蹤。線索可讓 CloudTrail 將事件作為日誌檔案交付到您指定的 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案](#)和[接收多個帳戶的 CloudTrail 日誌檔案](#)

Security Lake 動作由 CloudTrail 記錄，並記錄在 [Security Lake API 參考](#)中。例如，對 UpdateDataLake、ListLogSources 以及 CreateSubscriber 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 請求是使用根登入資料還是 AWS Identity and Access Management 使用者登入資料提出。

- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需更多詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

## 了解 Security Lake 日誌檔案項目

CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 Security Lake GetSubscriber動作的 CloudTrail 日誌項目。

```
{
  "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"
}
```

# 標記 Security Lake 資源

標籤是選用的標籤，您可以定義和指派給 AWS 資源，包括特定類型的 Amazon Security Lake 資源。標籤可協助您以不同方式識別、分類和管理資源，例如依用途、擁有者、環境或其他條件。例如，您可以使用標籤來套用政策、配置成本、區分資源，或識別支援特定合規要求或工作流程的資源。

您可以將標籤指派給下列類型的 Security Lake 資源：訂閱者，以及 AWS 帳戶個別中的資料湖組態 AWS 區域。

## 主題

- [標記基礎知識](#)
- [在 IAM 政策中使用標籤](#)
- [將標籤新增至 Amazon Security Lake 資源](#)
- [編輯 Amazon Security Lake 資源的標籤](#)
- [從 Amazon Security Lake 資源移除標籤](#)

## 標記基礎知識

資源最多可以擁有 50 個標籤。每個標籤皆包含由您定義的必要「標籤金鑰」與選用「標籤值」。標籤索引鍵是一般標籤，可做為更特定標籤值的類別。標籤值是標籤金鑰的描述項。

例如，如果您新增訂閱者來分析來自不同環境的安全資料（一組訂閱者用於雲端資料，另一組用於內部部署資料），您可以為這些訂閱者指派 Environment 標籤金鑰。關聯的標籤值可能 Cloud 適用於從分析資料的訂閱者 AWS 服務，也可能 On-Premises 適用於其他訂閱者。

當您定義標籤並將其指派給 Amazon Security Lake 資源時，請記住下列事項：

- 每個資源的上限為 50 個標籤。
- 對於每個資源，每個標籤索引鍵都必須是唯一的，而且只能有一個標籤值。
- 標籤鍵與值皆區分大小寫。最佳實務是，建議您定義一個策略來將標籤資本化，並在整個資源中一致地實作該策略。
- 標籤索引鍵最多可有 128 個 UTF-8 字元。標籤值最多可有 256 個 UTF-8 字元。字元可以是字母、數字、空格或下列符號：\_ . : / = + - @
- 字aws: 首會保留供使用 AWS。您無法在定義的任何標籤索引鍵或值中使用它。此外，您無法變更或移除使用此字首的標籤索引鍵或值。使用此字首的標籤不會計入每個資源 50 個標籤的配額。

- 您指派的任何標籤僅適用於您的 AWS 帳戶，且僅適用於您指派標籤 AWS 區域的。
- 如果您使用 Security Lake 將標籤指派給資源，則標籤只會套用至直接存放在適用中 Security Lake 中的資源 AWS 區域。它們不會套用到 Security Lake 為您在其他中建立、使用或維護的任何相關支援資源 AWS 服務。例如，如果您將標籤指派給資料湖，則標籤只會套用至指定區域的 Security Lake 中的資料湖組態。它們不會套用至存放日誌和事件資料的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。若要同時將標籤指派給相關聯的資源，您可以使用 AWS Resource Groups 或存放資源 AWS 服務的，例如 Amazon S3 for a S3 儲存貯體。將標籤指派給相關聯的資源，可協助您識別資料湖的支援資源。
- 如果您刪除資源，指派給資源的任何標籤也會一併刪除。

如需其他限制、秘訣和最佳實務，請參閱 [《標記 AWS 資源使用者指南》](#) 中的標記您的 AWS 資源。

### Important

請勿在標籤中存放機密或其他類型的敏感資料。標籤可從許多存取 AWS 服務，包括 AWS 帳單與成本管理。它們不適用於敏感資料。

若要新增和管理 Security Lake 資源的標籤，您可以使用 Security Lake 主控台或 Security Lake API。

## 在 IAM 政策中使用標籤

開始標記資源後，您可以在 AWS Identity and Access Management (IAM) 政策中定義以標籤為基礎的資源層級許可。透過以這種方式使用標籤，您可以精細控制中的哪些使用者和角色 AWS 帳戶具有建立和標記資源的許可，以及哪些使用者和角色具有更廣泛地新增、編輯和移除標籤的許可。若要根據標籤控制存取，您可以在 IAM 政策的 [條件元素](#) 中使用 [標籤相關條件索引鍵](#)。

例如，您可以建立政策，以允許使用者完整存取所有 Amazon Security Lake 資源，如果資源的 Owner 標籤指定其使用者名稱：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securitylake:*",
      "Resource": "*",
      "Condition": {
```

```
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
    }
}
]
```

如果您定義標籤型、資源層級許可，則許可會立即生效。這表示您的資源一旦建立就會更安全，而且您可以快速開始強制使用新資源的標籤。您也可以使用資源層級許可，以控制哪些標籤金鑰和值可以與新的和現有的資源相關聯。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用標籤控制對 AWS 資源的存取](#)。

## 將標籤新增至 Amazon Security Lake 資源

若要將標籤新增至 Amazon Security Lake 資源，您可以使用 Security Lake 主控台或 Security Lake API。

### Important

將標籤新增至資源可能會影響對資源的存取。將標籤新增至資源之前，請檢閱任何可能使用標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

### Console

當您為 啟用 Security Lake AWS 區域 或建立訂閱者時，Security Lake 主控台會提供將標籤新增至資源的選項：區域或訂閱者的資料湖組態。當您建立資源時，請遵循主控台上的指示，將標籤新增至資源。

若要使用 Security Lake 主控台將一或多個標籤新增至現有資源，請遵循下列步驟。

#### 將標籤加入資源

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 根據您要新增標籤的資源類型，執行下列其中一項：
  - 對於資料湖組態，請在導覽窗格中選擇區域。然後，在區域資料表中，選取區域。
  - 對於訂閱者，在導覽窗格中選擇訂閱者。然後，在我的訂閱者資料表中，選取訂閱者。

如果訂閱者未出現在資料表中，請使用頁面右上角的 AWS 區域 選取器來選取您建立訂閱者的區域。資料表僅列出目前區域的現有訂閱者。

3. 選擇編輯。
4. 展開 Tags (標籤) 區段。本節列出目前指派給資源的所有標籤。
5. 在 標籤 區域，選擇 新增。
6. 在金鑰方塊中，輸入要新增至資源之標籤的標籤金鑰。然後，在值方塊中，選擇性地輸入索引鍵的標籤值。

標籤金鑰最多可包含 128 個字元。標籤值最多可包含 256 個字元。字元可以是字母、數字、空格或下列符號：\_ . : / = + - @

7. 若要將另一個標籤新增至資源，請選擇新增標籤，然後重複上述步驟。您可以將最多 50 個標籤指派給資源。
8. 完成新增標籤後，請選擇儲存。

## API

若要以程式設計方式建立資源並新增一或多個標籤，請針對您要建立的資源類型使用適當的 Create 操作：

- Data lake 組態 – 使用 [CreateDataLake](#) 操作，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [create-data-lake](#) 命令。
- 訂閱者 – 使用 [CreateSubscriber](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [create-subscriber](#) 命令。

在您的請求中，使用 `tags` 參數來指定要新增至資源的每個標籤的標籤索引鍵 (key) 和選用標籤值 (value)。tags 參數會指定物件陣列。每個物件都會指定標籤索引鍵及其相關聯的標籤值。

若要將一或多個標籤新增至現有資源，請使用 Security Lake API 的 [TagResource](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [tag-resource](#) 命令。在請求中，指定您要新增標籤的資源的 Amazon Resource Name (ARN)。使用 `tags` 參數來指定要新增的每個標籤的標籤索引鍵 (key) 和選用標籤值 (value)。如同 Create 操作和命令一樣，tags 參數會指定物件陣列、每個標籤索引鍵的一個物件及其相關聯的標籤值。

例如，下列 AWS CLI 命令會將標籤值為 Environment 標籤的 Cloud 標籤索引鍵新增至指定的訂閱者。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ 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` 指定要新增標籤的訂閱者的 ARN。
- `Environment` 是要新增至訂閱者的標籤的標籤索引鍵。
- `Cloud` 是指定標籤索引鍵 (`Environment`) 的標籤值。

在下列範例中，命令會將數個標籤新增至訂閱者。

```
$ 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
```

對於tags陣列中的每個物件，都需要 `key` 和 `value` 引數。不過，`value` 引數的值可以是空字串。如果您不想將標籤值與標籤索引鍵建立關聯，請不要為 `value` 引數指定值。例如，下列命令會新增沒有關聯 `Owner` 標籤值的標籤金鑰：

```
$ aws securitylake tag-resource \  
--resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \  
--tags key=Owner,value=
```

如果標記操作成功，Security Lake 會傳回空的 HTTP 200 回應。否則，Security Lake 會傳回 HTTP 4xx 或 500 回應，指出操作失敗的原因。

## 編輯 Amazon Security Lake 資源的標籤

若要編輯 Amazon Security Lake 資源的標籤（標籤索引鍵或標籤值），您可以使用 Security Lake 主控台或 Security Lake API。

### Important

編輯資源的標籤可能會影響對資源的存取。在編輯資源的標籤索引鍵或值之前，請檢閱可能使用標籤來控制資源存取的任何 AWS Identity and Access Management (IAM) 政策。

## Console

請依照下列步驟，使用 Security Lake 主控台編輯資源的標籤。

### 編輯資源的標籤

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 根據您要編輯其標籤的資源類型，執行下列其中一項操作：
  - 對於資料湖組態，請在導覽窗格中選擇區域。然後，在區域資料表中，選取區域。
  - 對於訂閱者，在導覽窗格中選擇訂閱者。然後，在我的訂閱者資料表中，選取訂閱者。

如果訂閱者未出現在資料表中，請使用頁面右上角的 AWS 區域 選取器來選取您建立訂閱者的區域。資料表只會列出目前區域的現有訂閱者。

3. 選擇編輯。
4. 展開 Tags (標籤) 區段。標籤區段會列出目前指派給資源的所有標籤。
5. 執行下列任何一項：
  - 若要將標籤值新增至現有的標籤金鑰，請在標籤金鑰旁的值方塊中輸入值。
  - 若要變更現有的標籤金鑰，請選擇標籤旁的移除。然後選擇新增標籤。在出現的金鑰方塊中，輸入新的標籤金鑰。或者，在值方塊中輸入相關聯的標籤值。
  - 若要變更現有的標籤值，請在包含值的值方塊中選擇 X。然後在值方塊中輸入新的標籤值。
  - 若要移除現有的標籤值，請在包含值的值方塊中選擇 X。
  - 若要移除現有標籤（包括標籤索引鍵和標籤值），請選擇標籤旁的移除。

資源最多可以擁有 50 個標籤。標籤金鑰最多可包含 128 個字元。標籤值最多可包含 256 個字元。字元可以是字母、數字、空格或下列符號：\_ . : / = + - @

6. 當您完成編輯標籤時，請選擇儲存。

## API

當您以程式設計方式編輯資源的標籤時，會使用新的值覆寫現有的標籤。因此，編輯標籤的最佳方式取決於您要編輯標籤金鑰、標籤值或兩者。若要編輯標籤金鑰，[請移除目前的標籤並新增標籤](#)。

若要編輯或僅移除與標籤金鑰相關聯的標籤值，請使用 Security Lake API 的 [TagResource](#) 操作覆寫現有的值。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [tag-resource](#) 命令。在請求中，指定您要編輯或移除其標籤值之資源的 Amazon Resource Name (ARN)。

若要編輯標籤值，請使用 `tags` 參數來指定您要變更其標籤值的標籤索引鍵。同時指定金鑰的新標籤值。例如，下列 AWS CLI 命令 `On-Premises` 會將指派給指定訂閱者的標籤金鑰的 `Environment` 標籤值從 `Cloud` 變更為 `On-Premises`。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (`\`) 行接續字元來改善可讀性。

```
$ 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` 指定訂閱者的 ARN。
- `Environment` 是與要變更的標籤值相關聯的標籤金鑰。
- `On-Premises` 是指定標籤金鑰 (`Environment`) 的新標籤值 `Environment`。

若要從標籤索引鍵移除標籤值，請勿在 `tags` 參數中指定索引鍵 `value` 引數的值。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 會傳回空的 HTTP 200 回應。否則，Security Lake 會傳回 HTTP 4xx 或 500 回應，指出操作失敗的原因。

## 檢閱 Amazon Security Lake 資源的標籤

您可以使用 Security Lake 主控台或 Security Lake API 來檢閱 Amazon Security Lake 資源的標籤（標籤索引鍵和標籤值）。

### Console

請依照下列步驟，使用 Security Lake 主控台檢閱資源的標籤。

#### 檢閱資源的標籤

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。

2. 根據您要檢閱其標籤的資源類型，執行下列其中一項操作：

- 對於資料湖組態，請在導覽窗格中選擇區域。在區域資料表中，選取區域，然後選擇編輯。然後展開標籤區段。
- 對於訂閱者，在導覽窗格中選擇訂閱者。然後，在我的訂閱者資料表中，選擇訂閱者的名稱。

如果訂閱者未出現在資料表中，請使用頁面右上角的 AWS 區域 選取器來選取您建立訂閱者的區域。資料表只會列出目前區域的現有訂閱者。

標籤區段會列出目前指派給資源的所有標籤。

## API

若要以程式設計方式擷取和檢閱現有資源的標籤，請使用 Security Lake API 的 [ListTagsForResource](#) 操作。在您的請求中，使用 `resourceArn` 參數來指定資源的 Amazon Resource Name (ARN)。

如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [list-tags-for-resource](#) 命令，並使用 `resource-arn` 參數來指定資源的 ARN。例如：

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

在上述範例中，`arn#aws#securitylake#us-east-1#123456789012#subscriber/1234abcd-12ab-34cd-56ef-1234567890ab` 是現有訂閱者的 ARN。

如果操作成功，Security Lake 會傳回tags陣列。陣列中的每個物件都會指定目前指派給資源的標籤（包括標籤索引鍵和標籤值）。例如：

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Cloud"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    },
    {
```

```
        "key": "Owner",
        "value": ""
    }
]
}
```

其中 Environment、CostCenter 和 Owner 是指派給資源的標籤金鑰。Cloud 是與標籤金鑰相關聯的 Environment 標籤值。12345 是與標籤金鑰相關聯的 CostCenter 標籤值。Owner 標籤索引鍵沒有相關聯的標籤值。

## 從 Amazon Security Lake 資源移除標籤

若要從 Amazon Security Lake 資源移除標籤，您可以使用 Security Lake 主控台或 Security Lake API。

### Important

從資源移除標籤可能會影響對資源的存取。移除標籤之前，請檢閱任何可能使用標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

### Console

請依照下列步驟，使用 Security Lake 主控台從資源移除一或多個標籤。

#### 從資源移除標籤

1. 開啟位於 <https://console.aws.amazon.com/securitylake/> 的 Security Lake 主控台。
2. 根據您要從中移除標籤的資源類型，執行下列其中一項：
  - 對於資料湖組態，請在導覽窗格中選擇區域。然後，在區域資料表中，選取區域。
  - 對於訂閱者，在導覽窗格中選擇訂閱者。然後，在我的訂閱者資料表中，選取訂閱者。

如果訂閱者未出現在資料表中，請使用頁面右上角的 AWS 區域 選取器來選取您建立訂閱者的區域。資料表只會列出目前區域的現有訂閱者。

3. 選擇編輯。
4. 展開 Tags (標籤) 區段。標籤區段會列出目前指派給資源的所有標籤。
5. 執行下列任何一項：

- 若要僅移除標籤的標籤值，請在包含要移除值的值方塊中選擇 X。
  - 若要同時移除標籤的標籤索引鍵和標籤值（成對），請選擇要移除之標籤旁的移除。
6. 若要從資源中移除其他標籤，請為每個要移除的其他標籤重複上述步驟。
  7. 當您完成移除標籤時，請選擇儲存。

## API

若要以程式設計方式從資源移除一或多個標籤，請使用 Security Lake API 的 [UntagResource](#) 操作。在您的請求中，使用 `resourceArn` 參數來指定要從中移除標籤之資源的 Amazon Resource Name (ARN)。使用 `tagKeys` 參數來指定要移除之標籤的標籤索引鍵。若要移除多個標籤，請附加要移除之每個標籤的 `tagKeys` 參數和引數，以 ampersand (&) 分隔，例如 `tagKeys=key1&tagKeys=key2`。若要僅從資源移除特定標籤值（而非標籤金鑰），請[編輯標籤](#)，而不是移除標籤。

如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [untag-resource](#) 命令，從資源中移除一或多個標籤。針對 `resource-arn` 參數，指定要從中移除標籤之資源的 ARN。使用 `tag-keys` 參數來指定要移除之標籤的標籤索引鍵。例如，下列命令會從指定的訂閱者移除 `Environment` 標籤（標籤索引鍵和標籤值）：

```
$ 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` 指定要從中移除標籤的訂閱者的 ARN，`Environment` 是要移除標籤的標籤索引鍵。

若要從資源中移除多個標籤，請新增每個額外的標籤索引鍵做為 `tag-keys` 參數的引數。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 會傳回空的 HTTP 200 回應。否則，Security Lake 會傳回 HTTP 4xx 或 500 回應，指出操作失敗的原因。

## 對 Security Lake 中的問題進行故障診斷

如果您在使用 Amazon Security Lake 時遇到問題，請使用下列疑難排解資源。

下列主題提供與資料湖狀態、Lake Formation、在 Amazon Athena 中查詢和 IAM 相關的錯誤 AWS Organizations 和問題的疑難排解建議。如果您發現此處未列出的問題，您可以使用此頁面上的 Feedback 按鈕進行報告。

如果您在使用 Security Lake 時遇到問題，請參閱下列主題。

### 主題

- [對資料湖狀態進行故障診斷](#)
- [對 Lake Formation 問題進行故障診斷](#)
- [對 Amazon Athena 中的查詢進行故障診斷](#)
- [對 Organizations 問題進行故障診斷](#)
- [對 Amazon Security Lake 身分和存取進行故障診斷](#)

## 對資料湖狀態進行故障診斷

Security Lake 主控台的問題頁面會顯示影響資料湖的問題摘要。例如，如果您尚未為組織建立 CloudTrail 追蹤，Security Lake 就無法為 AWS CloudTrail 管理事件啟用日誌收集。問題頁面涵蓋過去 14 天內發生的問題。您可以查看每個問題的描述和建議的修補步驟。

若要以程式設計方式存取問題摘要，您可以使用 Security Lake API [ListDataLakeExceptions](#) 的操作。如果您使用的是 AWS CLI，請執行 [list-data-lake-exceptions](#) 命令。對於 regions 參數，您可以指定一或多個區域代碼，例如 us-east-1 美國東部（維吉尼亞北部）區域，以查看影響這些區域的問題。如果您未包含 regions 參數，則會傳回影響所有區域的問題。如需區域代碼清單，請參閱 [Amazon Security Lake 端點](#) AWS 一般參考。

例如，下列 AWS CLI 命令會列出影響 us-east-1 和 eu-west-3 區域的問題。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securitylake list-data-lake-exceptions \  
--regions "us-east-1" "eu-west-3"
```

若要將問題或錯誤通知 Security Lake 使用者，請使用 Security Lake API [CreateDataLakeExceptionSubscription](#) 的操作。使用者可透過電子郵件、交付至 Amazon Simple Queue Service (Amazon SQS) 佇列、交付至 AWS Lambda 函數或其他支援的通訊協定收到通知。

例如，下列 AWS CLI 命令會透過簡訊交付，將 Security Lake 例外狀況的通知傳送至指定的帳戶。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securitylake create-data-lake-exception-subscription \  
--notification-endpoint "123456789012" \  
--exception-time-to-live 30 \  
--subscription-protocol "sms"
```

若要檢視例外狀況訂閱的詳細資訊，您可以使用 [GetDataLakeExceptionSubscription](#) 操作。若要更新例外狀況訂閱，您可以使用 [UpdateDataLakeExceptionSubscription](#) 操作。若要刪除例外狀況訂閱並停止通知，您可以使用 [DeleteDataLakeExceptionSubscription](#) 操作。

## 對 Lake Formation 問題進行故障診斷

使用下列資訊來協助您診斷和修正使用 Security Lake 和 AWS Lake Formation 資料庫或資料表時可能遇到的常見問題。如需 Lake Formation 疑難排解主題的詳細資訊，請參閱 AWS Lake Formation 開發人員指南中的 [疑難排解](#) 一節。

### 找不到資料表

嘗試建立訂閱者時，您可能會收到此錯誤。

若要解決此錯誤，請確定您已在區域中新增來源。如果您在 Security Lake 服務處於預覽版本時新增了來源，則必須在建立訂閱者之前再次新增它們。如需新增來源的詳細資訊，請參閱 [Security Lake 中的來源管理](#)。

### 400 AccessDenied

當您 [新增自訂來源](#) 並呼叫 CreateCustomLogSource API 時，您可能會收到此錯誤。

若要解決錯誤，請檢閱 Lake Formation 許可。呼叫 API 的 IAM 角色應具有 Security Lake 資料庫的建立資料表許可。如需詳細資訊，請參閱《AWS Lake Formation 開發人員指南》中的 [使用 Lake Formation 主控台和具名資源方法授予資料庫許可](#)。

### SYNTAX\_ERROR : 第 1 : 8 行 : 不允許來自沒有資料欄之關係的 SELECT \*

在 Lake Formation 中第一次查詢來源資料表時，您可能會收到此錯誤。

若要解決錯誤，請將SELECT許可授予您在登入時正在使用的 IAM 角色 AWS 帳戶。如需如何授予SELECT許可的指示，請參閱《AWS Lake Formation 開發人員指南》中的[使用 Lake Formation 主控台和具名資源方法授予資料表許可](#)。

Security Lake 無法將發起人的主要 ARN 新增至 Lake Formation 資料湖管理員。目前的資料湖管理員可能包含不再存在的無效主體。

啟用 Security Lake 或新增 AWS 服務 做為日誌來源時，您可能會收到此錯誤。

若要解決錯誤，請遵循下列步驟：

1. 開啟 Lake Formation 主控台，網址為 <https://console.aws.amazon.com/lakeformation/>。
2. 以管理使用者身分登入。
3. 在導覽窗格中的許可下，選擇管理角色和任務。
4. 在 Data lake 管理員區段中，選擇選擇管理員。
5. 清除在 IAM 中找不到的標記主體，然後選擇儲存。
6. 再次嘗試 Security Lake 操作。

Security Lake CreateSubscriber with Lake Formation 未建立新的 RAM 資源共享邀請，以供接受

如果您在 Security Lake 中建立 Lake Formation 訂閱者之前，與 [Lake Formation 第 2 版或第 3 版跨帳戶資料共用](#) 共用資源，您可能會看到此錯誤。這是因為 Lake Formation AWS 第 2 版和第 3 版跨帳戶共用透過映射多個跨帳戶許可授予與一個 RAM 資源共用來最佳化 AWS RAM 資源共用的數量。

請務必檢查資源共用名稱是否具有您在建立訂閱者時指定的外部 ID，且資源共用 ARN 符合 CreateSubscriber 回應中的 ARN。

## 對 Amazon Athena 中的查詢進行故障診斷

使用下列資訊來協助您診斷和修正使用 Athena 查詢存放在 Security Lake S3 儲存貯體中的物件時可能遇到的常見問題。如需更多 Athena 疑難排解主題，請參閱《[Amazon Athena](#) Amazon Athena 疑難排解一節。

## 查詢不會在資料湖中傳回新物件

即使 Security Lake 的 S3 儲存貯體包含這些物件，您的 Athena 查詢可能不會在資料湖中傳回新物件。如果您已停用 Security Lake，然後再次啟用它，則可能會發生這種情況。因此，AWS Glue 分割區可能無法正確註冊新的物件。

若要解決錯誤，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/lambda/> 開啟 AWS Lambda 主控台。
2. 從導覽列的區域選擇器中，選擇啟用 Security Lake 但 Athena 查詢未傳回結果的區域。
3. 從導覽窗格中，選擇函數，並根據來源版本從下列清單中選擇函數：
  - Source version 1 (OCSF 1.0.0-rc.2) – SecurityLake\_Glue\_Partition\_Updater\_Lambda\_#region> 函數。
  - Source version 2 (OCSF 1.1.0) – AmazonSecurityLakeMetastoreManager\_#region> 函數。
4. 在組態索引標籤上，選擇觸發。
5. 選取函數旁的選項，然後選擇編輯。
6. 選取啟用觸發，然後選擇儲存。這會將函數狀態變更為已啟用。

## 無法存取 AWS Glue 資料表

查詢存取訂閱者可能無法存取包含 Security Lake 資料的 AWS Glue 資料表。

首先，請確定您已遵循 [中概述的步驟設定跨帳戶資料表共用（訂閱者步驟）](#)。

如果訂閱者仍然無法存取，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/glue/> 開啟 AWS Glue 主控台。
2. 從導覽窗格中，選擇 Data Catalog 和 Catalog 設定。
3. 准許訂閱者使用資源型政策存取 AWS Glue 資料表。如需建立資源型政策的相關資訊，請參閱《AWS Glue 開發人員指南》中的 [的資源型政策範例 AWS Glue](#)。

## 對 Organizations 問題進行故障診斷

使用下列資訊來協助您診斷和修正使用 Security Lake 和 時可能遇到的常見問題 AWS Organizations。如需更多 Organizations 故障診斷主題，請參閱 AWS Organizations 使用者指南中的 [故障診斷](#) 一節。

呼叫 `CreateDataLake` 操作時發生存取遭拒錯誤：您的帳戶必須是組織或獨立帳戶的委派管理員帳戶。

如果您刪除委派管理員帳戶所屬的組織，然後嘗試使用 Security Lake 主控台或 [CreateDataLake](#) API 來使用該帳戶設定 Security Lake，則可能會收到此錯誤。

若要解決錯誤，請使用來自不同組織或獨立帳戶的委派管理員帳戶。

## 對 Amazon Security Lake 身分和存取進行故障診斷

使用下列資訊來協助您診斷和修正使用 Security Lake 和 IAM 時可能遇到的常見問題。

### 我無權在 Security Lake 中執行動作

如果 AWS Management Console 告訴您未獲授權執行動作，則必須聯絡管理員尋求協助。您的管理員是為您提供憑證的人員。

當 `mateojackson` IAM 使用者嘗試使用主控台檢視虛構但 `subscriber` 沒有虛構 `SecurityLake:GetSubscriber` 許可的詳細資訊時，會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
YOURSERVICEPREFIX: GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會要求管理員更新其政策，以允許他使用 `SecurityLake:GetSubscriber` 動作存取 `subscriber` 資訊。

### 我想要將許可擴展到受管政策之外

訂閱者或自訂日誌來源 APIs 建立的所有 IAM 角色都受

`AmazonSecurityLakePermissionsBoundary` 受受管政策約束。如果您想要將許可擴展到受管政策之外，您可以從角色的許可邊界移除受管政策。不過，在與 `dataLakes` 和訂閱者的變動 Security Lake APIs 互動時，必須連接許可界限，IAM 才能變動 IAM 角色。

### 我未獲授權執行 `iam:PassRole`

如果您收到錯誤，表示您無權執行 `iam:PassRole` 動作，則必須更新您的政策，以允許您將角色傳遞至 Security Lake。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM marymajor 使用者嘗試使用主控台在 Security Lake 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我想要允許以外的人員 AWS 帳戶 存取我的 Security Lake 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Security Lake 是否支援這些功能，請參閱 [Security Lake 如何與 IAM 搭配使用](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱 [《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個資源中提供存取權給 IAM 使用者](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 [《IAM 使用者指南》中的提供存取權給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 [《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取](#)。

# Security Lake 定價的判斷方式

Amazon Security Lake 定價基於兩個維度：資料擷取和資料轉換。Security Lake 也會與其他合作 AWS 服務來存放和共用您的資料，而且您可能會針對這些活動產生個別的費用。

當您第一次在 Security Lake 支援的任何 AWS 帳戶中開啟日誌集合 AWS 區域時，該帳戶會自動註冊 15 天免費試用 Security Lake。在免費試用期間，您可能仍會從其他服務產生費用。

若要了解 Security Lake 定價背後的方法，請觀看下列影片：[Amazon Security Lake 定價-->](#)

## 資料擷取

這些成本衍生自擷取 AWS CloudTrail 日誌和其他 AWS 服務日誌和事件 (Amazon Route 53 解析程式查詢日誌、AWS Security Hub 調查結果和 Amazon VPC 流程日誌) 的數量。

## 資料轉換

這些成本衍生自 Security Lake 標準化為 [Security Lake 中的開放式網路安全結構描述架構 \(OCSF\)](#) 結構描述並轉換為 Apache Parquet 格式的 AWS 服務日誌和事件量。

## 相關服務的成本

以下是您在安全資料湖中存放和共用資料 AWS 服務時，可能從其他產生的一些成本：

- Amazon S3 – 這些成本衍生自維護 Security Lake 帳戶中的 Amazon S3 儲存貯體、將資料存放在該帳戶中，以及評估和監控儲存貯體的安全性和存取控制。如需詳細資訊，請參閱 [Simple Storage Service \(Amazon S3\) 定價](#)。
- Amazon SQS – 這些成本衍生自建立訊息傳遞的 Amazon SQS 佇列。如需詳細資訊，請參閱 [Amazon SQS 定價](#)。
- Amazon EventBridge – 這些成本衍生自 Amazon EventBridge 傳送物件通知至訂閱端點。如需詳細資訊，請參閱 [Amazon EventBridge 定價](#)。
- AWS Glue – 每月成本取決於從每 GB AWS 服務擷取的日誌和事件資料量。您的資料會存放在 Amazon Simple Storage Service 中，並收取標準 Amazon S3 費用。Security Lake AWS 也會代您協調其他服務。對於作為安全資料湖一部分而設定 AWS 的服務和資源，您將產生單獨的費用。請參閱 [AWS Glue](#)、[Amazon EventBridge](#)、[AWS Lambda](#)、[Amazon SQS](#) 和 [Amazon Simple Notification Service](#) 的定價。您需負責從 Security Lake 查詢資料並儲存查詢結果，以承擔產生的成本。

訂閱者從 Security Lake 查詢資料並儲存查詢結果所產生的成本，由訂閱者負責。

如需成本和輔助服務的完整清單，請參閱 [Security Lake 定價](#)。

## 檢閱 Security Lake 用量和預估成本

Amazon Security Lake 主控台的用量頁面可讓您檢閱目前的 Security Lake 用量，以及未來的用量和成本估算。如果您目前正在參加 15 天免費試用，則您在試用期間的使用量可協助您預估免費試用結束後使用 Security Lake 的成本。如需 Security Lake 定價的概觀，請參閱 [Security Lake 定價的判斷方式](#)。如需詳細資訊和成本範例，請參閱 [Amazon Security Lake 定價](#)。

在 Security Lake 中，估計用量成本會以美元報告，並僅適用於目前的 AWS 區域。這些成本涵蓋組織中所有帳戶的 Security Lake 用量，並包含轉換為開放網路安全結構描述架構 (OCSF) 和 Apache Parquet 格式。不過，預測成本不包含 Security Lake 使用的其他服務的成本，例如 Amazon Simple Storage Service (Amazon S3) 和 AWS Glue。

在用量頁面上，您可以選擇檢視用量和成本資料的期間。預設期間是最後 1 個日曆天。您必須擁有至少 1 天的 Security Lake 用量，才能查看成本預測。

頁面頂端顯示所有帳戶的預測成本。這是根據您在所選時間範圍內的實際用量，未來 30 個日曆天內目前預測 AWS 區域的 Security Lake 成本。實際用量和預測成本反映組織中的所有帳戶。

在頁面的其餘部分，用量和成本資料會分為兩個資料表，如下所示：

- 依來源區分的用量和成本 – 這是您目前的 Security Lake 用量依資料來源細分，以及根據您在所選時間範圍內的實際用量，未來 30 個日曆日的預估用量和成本。實際用量、預測用量和預測成本會反映組織中的所有帳戶。如果您選取來源，分割面板會開啟，顯示哪些帳戶從該來源產生日誌和事件。對於每個帳戶，分割面板包含來自該來源的實際用量，以及預測用量和成本。
- 依帳戶的用量和成本 – 這是您目前的 Security Lake 用量依帳戶細分，以及根據您在所選時間範圍內的實際用量，未來 30 個日曆日的預估用量和成本。如果您選取帳戶，將開啟一個分割面板，其中顯示對該帳戶用量做出貢獻的來源。對於每個貢獻來源，分割面板包含實際用量和預測用量和成本。

所有支援的 AWS 資料來源都會出現在上述資料表中，即使您尚未在 Security Lake 中新增特定來源。如果您正在參加免費試用，我們建議您新增所有 AWS 來源，以取得完整的日誌和事件組的成本估算。如需新增 AWS 來源的說明，請參閱 [在 Security Lake AWS 服務中從收集資料](#)。自訂來源不包含在用量或成本計算中。

請依照下列步驟，在 Security Lake 主控台中檢閱您的用量和成本資料。

## 檢閱 Security Lake 用量和預測成本（主控台）

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選取您要檢閱用量和成本的區域。
3. 在導覽窗格中，選擇設定，然後選擇用量。
4. 選取您要查看用量和成本資料的期間。預設為最後 1 天。
5. 選取依資料來源或依帳戶索引標籤，以詳細檢閱用量和成本。

## Security Lake 區域和端點

如需 Security Lake 支援的區域和服務端點清單，請參閱 中的 [Amazon Security Lake 端點](#) AWS 一般參考。

建議您在所有支援的 中啟用 Security Lake AWS 區域。這可讓您使用 Security Lake 來偵測和調查未經授權的或異常活動，即使您未主動使用的區域也是如此。

# 停用 Security Lake

當您停用 Amazon Security Lake 時，Security Lake 會 AWS 停止從您的來源收集日誌和事件。現有的 Security Lake 設定和在 中建立的資源 AWS 帳戶 都會保留。此外，您存放在 中或發佈到其他的資料 AWS 服務，例如 AWS Lake Formation 資料表和 AWS CloudTrail 日誌中的敏感資料，仍然可用。存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的資料仍會根據您的 [Amazon S3 儲存生命週期](#) 保持可用。

從 Security Lake 主控台的設定頁面停用 Security Lake 會停止目前啟用 AWS 區域 Security Lake 的所有 中的 AWS 日誌和事件集合。您可以使用主控台上的區域頁面，在特定區域中停止日誌收集。Security Lake API 和 AWS CLI 也會在您於請求中指定的區域中停止日誌收集。

如果您使用 整合，AWS Organizations 而您的帳戶是集中管理多個 Security Lake 帳戶的組織的一部分，則只有委派的 Security Lake 管理員可以停用 Security Lake 本身和成員帳戶。不過，離開組織會停止成員帳戶的日誌收集。

當您停用組織的 Security Lake 時，如果您遵循此頁面提供的停用指示，委派管理員指定會保留。您不需要再次指定委派管理員，即可重新啟用 Security Lake。

對於自訂來源，停用 Security Lake 時，您必須停用 Security Lake 主控台以外的每個來源。未停用整合將導致來源整合繼續將日誌傳送至 Amazon S3。此外，您必須停用訂閱者整合，否則訂閱者仍然可以取用來自 Security Lake 的資料。如需如何移除自訂來源或訂閱者整合的詳細資訊，請參閱個別供應商的文件。

## Important

您必須先刪除 AWS Glue 資料庫，才能重新啟用 Security Lake，以確保查詢正常運作。

當 Security Lake 重新啟用時，會建立新的資料湖 Amazon S3 儲存貯體，並在此新的 S3 儲存貯體中收集資料。如果您先前已刪除 AWS Glue 資料表，則會建立新的一組 AWS Glue 資料表。

在停用 Security Lake 之前收集的所有資料都會保留在舊的 Amazon S3 儲存貯體中。如果您想要查詢舊資料，您必須使用 Amazon S3 Sync 命令將它們移至新的儲存貯體。如需詳細資訊，請參閱 命令參考中的 [Sync](#) AWS CLI 命令。

本主題說明如何使用 Security Lake 主控台、Security Lake API 或 來停用 Security Lake AWS CLI。

## Console

1. 在 <https://console.aws.amazon.com/securitylake/> 開啟 Security Lake 主控台。
2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。
3. 選擇停用安全湖。
4. 出現確認提示時，輸入 **Disable**，然後選擇停用。

## API

若要以程式設計方式停用 Security Lake，請使用 Security Lake API [DeleteDataLake](#) 的操作。如果您使用的是 AWS CLI，請執行 [delete-data-lake](#) 命令。在您的請求中，使用 `regions` 清單來指定您要停用 Security Lake 的每個區域的區域代碼。如需區域代碼清單，請參閱 [Amazon Security Lake 端點](#) AWS 一般參考。

對於使用 Security Lake 部署 AWS Organizations，只有組織的委派 Security Lake 管理員可以停用組織中帳戶的 Security Lake。

例如，下列 AWS CLI 命令會在 `ap-northeast-1` 和 `eu-central-1` 區域中停用 Security Lake。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (`\`) 行接續字元來改善可讀性。

```
$ aws securitylake delete-data-lake \  
--regions "ap-northeast-1" "eu-central-1"
```

# Amazon Security Lake 使用者指南的文件歷史記錄

下表說明自上次發行 Amazon Security Lake 以來文件的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

文件最近更新時間：2025 年 4 月 24 日

變更	描述	日期
<a href="#">已更新功能 - 服務連結角色</a>	Security Lake 現在會在資料湖建立期間自動建立 AWSServiceRoleForSecurityLakeResourceManagement SLR。如需詳細資訊，請參閱 <a href="#">考量</a> 。	2025 年 4 月 24 日
<a href="#">大幅重寫主題 - AWS 整合</a>	已更新指定 Security Lake 與特定整合的內容 AWS 服務。如需詳細資訊，請參閱 <a href="#">AWS 服務整合</a> 。	2025 年 3 月 31 日
<a href="#">已更新功能 - 管理多個帳戶</a>	Security Lake 主控台現在支援在帳戶加入您的組織時管理帳戶的自動啟用組態。如需詳細資訊，請參閱 <a href="#">在主控台中編輯新帳戶組態</a> 。	2025 年 3 月 10 日
<a href="#">更新功能 - AWS WAF 日誌中的資料保護</a>	在 Security Lake 帳戶的 Web ACL 中啟用時，新增對資料保護的支援。如需詳細資訊，請參閱 <a href="#">AWS WAF Security Lake 中的日誌</a> 。	2025 年 2 月 17 日
<a href="#">新功能 - 新增對 VPC 端點的支援</a>	Security Lake 現在已與整合 AWS PrivateLink，並支援 VPC 端點。如需 AWS PrivateLink 整合的詳細資訊，請參閱 <a href="#">Amazon Security</a>	2025 年 2 月 4 日

## [Lake 和界面 VPC 端點 \(AWS PrivateLink\)。](#)

### [新功能](#)

Security Lake 現在支援 OpenSearch Service 直接查詢，以分析 Security Lake 中的資料。如需詳細資訊，請參閱[與 OpenSearch Service 整合](#)。

2024 年 12 月 1 日

### [新的服務連結角色](#)

我們新增了新的服務連結角色 [AWSServiceRoleForSecurityLakeResourceManagement](#)。此服務連結角色可為 Security Lake 提供許可，以執行持續的監控和效能改善，進而降低延遲和成本。

2024 年 11 月 14 日

### [區域可用性](#)

Security Lake 現已在 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 提供 AWS 區域。如需目前可使用 Security Lake 的區域完整清單，請參閱中的 [Amazon Security Lake 端點](#) AWS 一般參考。

2024 年 6 月 10 日

### [更新現有的 受管政策](#)

我們已將 AWS WAF 動作新增至政策的 AWS 受管 [SecurityLakeServiceLinkedRole](#) 政策。其他動作允許 Security Lake 在 Security Lake 中啟用為 AWS WAF 日誌來源時收集日誌。

2024 年 5 月 22 日

<a href="#">新的 AWS 日誌來源</a>	Security Lake 新增 <a href="#">AWS WAF 日誌</a> 做為 AWS 日誌來源。AWS WAF 可協助您監控最終使用者傳送至應用程式的 Web 請求。	2024 年 5 月 22 日
<a href="#">現有 受管政策的更新</a>	我們已將 SID 動作新增至 <a href="#">AmazonSecurityLakePermissionsBoundary</a> 政策。	2024 年 5 月 13 日
<a href="#">現有 受管政策的更新</a>	我們更新了 <a href="#">AmazonSecurityLakeMetastoreManager</a> 政策，以新增中繼資料清除動作，可讓您刪除資料湖中的中繼資料。	2024 年 3 月 27 日
<a href="#">新的來源版本</a>	<a href="#">更新您的角色許可</a> ，從新的資料來源版本擷取資料。	2024 年 2 月 29 日
<a href="#">新的 AWS 日誌來源</a>	Security Lake 新增 <a href="#">EKS 稽核日誌</a> 作為 AWS 日誌來源。EKS 稽核日誌可協助您偵測 Amazon Elastic Kubernetes Service 內 EKS 叢集中的潛在可疑活動。	2024 年 2 月 29 日
<a href="#">現有 受管政策的更新</a>	我們已更新政策以允許新 <a href="#">AmazonSecurityLakeMetastoreManagerV2</a> 角色 <code>iam:PassRole</code> ，並讓 Security Lake 部署或更新資料湖元件。	2024 年 2 月 23 日

<a href="#">新的 受管政策</a>	我們新增了新的 <a href="#">AWS 受管政策</a> ，即AmazonSecurityLakeMetastore Manager 政策。此政策授予 Security Lake 在資料湖中管理中繼資料的許可。	2024 年 1 月 23 日
<a href="#">區域可用性</a>	Security Lake 現已在下列地區提供 AWS 區域：亞太區域（大阪）、加拿大（中部）、歐洲（巴黎）和歐洲（斯德哥爾摩）。如需目前可使用 Security Lake 的區域完整清單，請參閱中的 <a href="#">Amazon Security Lake 端點</a> AWS 一般參考。	2023 年 10 月 26 日
<a href="#">新功能</a>	您現在可以為具有查詢存取權的訂閱者編輯特定設定。您也可以為 <a href="#">Security Lake 資源指派標籤</a> AWS 帳戶。	2023 年 7 月 20 日
<a href="#">新的 受管政策</a>	Security Lake 新增了新的 <a href="#">AWS 受管政策</a> ，即AmazonSecurityLakeAdministrator 政策。此政策會授予管理許可，允許主體完整存取所有 Security Lake 動作。	2023 年 5 月 30 日
<a href="#">一般可用性</a>	Security Lake 現已正式推出。	2023 年 5 月 30 日
<a href="#">新功能</a>	Security Lake 現在會將指標傳送至 <a href="#">Amazon CloudWatch</a> 。	2023 年 5 月 4 日
<a href="#">區域可用性</a>	Security Lake 現已在下列地區提供 AWS 區域：亞太區域（新加坡）、歐洲（倫敦）和南美洲（聖保羅）。	2023 年 3 月 22 日

## 新功能

現在，當您使用 Security Lake 主控台 [啟用和開始使用 Security Lake](#) 時，Security Lake 會代表您建立 AWS Identity and Access Management (IAM) 角色。

2023 年 2 月 15 日

## 初始版本

這是 Amazon Security Lake 使用者指南的初始版本。

2022 年 11 月 29 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。