aws

使用者指南

Amazon Security Lake

Amazon Security Lake: 使用者指南

Table of Contents

什麼是亞馬遜安全湖？

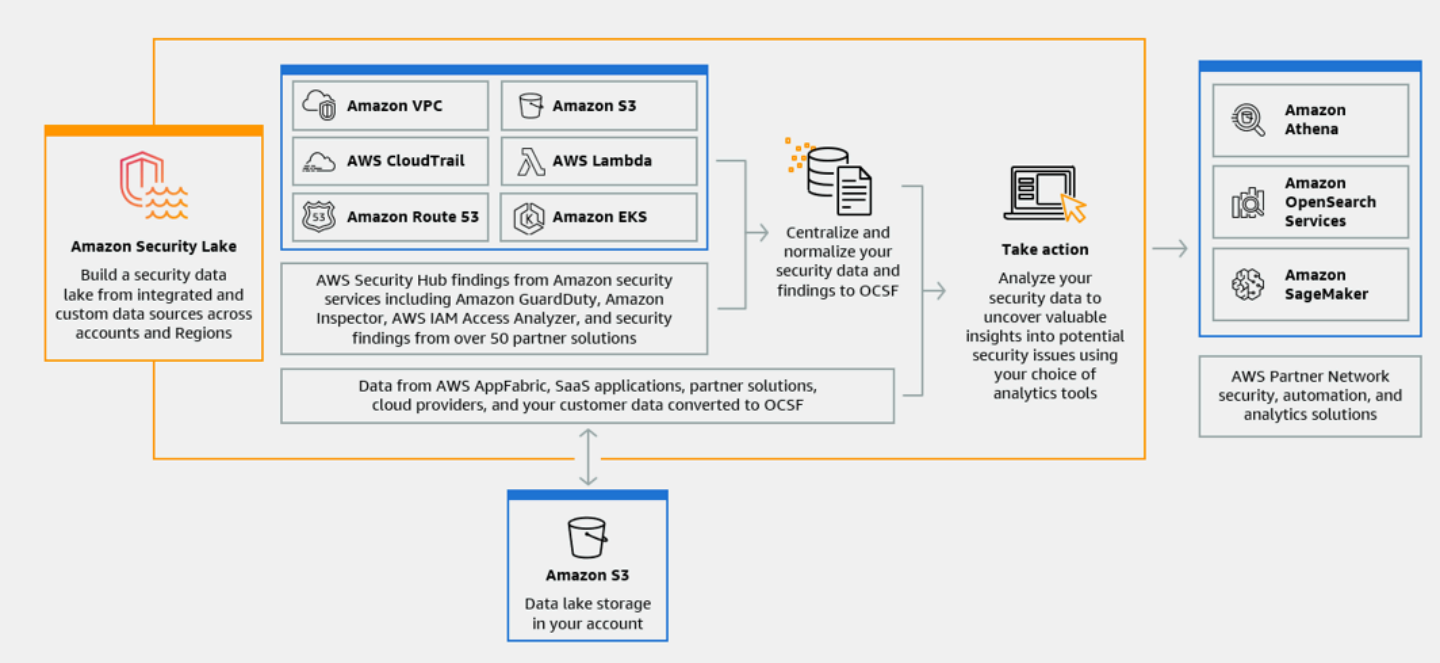
亞馬遜安全湖是一種全受管的安全性資料湖服務。您可以使用 Security Lake，將來自環AWS境、SaaS 供應商、內部部署、雲端來源和第三方來源的安全性資料，自動集中到儲存在您的. AWS 帳戶 Security Lake 可協助您分析安全性資料，讓您更全面地瞭解整個組織的安全性狀態。透過 Security Lake，您還可以改善工作負載、應用程式和資料的保護。

資料湖由 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體提供支援，您可以保留資料的擁有權。

Security Lake 會自動從整合式和協力廠商服務收集與安全性相關的記錄檔AWS 服務和事件資料。它還可以透過可自訂的保留和複寫設定，協助您管理資料的生命週期。安全湖將擷取的資料轉換為 Apache Parquet 格式，以及稱為開放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 可將來自各種企業安全性資料來源的安全性資料標準化AWS並結合。

其他AWS 服務和第三方服務可以訂閱儲存在 Security Lake 中的資料，以進行事件回應和安全性資料分析。

安全湖概述



安全湖的特點

以下是 Security Lake 協助您集中化、管理和訂閱安全性相關記錄檔和事件資料的一些重要方法。

資料彙總到您的帳戶

Security Lake 會在您的帳戶中建立專用的安全性資料湖。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記錄和事件資料。資料湖由 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體提供支援，您可以保留資料的擁有權。

各種支援的記錄檔和事件來源

Security Lake 會從多個來源 (包括內部部署和協力廠商服務) 收集安全性記錄檔和事件。AWS 服務擷取日誌後，無論來源為何，您都可以集中存取記錄並管理其生命週期。如需 Security Lake 從中收集記錄檔和事件之來源的詳細資訊，請參閱 Amazon Security Lake ake ake ake ake ake ake ake 鍵

數據轉換和規範化

Security Lake 會自動分割來自本地支援的傳入資料，AWS 服務並將其轉換為儲存和查詢效率的 Parquet 格式。它還將本地支持AWS 服務的數據轉換為開放網絡安全架構框架（OCSF）開源模式。這使得數據與其他AWS 服務和第三方提供商兼容，而無需後處理。由於 Security Lake 將資料標準化，因此許多安全性解決方案可以同時使用此資料。

訂閱者的多種存取層級

訂閱者使用儲存在安全湖中的資料。您可以選擇訂閱者對您資料的存取層級。訂閱者只能使用您指定之來源和AWS 區域中的資料。訂閱者可能會在寫入資料湖時自動收到有關新物件的通知。或者，訂閱者可以從資料湖查詢資料。安全湖自動創建和交換安全湖和用戶之間所需的憑據。

多帳戶和多區域資料管理

您可以跨所有可用的區域以及跨多個集中啟用 Security Lake AWS 帳戶。在 Security Lake 中，您也可以指定彙總區域，以合併來自多個區域的安全性記錄檔和事件資料。這有助於您遵守資料落地法規遵循要求。

可配置和可定制

安全湖是可配置和可定制的服務。您可以指定要設定記錄收集的來源、帳戶和區域。您也可以指定訂戶對資料湖的存取層級。

資料生命週期管理與優化

Security Lake 透過自動化儲存分層功能，透過可自訂的保留設定和儲存成本來管理資料的生命週期。安全湖自動分區和傳入的安全數據轉換為存儲和查詢高效的 Apache 拼花格式。

存取安全湖

如需目前提供安全湖泊的區域清單，請參閱Amazon Security Lake Security Lake Security Lake。若要深入了解區域，請參閱 AWS AWS 一般參考.

在每個區域中，您可以透過下列任何一種方式存取安全湖：

AWS Management Console

這AWS Management Console是一個基於瀏覽器的介面，您可以使用它來建立和管理AWS資源。安全湖控制台可讓您存取安全湖帳戶和資源。您可以使用安全湖主控台執行大部分的安全湖工作。

安全湖 API

若要以程式設計方式存取安全湖泊，請使用安全湖 API，並直接向服務發出 HTTPS 要求。如需詳細資訊，請參閱安全性湖 API 參考。

AWS Command Line Interface (AWS CLI)

使用AWS CLI，您可以在系統的命令列中發出指令，以執行 Security Lake 工作和AWS工作。使用命令行可以比使用控制台更快，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。如需安裝與使用 AWS CLI 的資訊，請參閱《AWS Command Line Interface》。

AWS SDK

AWS提供包含程式庫和範例程式碼的開發套件，適用於各種程式設計語言和平台，例如 Java、Go、Python、C++ 和 .NET。SDK 提供方便的程式設計存取安全湖和其他功能。AWS 服務他們還處理諸如密碼編譯簽名請求，管理錯誤以及自動重試請求等任務。如需安裝和使用 AWS SDK 的詳細資訊，請參閱建置在其上AWS的工具。

相關服務

以下是安全湖使用的其他AWS 服務內容：

- 亞馬遜 EventBridge — Security Lake EventBridge 用於在將物件寫入資料湖時通知訂閱者。
- AWS Glue— Security Lake 使用AWS Glue檢索器建立資料AWS Glue Data Catalog表，並將新寫入的資料傳送至「資料目錄」。Security Lake 也會在「資料目錄」中儲存AWS Lake Formation表格的分割區中繼資料。
- AWS Lake Formation-安全湖為每個源創建一個單獨的湖泊形成表，為安全湖提供數據。Lake Formation 表格包含每個來源資料的相關資訊，包括結構描述、分割區和資料位置資訊。訂閱者可以選擇透過查詢湖泊形成表來使用資料。

- AWS Lambda— Security Lake 使用 Lambda 函數支援原始資料上的擷取、轉換和載入 (ETL) 任務，以及在AWS Glue中註冊來源資料的分區。
- 亞馬遜 S3 — 安全湖將您的資料存放為 Amazon S3 物件。儲存類別和保留設定是以 Amazon S3 供應項目為基礎。安全湖不支持亞馬遜 S3 選擇。

除了下列項目之外，安全性湖還會從自訂來源收集資料AWS 服務：

- AWS CloudTrail管理和資料事件 (S3、Lambda)
- Amazon Route 53 Resolver 查詢日誌
- AWS Security Hub 問題清單
- 亞馬遜虛擬私有雲 (亞馬遜 VPC) 流程日誌

如需這些來源的詳細資訊，請參閱收集資料 AWS 服務。您可以建立可讀取 OCSF 結構描述中資料的訂閱者，以使用安全資料湖中的 Amazon S3 物件。您也可以使用亞馬遜雅典娜、Amazon Redshift 以及與AWS Glue之整合的第三方訂閱服務來查詢資料。

概念和術語

本節說明可協助您使用 Amazon Simple Storage Service 和術語。

貢獻地區

為彙總區域貢獻資料的一或多AWS 區域個。

資料湖

存放於 Amazon Simple Storage Service (Amazon S3)，且由安全湖管理的持續資料。安全湖使用 AWS Glue將新寫入的資料傳送至資料目錄。Security Lake 也會為每個將資料提供給資料湖的來源建立一個AWS Lake Formation表格。資料湖通常會儲存下列項目：

- 結構化和非結構化資料
- 原始資料和轉換資料

Security Lake 是一項資料湖服務，專為收集與安全性相關的記錄檔和事件而設計。

開放網路安全架構架構架構 (OCSF)

安全日誌和事件的標準化開放原始碼結構描述。它是由AWS各種安全領域的其他安全行業領導者開發的。安全湖會自動將其收集的記錄檔和事件AWS 服務轉換為 OCSF 結構描述。自訂來源會將其記錄檔和事件轉換為 OCSF，然後再將其傳送至安全湖。

累計區域

合併AWS 區域來自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遵守地區法規遵循要求。

來源

從單一系統產生的一組記錄檔和事件，符合 OCSF 中的特定事件類別。安全湖可從來源收集資料。來源可能是其他服務，AWS 服務也可能是第三方服務。對於第三方來源，您必須先將資料轉換為 OCSF 結構描述，然後才能將其傳送至安全湖。

Subscriber

消耗來自安全湖泊的記錄檔和事件的服務。訂閱者可能是其他服務AWS 服務或第三方服務。

開始使用 Amazon 安全湖

本節說明如何啟用和開始使用安全湖泊。您將學習如何設定資料湖設定和設定記錄收集。您可以透過 AWS Management Console 或以程式設計方式啟用和使用安全性湖泊。無論您使用哪種方法，都必須先設定 AWS 帳戶 和系統管理使用者。之後的步驟根據訪問方法而有所不同。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。

初始 AWS 帳戶 設定

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 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，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為最佳安全實務，將管理存取權指派給管理使用者，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 註冊過程完成後，會向您發送確認電子郵件。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。

建立管理使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console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)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立管理使用者

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，將管理權限授予管理使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

識別您將用來啟用安全湖泊的帳戶

安全湖與 AWS Organizations 整合，可管理組織中多個帳戶的記錄收集。如果您想要為組織使用 Security Lake，則必須使用您的組 Organizations 管理帳戶來指定委派的 Security Lake 管理員。然後，您必須使用委派系統管理員的認證來啟用 Security Lake、新增成員帳戶，並為其啟用 Security Lake。如需詳細資訊，請參閱 管理多個帳戶 AWS Organizations。

或者，您可以針對不屬於組 Organizations 的獨立帳戶使用 Security Lake，而不需要組織整合。

啟用 Amazon 安全湖時的考量

啟用安全湖之前，請考慮下列事項：

- Security Lake 提供跨區域管理功能，這表示您可以建立資料湖並設定跨 AWS 區域區域的記錄收集。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地區端點。您也可以新增彙總區域，將多個區域的資料彙總至單一區域。

- 我們建議您在所有支持的中激活安全湖 AWS 區域。如果您這麼做，Security Lake 可以收集與未經授權或不尋常活動相關的資料，即使在您未主動使用的區域也是如此。如果未在所有支援的區域中啟動 Security Lake，則會降低從您在多個區域使用的其他服務收集資料的能力。
- 當您在任何地區首次啟用 Security Lake 時，它會為`AWSServiceRoleForSecurityLake`您的帳戶建立服務連結角色。此角色包括代表您呼叫其他 AWS 服務 人並操作安全性資料湖的權限。如需服務連結角色如何運作的詳細資訊，請參閱 IAM 使用者指南中的使用服務連結角色。如果您啟用 Security Lake 作為委派的安全湖管理員，Security Lake 會在組織中的每個成員帳戶中建立服務連結角色。
- 安全湖不支援 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標準化記錄資料至資料湖的傳遞。

在主控台上開始使用

本教學課程說明如何啟用和設定安全湖透過 AWS Management Console. 作為其中的一部分 AWS Management Console，Security Lake 主控台提供簡化的入門流程，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 會收集來自各種來源以及您 AWS 帳戶 和的記錄檔和事件資料 AWS 區域。請遵循這些指示，識別您希望安全湖收集哪些資料。您只能使用這些指示來新增原生支援的 AWS 服務 來源。若要取得有關新增自訂來源的資訊，請參閱從自訂來源收集資料。

若要設定記錄來源收集

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 使用頁面右上角的選取 AWS 區域 器，選取 [區域]。您可以在上線時啟用目前區域和其他區域的安全性湖泊。
3. 選擇開始使用。
4. 針對 [選取記錄檔和事件來源]，選擇下列其中一個選項：

    a. 內嵌預設 AWS 來源 — 當您選擇建議的選項時， CloudTrail 不會包含 S3 資料事件進行擷取。這是因為擷取大量 S3 資料事件可能會大幅影響使用成本。 CloudTrail 若要內嵌此來源，請選取「內嵌特定 AWS 來源」選項。

    b. 內嵌特定 AWS 來源 — 使用此選項，您可以選取一或多個要擷取的記錄和事件來源。

> **Note**
>
> 當您第一次在帳戶中啟用 Security Lake 時，所有選取的記錄檔和事件來源都會是 15 天免費試用期的一部分。如需使用統計資料的詳細資訊，請參閱檢閱用量和預估成本。

5. 對於版本，請選擇您要從中擷取記錄檔和事件來源的資料來源版本。

> **Important**
>
> 如果您沒有在指定區域中啟用新版 AWS 記錄來源的必要角色權限，請聯絡 Security Lake 系統管理員。如需詳細資訊，請參閱更新角色權限。

6. 對於 「選取區域」，請選擇是否從所有支援的區域或特定區域內嵌記錄檔和事件來源。如果您選擇「特定區域」，請選取要從哪些區域擷取資料。
7. 對於服務存取，請建立新的 IAM 角色或使用現有的 IAM 角色，以授予 Security Lake 權限，從您的來源收集資料並將其新增至資料湖。在您啟用安全湖泊的所有區域中，都會使用一個角色。
8. 選擇下一步。

步驟 2：定義儲存設定和彙總區域 (選擇性)

您可以指定希望安全湖存放資料的 Amazon S3 儲存類別以及存放資料的時間。您也可以指定彙總區域，以合併來自多個區域的資料。這些是可選步驟。如需詳細資訊，請參閱 安全湖中的生命週期管理。

若要設定儲存和彙總設定

1. 如果您要將多個貢獻區域的資料合併至累計區域，請針對「選取累計區域」選擇「新增累計區域」。指定彙總「區域」和將貢獻給它的「區域」。您可以設定一或多個彙總區域。
2. 對於選取的儲存類別，請選擇 Amazon S3 儲存類別。預設儲存類別為 S3 標準。如果您希望資料在該時間之後轉換至另一個儲存類別，請提供保留期間 (以天為單位)，然後選擇 [新增轉換]。保留期結束後，物件會過期，Amazon S3 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彙總區域，請針對服務存取建立新的 IAM 角色，或使用現有的 IAM 角色，以授予 Security Lake 跨多個區域複寫資料的權限。
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、彙總區域以及您的保留設定。然後，建立您的資料湖。

檢閱和建立資料湖的步驟

1. 啟用 Security Lake 時，請檢閱記錄和事件來源、區域、彙總區域和儲存區類別。
2. 選擇建立。

建立資料湖之後，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」數目的總覽、訂戶和問題的相關資訊。

「問題」功能表會顯示過去 14 天影響安全湖服務或 Amazon S3 儲存貯體的問題摘要。如需每個問題的其他詳細資訊，您可以移至 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資料 AWS Lake Formation 庫和表格中的資料。當您使用主控台時，Security Lake 會自動將資料庫檢視權限授與您用來啟用 Security Lake 的角色。角色至少必須具有資料分析師權限。如需有關權限等級的詳細資訊，請參閱 Lake Formation 角色和 IAM 許可參考。如需授與SELECT權限的指示，請參閱AWS Lake Formation 開發人員指南中的使用具名資源方法授與資料目錄權限。

步驟 5：建立訂閱者

建立資料湖後，您可以新增訂閱者以使用您的資料。訂閱者可以直接存取 Amazon S3 儲存貯體中的物件或查詢資料湖來使用資料。如需有關訂閱者的詳細資訊，請參閱Amazon 安全湖中的訂閱者管理。

以編程方式開始

本教學課程說明如何以程式設計方式啟用和開始使用安全湖。Amazon 安全湖 API 可讓您以程式設計方式全面地存取安全湖帳戶、資料和資源。或者，您可以使用 AWS 命令行工具（ AWS Command Line Interface或用於 PowerShell-的AWS 工具 ）或 AWS SDK 來訪問安全湖。

步驟 1：建立 IAM 角色

如果您以程式設計方式存取 Security Lake，則必須建立一些 AWS Identity and Access Management (IAM) 角色，才能設定資料湖。

> **Important**
>
> 如果您使用安全湖主控台啟用和設定安全湖，則不需要建立這些 IAM 角色。

如果您要執行以下一或多個動作，則必須在 IAM 中建立角色 (選擇連結以查看每個動作的 IAM 角色的詳細資訊)：

- 建立自訂來源 — 自訂來源是將資料傳送至 Security Lake 的本機支援以外 AWS 服務 的來源。
- 建立具有資料存取權的訂閱者 — 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 — 彙總區域會合併多個 AWS 區域資料。

建立前面提到的角色之後，請將AmazonSecurityLakeAdministrator AWS 受管理的原則附加至您用來啟用 Security Lake 的角色。此原則會授與管理權限，允許主體登入 Security Lake 並存取所有安全性湖泊動作。

附加受AmazonSecurityLakeMetaStoreManager AWS 管理的政策，以建立資料湖或從 Security Lake 查詢資料。此原則對於 Security Lake 來支援從來源接收的原始記錄檔和事件資料上的擷取、轉換和載入 (ETL) 工作是必要的。

步驟 2：啟用 Amazon 安全湖

若要以程式設計方式啟用安全性湖泊，請使用安全湖 API 的CreateDataLake作業。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`欄位來指定要在其中啟用 Security Lake 的地區代碼。如需區域代碼的清單，請參閱 AWS 一般參考.

範例 1

下列範例命令會啟用`us-east-1`和`us-east-2`區域中的安全性湖泊。在這兩個區域中，此資料湖都使用 Amazon S3 受管金鑰加密。物件會在 365 天後過期，物件會在 60 天後轉換至 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

下列範例命令會啟用us-east-2區域中的安全性湖泊。此資料湖使用 AWS Key Management Service (AWS KMS) 中建立的客戶管理金鑰加密。物件會在 500 天後過期，物件會在 30 天後轉換至 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作業，或者如果使用update-data-lake命令。 AWS CLI不要使用該CreateDataLake操作。

步驟 3：設定來源

Security Lake 會收集來自各種來源以及您 AWS 帳戶 和的記錄檔和事件資料 AWS 區域。請遵循這些指示，識別您希望安全湖收集哪些資料。您只能使用這些指示來新增原生支援的 AWS 服務 來源。若要取得有關新增自訂來源的資訊，請參閱從自訂來源收集資料。

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作業。針對每個來源，指定參數的區域唯一sourceName值。選擇性地使用其他參數，將來源範圍限制為特定帳戶 (accounts) 或特定版本 (sourceVersion)。

> **Note**
>
> 如果您未在要求中包含選用參數，Security Lake 會根據您排除的參數，將您的要求套用至所有帳戶或指定來源的所有版本。例如，如果您是組織的委派 Security Lake 系統管理員，而您排

除accounts參數，Security Lake 會將您的要求套用至組織中的所有帳戶。同樣地，如果您排除sourceVersion參數，Security Lake 會將您的要求套用至指定來源的所有版本。

如果您的請求指定了尚未啟用安全湖泊的區域，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 的那些區域。或者，您可以在該地區啟用安全湖，然後再次提交您的請求。

當您第一次在帳戶中啟用 Security Lake 時，所有選取的記錄檔和事件來源都會是 15 天免費試用期的一部分。如需使用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)

您可以指定希望安全湖存放資料的 Amazon S3 儲存類別以及存放資料的時間。您也可以指定彙總區域，以合併來自多個區域的資料。這些是可選步驟。如需詳細資訊，請參閱 安全湖中的生命週期管理。

若要在啟用安全湖泊時以程式設計方式定義目標，請使用 Security Lake API 的CreateDataLake作業。如果您已啟用 Security Lake，並且想要定義目標，請使用UpdateDataLake作業，而非CreateDataLake作業。

對於任一作業，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提供給彙總區域的「區域」。在replicationConfiguration物件regions陣列中，指定每個彙總「區域」的「地區」代碼。如需區域代碼的清單，請參閱 AWS 一般參考.
- 若要指定資料的保留設定，請使用下列lifecycleConfiguration參數：
  - 針對transitions，指定要在特定 Amazon S3 儲存類別中存放 S3 物件的總天數 (storageClass)。days
  - 對於expiration，指定建立物件後，使用任何儲存類別在 Amazon S3 中存放物件的總天數。此保留期結束時，物件會過期，Amazon S3 會刪除物件。

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

例如，下列命令會以彙總區域的ap-northeast-2形式建立資料湖。該us-east-1地區將為該地ap-northeast-2區貢獻數據。此範例也會為新增至資料湖的物件建立 10 天的到期期限。

```
$ 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"
```

您現在已建立資料湖。使用 Security Lake API 的ListDataLakes操作來驗證啟用安全湖泊和您在每個區域中的資料湖設定。

如果在建立資料湖時出現問題或錯誤，您可以使用ListDataLakeExceptions作業來檢視例外清單，並通知使用者有關CreateDataLakeExceptionSubscription作業的例外狀況。如需詳細資訊，請參閱 疑難排解資料湖狀態。

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資料 AWS Lake Formation 庫和表格中的資料。當您以程式設計方式啟用 Security Lake 時，不會自動授與資料庫檢視權限。中的資料湖管理員帳戶 AWS Lake Formation 必須將SELECT許可授與您要用來查詢相關資料庫和表格的 IAM 角色。角色至少必須具有資料分析師權限。如需有關權限等級的詳細資訊，請參閱 Lake Formation 角色和 IAM 許可參考。如需授與SELECT權限的指示，請參閱AWS Lake Formation 開發人員指南中的使用具名資源方法授與資料目錄權限。

步驟 6：建立訂閱者

建立資料湖後，您可以新增訂閱者以使用您的資料。訂閱者可以直接存取 Amazon S3 儲存貯體中的物件或查詢資料湖來使用資料。如需有關訂閱者的詳細資訊，請參閱Amazon 安全湖中的訂閱者管理。

管理多個帳戶 AWS Organizations

您可以使用 Amazon 安全湖收集來自多個安全日誌和事件 AWS 帳戶。為了協助自動化和簡化多個帳戶的管理，我們強烈建議您將 Security Lake 與 AWS Organizations.

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

委派的安全湖管理員可以啟用安全湖泊，並為成員帳戶設定安全性湖泊設定。委派的系統管理員可以在啟用 Security Lake 的所有組織內收集記錄檔和事件 (無論他們目前使用的是 AWS 區域 哪個區域端點)。委派的系統管理員也可以設定 Security Lake，以自動收集新組織帳戶的記錄檔和事件資料。

委派的 Security Lake 管理員可以存取關聯成員帳戶的記錄和事件資料。因此，他們可以將 Security Lake 設定為收集關聯成員帳戶所擁有的資料。他們還可以授予訂閱者使用關聯成員帳戶擁有的數據的權限。

若要為組織中的多個帳戶啟用 Security Lake，組織管理帳戶必須先指定組織的委派 Security Lake 管理員帳戶。然後委派的系統管理員可以啟用和設定組織的安全性湖泊。

如需有關設定「組 Organizations」的資訊，請參閱《AWS Organizations 使用指南》中的〈建立和管理組織〉。

委派安全湖系統管理員的重要考量

請注意下列定義委派系統管理員在 Security Lake 中的行為方式的因素：

委派的管理員在所有區域中都是相同的。

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

我們建議您將記錄封存帳戶設定為安全湖委派的系統管理員。

記錄封存帳戶是專門用來擷取和封存所有安全性相關記錄檔的帳戶。 AWS 帳戶 此帳戶的存取權通常僅限於少數使用者，例如稽核員和安全團隊進行合規性調查。建議您將記錄封存帳戶設定為 Security Lake 委派的系統管理員，以便您可以在最少的內容切換的情況下檢視安全性相關的記錄檔和事件。

此外，我們建議只有最少的一組使用者可以直接存取「記錄封存」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，您可以將其新增為 Security Lake 訂閱者。有關如何添加訂戶的更多內容，敬請參閱Amazon 安全湖中的訂閱者管理。

如果您不使用該 AWS Control Tower 服務，則可能沒有日誌存檔帳戶。如需記錄封存帳戶的詳細資訊，請參閱安全性 OU — AWS 安全性參考架構中的記錄封存帳戶。

一個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的系統管理員。

根據 AWS 安全性最佳作法和最低權限原則，您的組織管理帳戶無法成為委派的系統管理員。

委派的管理員必須是使用中組織的一部分。

當您刪除組織時，委派的系統管理員帳戶將無法再管理 Security Lake。您必須指定來自不同組織的委派管理員，或將 Security Lake 與不屬於組織的獨立帳戶搭配使用。

指定委派管理員所需的 IAM 許可

指定委派的 Security Lake 管理員時，您必須擁有啟用 Security Lake 的權限，並使用下列原則陳述式中列出的特定 AWS Organizations API 作業。

您可以在 AWS Identity and Access Management (IAM) 政策的結尾新增下列陳述式，以授與這些權限。

```
{
    "Sid": "Grant permissions to designate a delegated Security Lake administrator",
    "Effect": "Allow",
    "Action": [
        "securitylake:RegisterDataLakeDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

指定委派的安全湖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指定其組織的委派管理員帳戶。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安全湖`RegisterDataLakeDelegatedAdministrator`作業來指定委派的安全湖系統管理員帳戶。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，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. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   使用您組織的管理帳戶認證登入。

2. - 如果尚未啟用 Security Lake，請選取 [開始使用]，然後在 [啟用安全湖泊] 頁面上指定委派的 Security Lake 管理員。
   - 如果已啟用安全湖泊，請在 [設定] 頁面上指定委派的 Security Lake 管理員。
3. 在 [將管理委派給其他帳戶] 底下，選取已經擔任其他 AWS 安全性服務委派系統管理員的帳戶 (建議選項)。或者，輸入您要指定為委派 Security Lake 管理員之帳戶的 12 位數 AWS 帳戶 識別碼。
4. 選擇委派。如果尚未啟用 Security Lake，指定委派的系統管理員會為您目前區域中的該帳戶啟用安全湖。

API

若要以程式設計方式指定委派的系統管理員，請使用 Security Lake API 的RegisterDataLakeDelegatedAdministrator作業。您必須從組織管理帳戶呼叫作業。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`參數來指定要指定為組織委派管理員帳戶的 12 位數帳戶 ID。 AWS 帳戶

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
```

委派的管理員也可以選擇自動收集新組織帳戶的 AWS 記錄檔和事件資料。透過此設定，當帳戶新增至中的組織時，新帳戶中會自動啟用 Security Lake AWS Organizations。身為委派的管理員，您可以使用 Security Lake API 的CreateDataLakeOrganizationConfiguration操作來啟用此組態，或者，如果您使用的是 AWS CLI，則可以執行create-data-lake-organization-configuration命令來啟用此組態。在您的要求中，您也可以指定新帳戶的特定組態設定。

例如，以下 AWS CLI 命令會在新的組織帳戶中自動啟用安全湖和 Amazon Route 53 解析器查詢日誌、 AWS Security Hub 發現項目和 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"}]}]'
```

組織管理帳戶指定委派的系統管理員之後，系統管理員可以啟用和設定組織的 Security Lake。這包括啟用和設定 Security Lake，以收集組織中個別帳戶的 AWS 記錄檔和事件資料。如需詳細資訊，請參閱 收集資料 AWS 服務。

您可以使用此GetDataLakeOrganizationConfiguration作業取得有關組織目前新成員帳戶組態的詳細資料。

移除委派的安全湖管理員

只有組織管理帳戶可以移除其組織的委派 Security Lake 系統管理員。如果您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安全性湖泊。

您無法使用 Security Lake 主控台來變更或移除委派的系統管理員。這些工作只能以程式設計方式執行。

若要以程式設計方式移除委派的系統管理員，請使用 Security Lake API 的DeregisterDataLakeDelegatedAdministrator作業。您必須從組織管理帳戶呼叫作業。如果您正在使用 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 系統管理員。

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

若要保留委派的系統管理員指定，但變更新成員帳戶的自動組態設定，請使用 Security Lake API 的DeleteDataLakeOrganizationConfiguration作業，或者，如果您使用的 AWS CLI是delete-data-lake-organization-configuration命令。只有委派的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 發現項目。委派的系統管理員呼叫此作業之後，新成員帳戶不會將 Security Hub 發現項目提供給資料湖。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"}]}]'
```

安全湖受信任的存取

在您為組織設定安全性湖泊之後， AWS Organizations 管理帳戶可以透過 Security Lake 啟用受信任的存取。受信任的存取可讓 Security Lake 建立 IAM 服務連結角色，並代表您在組織及其帳戶中執行工作。若要取得更多資訊，請參閱《使 AWS Organizations 用AWS Organizations 者指南》 AWS 服務中的〈與其他配合

身為組織管理帳戶的使用者，您可以在中停用安全性湖泊的受信任存取權 AWS Organizations。如需停用受信任存取權的指示，請參閱《AWS Organizations 使用指南》中的如何啟用或停用受信任存取。

如果委派的 AWS 帳戶 系統管理員已暫停、隔離或關閉，我們建議您停用受信任的存取。

管理 區域

Amazon 安全湖可以收集您 AWS 區域 在其中啟用服務的安全日誌和事件。對於每個區域，您的資料都存放在不同的 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。

檢查地區狀態

安全湖可以跨多個收集數據 AWS 區域。若要追蹤資料湖的狀態，瞭解每個區域目前的設定方式會很有幫助。選擇您偏好的存取方式，然後依照下列步驟取得區域的目前狀態。

Console

若要檢查地區狀態

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 在導覽窗格中，選擇 [區域]。便會顯示「區域」頁面，提供目前啟用「安全湖泊」之區域的簡介。
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記錄檔收集的狀態，請使用安全湖 API 的GetDataLakeSources作業。如果您使用的是 AWS CLI，請執行get-data-lake-sources命令。對於`accounts`參數，請指定一個或多個 AWS 帳戶 ID 作為清單。如果您的要求成功，Security Lake 會傳回目前區域中這些帳戶的快照，包括 Security Lake 收集資料的 AWS 來源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已設定 Security Lake 之所有帳戶的記錄收集狀態。

例如，下列 AWS CLI 命令會擷取目前區域中指定帳戶的記錄收集狀態。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記錄收集狀態。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]'
```

若要判斷您是否已為某個區域啟用安全性湖泊，請使用此ListDataLakes作業。如果您使用的是 AWS CLI，請執行list-data-lakes命令。對於regions參數，請指定區域的區域代碼 — 例如，us-east-1美國東部 (維吉尼亞北部) 區域。如需區域代碼的清單，請參閱 AWS 一般參考. 此ListDataLakes作業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 會傳回資料湖在每個可用 Security Lake 的區域中的狀態和組態設定。

例如，下列 AWS CLI 命令會顯示「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，然後依照下列指示更新一或多個資料湖的設定 AWS 區域。

Console

1. 開啟安全湖主控台，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. 勾選「覆寫中所有帳戶的來源」核取方塊，以確認您在<Region>此處的選項會覆寫此區域先前的選項。
5. 對於 [選取儲存空間類別]，請選擇 [新增轉換]，為資料新增新的儲存類別。
6. 對於「標籤」，選擇性地指定或編輯「區域」的標籤。標籤是一種標籤，您可以定義並指派給特定類型的 AWS 資源，包括特定區域 AWS 帳戶 中的資料湖組態。如需進一步了解，請參閱標記 Amazon 安全湖資源。
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」段落中，選擇「新增累計區域」。選取貢獻的區域，並向 Security Lake 提供跨多個區域複寫資料的權限。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 的UpdateDataLake作業。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，us-east-1例如美國東部 (維吉尼亞北部) 區域。如需區域代碼的清單，請參閱 AWS 一般參考.

使用其他參數為您要變更的每個設定指定新值，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」的資料到期時間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"}]}}]'
```

設定彙總區域

彙總區域會合併來自一或多個貢獻區域的資料。指定彙總區域可協助您遵循區域法規遵循要求。

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：

- 資料複寫的 IAM 角色
- 用於註冊 AWS Glue 分區的 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，您必須在使用安全湖 API 或時建立這些角色 AWS CLI。

資料複寫的 IAM 角色

此 IAM 角色授予 Amazon S3 的許可，以跨多個區域複寫來源日誌和事件。

若要授與這些權限，請建立以前置詞開頭的 IAM 角色SecurityLake，並將下列範例政策附加至該角色。當您在安全湖中建立彙總區域時，您需要角色的 Amazon 資源名稱 (ARN)。在這個原則中，sourceRegions是貢獻區域，而且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}}"
          ]
        }
      }
    }
  ]
}
```

將下列信任政策附加到您的角色，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) 的客戶管理金鑰來加密 Security Lake 資料湖，除了資料複寫原則中的權限外，還必須授與下列權限。

```
{
    "Action": [
        "kms:Decrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "s3.{sourceRegion1}.amazonaws.com",
                "s3.{sourceRegion2}.amazonaws.com"
                ],
            "kms:EncryptionContext:aws:s3:arn": [
```

```
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion1}*",
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion2}*"
            ]
        }
    },
    "Resource": [
        "{sourceRegion1KmsKeyArn}",
        "{sourceRegion2KmsKeyArn}"
    ]
},
{
    "Action": [
        "kms:Encrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
            "s3.{destinationRegion1}.amazonaws.com",
            ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{destinationRegion1}*",
            ]
        }
    },
    "Resource": [
            "{destinationRegionKmsKeyArn}"
    ]
}
```

如需有關複寫角色的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的設定許可。

用於註冊 AWS Glue 分區的 IAM 角色

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

若要授與這些權限，請建立名為的角色 `AmazonSecurityLakeMetaStoreManager` (您可能已在上線至 Security Lake 時建立此角色)。如需有關此角色的詳細資訊 (包括範例原則)，請參閱步驟 1：建立 IAM 角色。

在 Lake Formation 主控台中，您還必須按照下列步驟
授AmazonSecurityLakeMetaStoreManager予以資料湖管理員身份的權限：

1. 開啟 Lake Formation 主控台，網址為 https://console.aws.amazon.com/lakeformation/。
2. 以系統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，請執行以下步驟來配置 Lake Formation 管理員。

    1. 在功能窗格的 [權限] 下，選擇 [系統管理角色和工作]。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，對於 IAM 使用者和角色，請選擇您建立的 AmazonSecurityLakeMetaStoreManagerIAM 角色，然後選擇 [儲存]。

如需有關變更資料湖管理員權限的詳細資訊，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式，然後依照下列步驟新增彙總區域。

> **Note**
>
> 一個區域可以將資料貢獻給多個彙總區域。不過，累計區域不能是其他累計區域的貢獻「區域」。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 在功能窗格的 [設定] 底下，選擇 [彙總區域]。
3. 選擇 「修改」，然後選擇「新增累計區域」。
4. 指定彙總「區域」與「貢獻區域」。如果您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，請針對服務存取建立新的 IAM 角色，或使用現有的 IAM 角色，以授予 Security Lake 跨多個區域複寫資料的權限。

6. 完成後，請選擇儲存。

您也可以在登機前往安全湖時新增彙總區域。如需詳細資訊，請參閱 開始使用 Amazon 安全湖。

API

若要以程式設計方式新增彙總套件區域，請使用安全性湖 API 的UpdateDataLake作業。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region欄位來指定您要將資料提供給彙總區域的「區域」。在replicationConfiguration參數regions陣列中，指定每個彙總「區域」的「地區」代碼。如需區域代碼的清單，請參閱 AWS 一般參考.

例如，下列命令會設定ap-northeast-2為彙總區域。該us-east-1地區將為該地ap-northeast-2區貢獻數據。此範例也會為新增至資料湖的物件建立 365 天的到期期限。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}}}]'
```

您也可以在登機前往安全湖時新增彙總區域。若要執行此CreateDataLake操作，請使用作業 (如果使用 AWS CLI，則使用create-data-lake指令)。如需在上線期間設定彙總區域的詳細資訊，請參閱開始使用 Amazon 安全湖。

更新或移除彙總套件區域

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

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 在功能窗格的 [設定] 底下，選擇 [彙總區域]。
3. 選擇 Modify (修改)。
4. 若要變更累計區域的貢獻區域，請在累計區域的資料列中指定更新的貢獻區域。
5. 若要移除累計區域，請在累計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，請使用安全性湖 API 的UpdateDataLake作業。如果您使用的是 AWS CLI，請執行update-data-lake命令。在您的要求中，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欄位來指定要新增之「地區」的「地區」代碼。在replicationConfiguration物件的regions陣列中，指定要提供資料的每個彙總 [區域] 的 [區域] 代碼。如需區域代碼的清單，請參閱 AWS 一般參考.
- 若要移除貢獻區域，請使用region欄位指定要移除之「地區」的「地區」代碼。對於replicationConfiguration參數，請勿指定任何值。

例如，下列命令會將us-east-1和設定us-east-2為貢獻區域。這兩個區域都會將資料貢獻給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"}]}}]'
```

Amazon Security Lake ake ake ake ake ake ake ake 鍵

來源是從單一系統產生的記錄檔和事件，符合開放網路安全架構架構架構 (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，包括本機支援AWS 服務的第三方自訂來源。

Security Lake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake 鍵。Security Lake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake akeAWS 帳戶AWS 區域 Security Lake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake 鍵。每個來源都會在 S3 儲存貯體中取得個別的前置詞，而 Security Lake 會將來自每個來源的資料組織在單獨的一組AWS Lake Formation表格中。

主題

- 收集資料 AWS 服務
- 從自訂來源收集資料

收集資料 AWS 服務

Amazon 安全湖可以從以下本地 AWS 服務支持的日誌和事件收集日誌和事件：

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

安全湖自動將這些數據轉換為開放網路安全架構架構架構 (OCSF)和 Apache 鑲木地板格式。

> **Tip**
>
> 若要在 Security Lake 中新增一或多個先前服務做為記錄來源，除了 CloudTrail 管理事件之外，您不需要在這些服務中個別設定記錄。如果您已在這些服務中設定記錄，則不需要變更記

錄設定，即可將它們新增為 Security Lake 中的記錄來源。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。

先決條件：驗證權限

若要在安全湖中新增 AWS 服務 為來源，您必須擁有必要的權限。確認附加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權限：

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

建議角色具有和s3:PutObject權限的下列條件和資源範圍。S3:getObject

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

```
}
```

這些動作可讓您從中收集記錄和事件， AWS 服務 並將其傳送至正確的 AWS Glue 資料庫和表格。

如果您使用 AWS KMS 金鑰進行資料湖的伺服器端加密，您還需要的權限`kms:DescribeKey`。

CloudTrail 事件記錄

AWS CloudTrail 為您的帳戶提供 AWS API 呼叫的歷史記錄，包括使用、 AWS SDK AWS Management Console、命令列工具和特定 AWS 服務進行的 API 呼叫。 CloudTrail 也可讓您識別哪些使用者和帳戶呼叫 AWS API 以取得支援的服務 CloudTrail、呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

安全湖可以收集與 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 資料事件是安全湖中的三個獨立來源。因此，當您將其中一個新增為擷取的記錄來源`sourceName`時，它們會有不同的值。管理事件 (也稱為控制平面事件) 可針對您的資源執行的管理作業提供深入分析 AWS 帳戶。 CloudTrail 資料事件 (也稱為資料平面作業) 會顯示在您的 AWS 帳戶. 這些作業通常是高容量的活動。

若要在 Security Lake 中收集 CloudTrail 管理事件，您必須至少有一個收集讀取和寫入 CloudTrail 管理事件的 CloudTrail多區域組織追蹤。必須啟用追蹤的記錄功能。如果您已在其他服務中設定記錄，則不需要變更記錄設定，即可將它們新增為 Security Lake 中的記錄來源。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。

多區域追蹤可將多個區域的日誌檔案交付到單一 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體，只 AWS 帳戶需一個儲存貯體即可。如果您已經透過 CloudTrail 主控台管理多區域追蹤 AWS Control Tower，或者不需要採取進一步的動作。

- 若要取得有關建立和管理追蹤的資訊 CloudTrail，請參閱《AWS CloudTrail 使用指南》中的〈為組織建立追蹤〉。
- 如需建立和管理追蹤的相關資訊 AWS Control Tower，請參閱AWS Control Tower 使用者指南 AWS CloudTrail中的記錄 AWS Control Tower 動作。

當您將 CloudTrail 事件新增為來源時，Security Lake 會立即開始收集您的 CloudTrail 事件記錄檔。它會透 CloudTrail 過獨立且重複的事件串流，直接從中取用 CloudTrail 管理和資料事件。

安全湖不會管理您的 CloudTrail 事件，也不會影響您現有的 CloudTrail 設定。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 使用指南中的檢視具有 CloudTrail 事件歷程記錄的事件。

下列清單提供了 Security Lake 如何將 CloudTrail 事件標準化為 OCSF 的對應參照的 GitHub 儲存庫連結。

GitHub 用 CloudTrail 於事件的 OCSF 儲存庫

- 來源版本 1 (第 2 版)
- 來源版本 2 (1.1.0 版)

Amazon EKS 審計日誌

當您將 Amazon EKS 稽核日誌新增為來源時，安全湖開始收集有關在彈性 Kubernetes 服務 (EKS) 叢集中執行的 Kubernetes 資源上執行的活動的深入資訊。EKS 稽核記錄可協助您在 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 控制平面記錄功能使用 EKS 稽核日誌事件。此程序不需要進行任何額外的設定，也不會影響您可能擁有的任何現有 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。

如需安全湖如何將 EKS 稽核日誌事件標準化為 OCSF 的相關資訊，請參閱 Amazon EKS 稽核日誌事件的 GitHub OCSF 儲存庫中的對應參考。

Route 53 Resolver 查詢日誌

Route 53 解析器查詢日誌會追蹤 Amazon Virtual Private Cloud (Amazon VPC) 內資源所進行的 DNS 查詢。這可協助您瞭解應用程式的運作方式，並發現安全性威脅。

當您在 Security Lake 中新增 Route 53 解析器查詢記錄檔做為來源時，Security Lake 會立即開始透過獨立且重複的事件資料流直接從 Route 53 收集解析器查詢記錄檔。

安全湖不會管理您的 Route 53 記錄檔，也不會影響您現有的解析程式查詢記錄設定。若要管理解析程式查詢記錄檔，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器查詢記錄組態。

下列清單提供安全性湖如何將 Route 53 記錄標準化為 OCSF 的對應參照的 GitHub 儲存庫連結。

GitHub 適用於路由 53 記錄的 OCSF 儲存庫

- 來源版本 1 (第 2 版)
- 來源版本 2 (1.1.0 版)

Security Hub 發現

Security Hub 發現項目可協助您瞭解中的安全性狀態， AWS 並讓您根據安全性產業標準和最佳做法來檢查您的環境。Security Hub 會從各種來源收集發現項目，包括與其他 AWS 服務第三方產品整合的整合，並檢查 Security Hub 控制項。安全性中樞會以稱為「 AWS 安全性尋找格式 (ASFF)」的標準格式來處理發現項目。

當您將 Security Hub 發現項目新增為 Security Lake 中的來源時，Security Lake 會立即開始透過獨立且重複的事件串流直接從 Security Hub 收集您的發現項目。安全湖也將調查結果從 ASFF 轉換為開放網路安全架構架構架構 (OCSF)（OCSF）。

安全湖不會管理您的 Security Hub 發現項目，也不會影響您的 Security Hub 設定。若要管理 Security Hub 發現項目，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 使用指南 AWS Security Hub中的發現項目。

下列清單提供安全性湖泊如何將安全 Security Hub 發現項目標準化為 OCSF 的對應參照的 GitHub 儲存庫連結。

GitHub Security Hub 發現項目的 OCSF 儲存庫

- 來源版本 1 (第 2 版)
- 來源版本 2 (1.1.0 版)

VPC 流量日誌

Amazon VPC 的 VPC 流量日誌功能會擷取環境內網路界面進出 IP 流量的相關資訊。

當您將 VPC 流程記錄新增為安全湖中的來源時，安全湖會立即開始收集您的 VPC 流程記錄。它會透過獨立且重複的流程日誌串流，直接從 Amazon VPC 取用 VPC 流程日誌。

安全湖不會管理您的 VPC 流程日誌或影響您的 Amazon VPC 組態。若要管理流程日誌，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。

下列清單提供安全性湖泊如何將 VPC 流程記錄標準化為 OCSF 的對應參照的 GitHub 存放庫連結。

GitHub 適用於 VPC 流程記錄的 OCSF 儲存庫

- 來源版本 1 (第 2 版)
- 來源版本 2 (1.1.0 版)

新增 AWS 服務 為來源

新增 AWS 服務 為來源後，Security Lake 會自動開始從中收集安全性記錄檔和事件。這些說明會告訴您如何在 Security Lake 中新增原生支援 AWS 服務 的來源。如需新增自訂來源的指示，請參閱從自訂來源收集資料。

Console

若要新增 AWS 記錄來源 (主控台)

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 從導覽窗格中選擇「來源」。
3. 選取您 AWS 服務 要從中收集資料的來源，然後選擇設定。
4. 在「來源設定」區段中，啟用來源，然後選取要用於資料擷取的資料來源版本。根據預設，安全湖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 AWS 記錄來源的必要角色權限，請聯絡 Security Lake 系統管理員。如需詳細資訊，請參閱更新角色權限。

若要讓訂閱者內嵌選取的資料來源版本，您還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 安全湖中的訂閱者管理。

或者，您可以選擇僅內嵌最新版本，並停用用於資料擷取的所有先前來源版本。

5. 在「區域」段落中，選取您要收集來源資料的區域。Security Lake 將從所選區域中的所有帳戶收集來自來源的資料。
6. 選擇 啟用 。

API

若要新增 AWS 記錄來源 (API)

若要以程式設計方式新增 AWS 服務 為來源，請使用安全湖 API 的CreateAwsLogSource作業。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，您可以將來源範圍限制為特定`accounts`或特定範圍`sourceVersion`。

> **Important**
>
> 當您未在命令中提供參數時，Security Lake 會假設遺失的參數是指整個集合。例如，如果您未提供`accounts`參數，則此命令會套用至組織中的整組帳戶。

下列範例會將 VPC 流程記錄新增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**
>
> 如果您將此要求套用至尚未啟用安全湖泊的區域，則會收到錯誤訊息。您可以在該區域中啟用安全性湖泊，或使用`regions`參數僅指定已在其中啟用 Security Lake 的區域來解決錯誤。

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

更新角色權限

如果您沒有必要的角色許可或資源 (新 AWS Lambda 函數和 Amazon Simple Queue Service (Amazon SQS) 佇列 — 若要從新版本的資料來源擷取資料，您必須更新`AmazonSecurityLakeMetaStoreManagerV2`角色許可並建立一組新的資源來處理來自您來源的資料。

選擇您偏好的方法，然後依照指示更新您的角色權限，並建立新資源，以處理指定區域中新版 AWS 記錄來源的資料。這是一次性動作，因為權限和資源會自動套用至 future 的資料來源版本。

Console

若要更新角色權限 (主控台)

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   使用委派的安全湖管理員的認證登入。

2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。
3. 選擇 [更新角色權限]。
4. 在「服務存取」區段中，執行下列其中一項作業：
   - 建立並使用新的服務角色 — 您可以使用安全性湖泊建立的 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

若要更新角色權限 (API)

若要以程式設計方式更新權限，請使用安全湖 API 的UpdateDataLake作業。若要使用更新權限 AWS CLI，請執行update-data-lake命令。

若要更新角色權限，您必須將原AmazonSecurityLakeMetastoreManager則附加至角色。

刪除角 AmazonSecurityLakeMetaStoreManager 色

> **Important**
>
> 將角色權限更新為後AmazonSecurityLakeMetaStoreManagerV2，請先確認資料湖是否正常運作，然後再移除舊AmazonSecurityLakeMetaStoreManager角色。建議至少等待 4 個小時，然後再移除角色。

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

請按照以下步驟從 Lake Formation 控制台中刪除AmazonSecurityLakeMetaStoreManager角色。

1. 登錄到 AWS Management Console，並打開 Lake Formation 控制台 https://console.aws.amazon.com/lakeformation/。
2. 在 Lake Formation 主控台中，從導覽窗格中選擇 [系統管理角色和工作]。
3. AmazonSecurityLakeMetaStoreManager從每個區域移除。

刪除 AWS 服務 作為源

選擇您的存取方法，然後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。移除來源時，Security Lake 會停止從指定區域和帳戶中的該來源收集資料，訂閱者也無法再使用來源的新資料。但是，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。若要取得有關移除自訂來源的資訊，請參閱從自訂來源收集資料。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
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一或多個區域。Security Lake 將停止從所選區域中的所有帳戶收集來自來源的資料。

API

若要以程式設計方式移除 AWS 服務 做為來源，請使用安全湖 API 的DeleteAwsLogSource作業。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，您可以將移除範圍限制為特定`accounts`或特定範圍`sourceVersion`。

> **Important**
>
> 當您未在命令中提供參數時，Security Lake 會假設遺失的參數是指整個集合。例如，如果您未提供`accounts`參數，則此命令會套用至組織中的整組帳戶。

下列範例會移除指定帳戶和區域中做為來源的 VPC 流程記錄。

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

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="1.0"
```

上述範例針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 行接續字元來提高可讀性。

取得來源集合的狀態

選擇您的存取方法，然後按照步驟取得目前區域中已啟用記錄收集的帳戶和來源的快照。

Console

若要取得目前區域中記錄收集的狀態

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 在功能窗格中，選擇 [帳戶]。
3. 將游標停留在「來源」欄中的數字上，即可查看已為選取的帳戶啟用哪些記錄。

API

若要取得目前區域中記錄檔收集的狀態，請使用安全湖 API 的GetDataLakeSources作業。如果您使用的是 AWS CLI，請執行get-data-lake-sources命令。對於accounts參數，您可以指定一個或多個 AWS 帳戶 ID 作為清單。如果您的要求成功，Security Lake 會傳回目前區域中這些帳戶的快照，包括 Security Lake 收集資料的 AWS 來源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已設定 Security Lake 之所有帳戶的記錄收集狀態。

例如，下列 AWS CLI 命令會擷取目前區域中指定帳戶的記錄收集狀態。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"
```

從自訂來源收集資料

Amazon 安全湖可以從第三方自訂來源收集日誌和事件。對於每個自訂來源，安全湖都會處理下列事項：

- 為 Amazon S3 儲存貯體中的來源提供唯一的前置詞。
- 在 AWS Identity and Access Management (IAM) 中建立角色，以允許自訂來源將資料寫入資料湖。此角色的權限界限是由名為的 AWS 受管理策略所設定AmazonSecurityLakePermissionsBoundary。
- 建立 AWS Lake Formation 表格以組織來源寫入安全湖的物件。
- 設定 AWS Glue 爬行者程式來分割來源資料。爬行者程式會 AWS Glue Data Catalog 以表格填入。它還會自動發現新的源數據並提取模式定義。

若要將自訂來源新增至安全湖泊，它必須符合下列需求：

1. 目標 — 自訂來源必須能夠將資料寫入 Security Lake，做為指派給來源的前置詞下方的一組 S3 物件。對於包含多種資料類別的來源，您應該將每個唯一的開放網路安全架構架構 (OCSF) 事件類別提供為單獨的來源。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。

   > **Note**
   >
   > 使用 OCSF 驗證工具來驗證自訂來源是否與OCSF Schema 1.1相容。

2. 格式 — 從自訂來源收集的每個 S3 物件都應該格式化為 Apache 實體檔案。
3. 結構描述 — 相同的 OCSF 事件類別應套用至 Parquet 格式化物件內的每個記錄。

擷取自訂來源的最佳做法

為了提高資料處理和查詢的效率，我們建議您在將自訂來源新增至 Security Lake 時遵循以下最佳做法：

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*bucket-name*/*source-location*/region=*region*/accountId=*accountID*/eventDay=*YYYYMMDD*。

範例分割區是aws-security-data-lake-*us-west-2-lake-uid*/*source-location*/region=*us-west-2*/accountId=*123456789012*/eventDay=*20230428*/。

- bucket-name— 安全湖存放您自訂來源資料的 Amazon S3 儲存貯體的名稱。

- `source-location`— S3 儲存貯體中自訂來源的前置詞。Security Lake 會將指定來源的所有 S3 物件存放在此前置詞下，且前置詞對於指定來源而言是唯一的。
- `region`— AWS 區域 將資料寫入的位置。
- `accountId`— AWS 帳戶 來源磁碟分割中的記錄與之相關的識別碼。
- `eventDay`— 事件發生的日期，格式為八個字元字串 (YYYYMMDD)。

物體大小和速率

寫入安全湖的物件應該緩衝記錄 5 分鐘。如果緩衝區期間包含太多資料而無法有效查詢，只要這些檔案的平均大小維持在 256 MB 以下，自訂來源就可以在 5 分鐘的視窗中寫入多筆記錄。輸送量低的自訂來源可以每 5 分鐘寫入較小的物件，以維持 5 分鐘的擷取延遲，並可長時間緩衝記錄。

鑲木地板

安全湖支持的版本 1.x 和 2. x 的鑲木地板。資料頁面大小應限制為 1 MB (未壓縮)。資料列群組大小不得超過 256 MB (壓縮)。對於在實木地板對象中進行壓縮，zstandard 是首選。

排序

在每個 Parquet 格式的對象中，記錄應按時間進行排序，以減少查詢數據的成本。

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，以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 AWS 區域 中`region`是您要新增自訂來源的格式。Security Lake 會將原則附加至允許存取資料湖的角色。如果您已使用客戶管理的 AWS KMS 金鑰加密資料湖，Security Lake 也會將原則與`kms:Decrypt`和`kms:GenerateDataKey`權限附加至該角色。此角色的權限界限是由名為的 AWS 受管理策略所設定`AmazonSecurityLakePermissionsBoundary`。

主題

- 驗證許可
- 建立 IAM 角色以允許寫入安全湖值區位置 (API 和 AWS CLI唯一步驟)

驗證許可

在新增自訂來源之前，請確認您具有執行下列動作的權限。

若要驗證您的許可，請使用 IAM 檢閱附加到 IAM 身分的 IAM 政策。然後，將這些策略中的資訊與下列新增自訂來源必須允許您執行的動作清單進行比較。

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

這些動作可讓您從自訂來源收集日誌和事件、將日誌和事件傳送到正確的 AWS Glue 資料庫和表格，然後將其存放在 Amazon S3 中。

如果您使用 AWS KMS 金鑰進行資料湖的伺服器端加密，您還需要kms:CreateGrantkms:DescribeKey、和的權限kms:GenerateDataKey。

> **Important**
>
> 如果您打算使用 Security Lake 主控台新增訂閱者，可以略過下一個步驟並繼續執行新增自訂來源。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 或 AWS CLI 新增訂閱者，請繼續下一步建立 IAM 角色，以允許對 Security Lake 值區位置的寫入存取權。

建立 IAM 角色以允許寫入安全湖值區位置 (API 和 AWS CLI唯一步驟)

如果您使用 Security Lake API 或 AWS CLI 新增自訂來源，請新增此 IAM 角色以授 AWS Glue 予檢索自訂來源資料和識別資料中分割區的權限。這些分割區是組織資料以及在「資料目錄」中建立和更新表格所必需的。

建立此 IAM 角色後，您需要角色的 Amazon 資源名稱 (ARN) 才能新增自訂來源。

您必須附加受arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole AWS 管理的策略。

若要授與必要的權限，您還必須在角色中建立並內嵌下列內嵌原則，以允許 AWS Glue 編目程式 從自訂來源讀取資料檔案，並在「資 AWS Glue 料目錄」中建立/更新表格。

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

附加以下信任策略以允許 AWS 帳戶 使用它，它可以根據外部 ID 承擔角色：

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

如果您要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，則您還必須將以下政策附加到該角色和 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}}"
    ]
}
```

新增自訂來源

建立 IAM 角色以呼叫 AWS Glue 爬行者程式之後，請依照下列步驟在 Security Lake 中新增自訂來源。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 使用頁面右上角的選取 AWS 區域 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「自訂來源詳細資料」區段中，輸入自訂來源的全域唯一名稱。然後，選取 OCSF 事件類別，該類別描述自訂來源將傳送至安全湖的資料類型。
5. 對於AWS 帳戶 具有寫入資料的權限，請輸入將記錄和事件寫入資料湖的自訂來源的 ID 和外部 ID。AWS 帳戶
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 呼叫權限 AWS Glue。
7. 選擇建立。

API

若要以程式設計方式新增自訂來源，請使用安全湖 API 的CreateCustomLogSource作業。使用您要在 AWS 區域 其中建立自訂來源的作業。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的值。
- `eventClasses`— 指定一或多個 OCSF 事件類別，以描述來源將傳送至安全湖的資料類型。如需安全性湖中作為來源支援的 OCSF 事件類別清單，請參閱開放網路安全結構描述架構 (OCSF)。
- `sourceVersion`— 選擇性地指定一個值，將記錄收集限制為特定版本的自訂來源資料。
- `crawlerConfiguration`— 指定您建立用來呼叫 AWS Glue 爬行者程式之 IAM 角色的 Amazon 資源名稱 (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`— 指定來源將用來將記錄檔和事件寫入資料湖的 AWS 身分識別和外部 ID。

下列範例會將自訂來源新增為指定區域中指定的記錄提供者帳戶中的記錄來源。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”]
```

保持自訂來源資料的更新 AWS Glue

在安全湖中新增自訂來源之後，安全湖會建立 AWS Glue 爬行者程式。爬行者程式會連線至您的自訂來源、決定資料結構，然後將 AWS Glue 資料目錄填入表格。

我們建議您手動執行爬蟲程式，讓您的自訂來源結構描述保持在最新狀態，並在 Athena 和其他查詢服務中維護查詢功能。具體而言，如果自訂來源的輸入資料集中發生下列任一變更，您應該執行爬行者程式：

- 資料集具有一或多個新的頂層欄。

- 資料集在具有資料`struct`類型的資料行中有一個或多個新欄位。

如需執行爬行者程式的指示，請參閱AWS Glue 開發人員指南中的排程 AWS Glue 爬蟲 (Crawler)。

安全湖無法刪除或更新您帳戶中現有的檢索器。如果您刪除自訂來源，建議您在 future 建立具有相同名稱的自訂來源時刪除關聯的爬行者程式。

刪除自訂來源

刪除自訂來源以停止將資料從來源傳送至安全湖。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您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，請使用安全湖 API 的DeleteCustomLogSource作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行delete-custom-log-source命令。使用您 AWS 區域 要刪除自訂來源的作業。

在您的請求中，使用`sourceName`參數來指定要刪除的自訂來源名稱。或者指定自訂來源的名稱，然後使用`sourceVersion`參數將刪除範圍限制為僅限自訂來源的特定資料版本。

下列範例會從安全性湖泊刪除自訂記錄來源。

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
```

Amazon 安全湖中的訂閱者管理

Amazon 安全湖訂閱者會從安全湖取用日誌和事件。為了控制成本並遵守最低權限存取最佳做法，您可以根據每個來源為訂閱者提供資料的存取權。如需來源的詳細資訊，請參閱 Amazon Security Lake ake ake ake ake ake ake ake 鍵。

安全湖支援兩種類型的使用者存取：

- 資料存取 — 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)，直接存取 S3 物件並接收新物件的通知。此訂閱類型會S3在 CreateSubscriberAPI 的accessTypes參數中識別為。
- 查詢存取 — 訂閱者使用 Amazon Athena 等服務，從 S3 儲存貯體中的資料 AWS Lake Formation 表查詢來源資料。此訂閱類型會LAKEFORMATION在 CreateSubscriberAPI 的accessTypes參數中識別為。

訂閱者只能存取您在建立訂戶時所 AWS 區域 選取的來源資料。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」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 區域。

> **Important**
>
> 安全性湖泊允許每位訂閱者新增的來源數目上限為 10。這可能是來 AWS 源和自訂來源的組合。

主題

管理安全湖訂戶的資料存取

在資料寫入 S3 儲存貯體時，可以存取 Amazon Security Lake 中來源資料的訂閱者會收到來源新物件的通知。依預設，訂閱者會透過其提供的 HTTPS 端點通知有關新物件的相關資訊。或者，您也可以輪詢 Amazon Simple Queue Service (Amazon SQS)，向訂閱者收到有關新物件的通知。

建立具有資料存取權之訂戶的先決條件

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。

主題

驗證許可

若要驗證您的許可，請使用 IAM 檢閱附加到 IAM 身分的 IAM 政策。然後，將這些策略中的資訊與下列 (權限) 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。

您需要執行下列動作的權限：

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

除了上述清單之外，您還需要執行下列動作的權限：

- `events:CreateApiDestination`
- `events:CreateConnection`
- `events:DescribeRule`
- `events:ListApiDestinations`

- events:ListConnections
- events:PutRule
- events:PutTargets
- s3:GetBucketNotification
- s3:PutBucketNotification
- sqs:CreateQueue
- sqs:DeleteQueue
- sqs:GetQueueAttributes
- sqs:GetQueueUrl
- sqs:SetQueueAttributes

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，您還需要取得其外部 ID。外部 ID 是訂閱者提供給您的唯一識別碼。安全湖會將外部 ID 新增至其建立的訂閱者 IAM 角色。當您透過 API 或在 Security Lake 主控台中建立訂閱者時，可以使用外部識別碼 AWS CLI。

如需有關外部 ID 的詳細資訊，請參閱 IAM 使用者指南中的如何在將資 AWS 源存取權授予第三方時使用外部 ID。

> **Important**
>
> 如果您打算使用 Security Lake 主控台新增訂閱者，可以略過下一個步驟並繼續執行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。
>
> 如果您打算使用安全湖 API 或 AWS CLI 新增訂閱者，請繼續執行下一個步驟以建立 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 和 AWS CLI唯一步驟)

如果您是透過 API 使用安全湖 AWS CLI，或者在 AWS Identity and Access Management (IAM) 中建立角色，以授予 Amazon EventBridge 許可以叫用 API 目的地，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 資源名稱 (ARN) 才能建立訂閱者。如果訂閱者輪詢來自 Amazon Simple Queue Service (Amazon SQS) 的資料，或直接從中查詢資料，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，請參閱管理安全湖訂戶的查詢存取。

將下列政策附加到您的 IAM 角色：

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

將以下信任政策附加到您的 IAM 角色，以 EventBridge 允許擔任該角色：

```
{
    "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 (或輪詢 Amazon SQS 佇列中的事件，如果這是慣用的通知方法)。此角色受到名為的受 AWS 管理策略保護AmazonSecurityLakePermissionsBoundary。

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，建立可存取目前資料的訂戶 AWS 區域。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要建立訂閱者的「地區」。
3. 在導覽窗格中，選擇 [訂閱者]。
4. 在「訂戶」頁面上，選擇「建立訂戶」。
5. 如需訂戶詳細資訊，請輸入訂戶名稱和選擇性說明。

   「地區」會自動填入您目前選取的項目， AWS 區域 且無法修改。
6. 對於記錄檔和事件來源，請選擇授權訂戶使用的來源。
7. 對於資料存取方法，請選擇 S3 設定訂閱者的資料存取。
8. 若為訂閱者認證，請提供訂閱者的 AWS 帳戶 ID 和外部識別碼。
9. (選擇性) 對於通知詳細資訊，如果您希望 Security Lake 建立訂閱者可輪詢物件通知的 Amazon SQS 佇列，請選取 SQS 佇列。如果您希望安全湖透過 EventBridge HTTPS 端點傳送通知，請選取訂閱端點。

   如果您選取訂閱端點，請同時執行下列動作：

   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. 對於服務存取，請建立新的 IAM 角色或使用現有的 IAM 角色，以 EventBridge授予呼叫 API 目標的權限，並將物件通知傳送至正確的端點。

      如需建立新 IAM 角色的相關資訊，請參閱建立 IAM 角色以叫用 EventBridge API 目的地。
10. (選擇性) 在標籤中，輸入最多 50 個要指派給訂閱者的標籤。

標籤是您可以定義並指派給特定 AWS 資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。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 Amazon 安全湖資源。

11. 選擇建立。

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作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行建立訂閱者命令。

在您的要求中，使用這些參數來指定訂戶的下列設定值：

- 對於sources，指定您希望訂戶存取的每個來源。
- 對於subscriberIdentity，指定訂閱者將用來存取來源資料的 AWS 帳戶 ID 和外部 ID。
- 對於subscriber-name，指定訂戶的名稱。
- 對於 accessTypes，請指定 S3。

範例 1

下列範例會針對 AWS 來源的指定訂閱者身分，建立可存取目前 AWS 區域中資料的訂閱者。

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

範例 2

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

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

```
--access-types S3
```

上述範例針對 Linux、macOS 或 Unix 進行格式化，並使用反斜線 (\) 行接續字元來提高可讀性。

(選擇性) 建立訂戶之後，請使用此CreateSubscriberNotification作業來指定將新資料寫入資料湖以供訂戶存取之來源的資料湖時，如何通知訂戶。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 端點進行通知，請指定`httpsNotificationConfiguration`參數值。
- 在`targetRoleArn`欄位中，指定您建立用來叫用 EventBridge API 目標的 IAM 角色的 ARN。

```
$ aws securitylake create-subscriber-notification \
--subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \
--configuration
 httpsNotificationConfiguration={"targetRoleArn"="arn:aws:iam::XXX:role/service-role/RoleName", "endpoint"="https://account-management.$3.$2.securitylake.aws.dev/v1/datalake"}
```

若要取得`subscriberID`，請使用安全湖 API 的ListSubscribers作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請運行列表訂閱者命令。

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

若要隨後變更訂閱者的通知方法 (Amazon SQS 佇列或 HTTPS 端點)，請使用UpdateSubscriberNotification作業，或者，如果您使用的是 AWS CLI，請執行命update-subscriber-notification令。您也可以使用 Security Lake 主控台變更通知方法：在「訂戶」頁面上選取訂戶，然後選擇「編輯」。

範例物件通知訊息

```
{
  "source": "aws.s3",
```

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

更新資料訂閱者

您可以變更訂戶使用的來源，以更新訂戶。您也可以指派或編輯訂閱者的標籤。標籤是一個標籤，您可以定義並指派給特定類型的 AWS 資源，包括訂閱者。如需進一步了解，請參閱 標記 Amazon 安全湖資源。

選擇其中一種存取方法，然後依照下列步驟為現有訂閱定義新來源。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 在導覽窗格中，選擇 [訂閱者]。
3. 選取訂戶。
4. 選擇 「編輯」，然後執行下列任一項作業：
   - 若要更新訂戶的來源，請在「記錄檔和事件來源」區段中輸入新的設定值。
   - 若要指派或編輯訂閱者的標記，請視需要在「標記」區段中變更標記。
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作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行更新訂閱者命令。在您的要求中，使用sources參數來指定您要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作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請運行列表訂閱者命令。

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

若要檢閱特定訂戶的目前設定值，請使用GetSubscriber作業。執行 ge t-user 命令。然後，Security Lake 會傳回訂閱者的名稱和說明、外部識別碼以及其他資訊。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行取得訂閱者命令。

若要更新訂閱者的通知方法，請使用此UpdateSubscriberNotification作業。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。

移除資料訂閱者

如果您不想讓訂閱者使用 Security Lake 的資料，您可以依照下列步驟移除訂閱者。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
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。這樣會刪除訂閱者和所有相關的通知設定。

API

根據您的案例，執行下列其中一個動作：

- 若要刪除訂閱者和所有相關聯的通知設定，請使用安全湖 API 的DeleteSubscriber作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行刪除訂閱者命令。

- 若要保留訂閱者，但停止 future 傳送給訂閱者的通知，請使用 Security Lake API 的DeleteSubscriberNotification作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請運行該delete-subscriber-notification命令。

管理安全湖訂戶的查詢存取

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。雖然安全湖的主要查詢引擎是 Athena，您也可以使用其他服務，如 Amazon Redshift Spectrum 和星火 SQL，與. AWS Glue Data Catalog

> **Note**
>
> 本節說明如何將查詢存取權授與協力廠商訂閱者。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。

建立具有查詢存取權之訂戶的先決條件

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。

主題

- 驗證許可
- 建立 IAM 角色以查詢安全湖資料 (API 和 AWS CLI唯一步驟)
- 授予 Lake Formation 管理員權限

驗證許可

在建立具有查詢存取權的訂閱者之前，請確認您有執行下列動作清單的權限。

若要驗證您的許可，請使用 IAM 檢閱附加到 IAM 身分的 IAM 政策。然後，將這些原則中的資訊與下列您必須被允許執行的動作清單做比較，才能建立具有查詢存取權的訂戶。

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

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

> **Important**
>
> 驗證權限之後：
>
> - 如果您打算使用 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執行授予 Lake Formation 管理員權限。安全湖建立所有必要的 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 新增具有查詢存取權的訂閱者，請繼續執行下一個步驟，以建立 IAM 角色以查詢安全湖資料。

建立 IAM 角色以查詢安全湖資料 (API 和 AWS CLI唯一步驟)

使用 Security Lake API 或 AWS CLI 將查詢存取權授與訂閱者時，您必須建立名為的角色AmazonSecurityLakeMetaStoreManager。安全性湖泊使用此角色來註冊 AWS Glue 磁碟分割和更新 AWS Glue 資料表。您可能已經在創建必要的 IAM 角色時創建了此角色。

授予 Lake Formation 管理員權限

您還需要將 Lake Formation 管理員許可添加到用於存取安全湖主控台和新增訂閱者的 IAM 角色。

您可以按照以下步驟將 Lake Formation 管理員權限授予您的角色：

1. 開啟 Lake Formation 主控台，網址為 https://console.aws.amazon.com/lakeformation/。
2. 以系統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，請執行以下步驟來配置 Lake Formation 管理員。

   1. 在功能窗格的 [權限] 下，選擇 [系統管理角色和工作]。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，對於 IAM 使用者和角色，請選擇存取 Security Lake 主控台時使用的管理員角色，然後選擇 [儲存]。

如需有關變更資料湖管理員權限的詳細資訊，請參閱AWS Lake Formation 開發人員指南中的建立資料湖管理員。

IAM 角色必須擁有您要授與訂閱者存取SELECT權的資料庫和資料表的權限。有關如何執行此操作的指示，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權限。

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。訂閱者只能查詢建立資料的資料。 AWS 區域 若要建立訂閱者，您必須擁有訂閱者的 AWS 帳戶 ID 和外部 ID。外部 ID 是訂閱者提供給您的唯一識別碼。如需有關外部 ID 的詳細資訊，請參閱 IAM 使用者指南中的如何在將資 AWS 源存取權授予第三方時使用外部 ID。

> **Note**
>
> 安全湖不支持 Lake Formation 跨帳戶數據共享版本 1。您必須將 Lake Formation 跨帳戶資料共用更新至第 2 版或第 3 版。如需透過 AWS Lake Formation 主控台或 AWS CLI 更新跨帳戶版本設定的步驟，請參閱開AWS Lake Formation 發人員指南中的若要啟用新版本。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   登入委派的系統管理員帳戶。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要建立訂閱者的「地區」。
3. 在導覽窗格中，選擇 [訂閱者]。
4. 在「訂戶」頁面上，選擇「建立訂戶」。
5. 如需訂戶詳細資訊，請輸入訂戶名稱和選擇性說明。

「地區」會自動填入您目前選取的項目， AWS 區域 且無法修改。

6. 對於記錄檔和事件來源，請選擇傳回查詢結果時希望 Security Lake 包含的來源。
7. 對於資料存取方法，請選擇 Lake Formation 以建立訂閱者的查詢存取權。
8. 若為訂閱者認證，請提供訂閱者的 AWS 帳戶 ID 和外部識別碼。
9. (選擇性) 在標籤中，輸入最多 50 個要指派給訂閱者的標籤。

   標籤是您可以定義並指派給特定 AWS 資源類型的標籤。每個標籤都包含必要的標籤鍵和一個可選的標籤值。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 Amazon 安全湖資源。
10. 選擇建立。

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作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行建立訂閱者命令。

在您的要求中，使用這些參數來指定訂戶的下列設定值：

- 對於 `accessTypes`，請指定 `LAKEFORMATION`。
- 對於`sources`，指定您希望 Security Lake 在傳回查詢結果時包含的每個來源。
- 對於`subscriberIdentity`，指定訂戶用來查詢來源資料的 AWS 識別碼和外部識別碼。

下列範例會針對指定的訂閱者身分，在目前 AWS 區域中建立具有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: 1.0}}] \
--subscriber-name subscriber name \
--access-types LAKEFORMATION
```

設定跨帳戶資料表共用 (訂閱者步驟)

安全湖使用 Lake Formation 跨帳戶表共享來支持用戶查詢訪問。當您在 Security Lake 主控台、API 或中建立具有查詢存取權的訂閱者時 AWS CLI，Security Lake 會在 AWS Resource Access Manager (AWS RAM) 中建立資源共用，與訂閱者共用相關 Lake Formation 表格的相關資訊。

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 會建立新的資源共用。如需詳細資訊，請參閱 編輯具有查詢存取權的訂閱者。

訂閱者應按照以下步驟使用 Lake Formation 表中的數據：

1. 接受資源共用 — 訂閱者必須接受包含在您建立或編輯訂閱者時所產生`resourceShareArn`和`resourceShareName`的資源共用。選擇下列其中一種存取方法：
   - 對於主控台和 AWS CLI，請參閱接受來自的資源共用邀請 AWS RAM。
   - 對於 API，請調用該 GetResourceShareInvitationsAPI。篩選`resourceShareArn`並找`resourceShareName`到正確的資源共用。使用 AcceptResourceShareInvitationAPI 接受邀請。

   資源共用邀請將在 12 小時後到期，因此您必須在 12 小時內驗證並接受邀請。如果邀請過期，您會繼續看到它處於某個`PENDING`狀態，但接受邀請不會讓您存取共用資源。當超過 12 小時後，刪除 Lake Formation 用戶並重新創建訂閱者以獲得新的資源共享邀請。
2. 建立共用資料表的資源連結 — 訂閱者必須在 (如果使用主控台) 或 AWS Lake Formation AWS Glue (如果使用 API/AWS CLI) 中建立連結至共用 Lake Formation 表格的資源連結。此資源連結會將訂閱者的帳號指向共用資料表。選擇下列其中一種存取方法：
   - 對於控制台和 AWS CLI，請參閱AWS Lake Formation 開發人員指南中的建立共用資料目錄表格的資源連結。
   - 對於 API，請調用該 AWS Glue CreateTableAPI。我們建議訂閱者還使用 CreateDatabaseAPI 創建一個唯一的數據庫來存儲資源鏈接表。
3. 查詢共用資料表 — Amazon Athena 等服務可以直接參考資料表，而 Security Lake 收集的新資料也會自動提供查詢。查詢會以訂閱者的方式執行 AWS 帳戶，而查詢產生的費用則會向訂閱者收取費用。您可以在自己的安全湖帳戶中控制資源的讀取存取權限。

如需有關授予跨帳戶權限的詳細資訊，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。

編輯具有查詢存取權的訂閱者

安全湖支援對具有查詢存取權的訂閱者進行編輯。您可以編輯訂戶的名稱、說明、外部識別碼、主體 (AWS 帳戶 ID)，以及訂戶能夠使用的記錄來源。選擇您偏好的方式，並依照步驟編輯目前具有查詢存取權的訂閱者 AWS 區域。

> **Note**
>
> 安全湖不支持 Lake Formation 跨帳戶數據共享版本 1。您必須將 Lake Formation 跨帳戶資料共用更新至第 2 版或第 3 版。如需透過 AWS Lake Formation 主控台或 AWS CLI 更新跨帳戶版本設定的步驟，請參閱開AWS Lake Formation 發人員指南中的若要啟用新版本。

Console

根據您要編輯的詳細資訊，請僅遵循針對該動作提供的步驟。

若要編輯訂戶名稱

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   登入委派的系統管理員帳戶。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要編輯訂閱者詳細資料的地區。
3. 在導覽窗格中，選擇 [訂閱者]。
4. 在「訂戶」頁面上，使用圓鈕來選擇您要編輯的訂戶。所選用戶的數據訪問方法必須是 LAKEFORMAT ION。
5. 選擇編輯。
6. 輸入新的「訂戶」名稱，然後選擇「儲存」。

若要編輯訂戶說明

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   登入委派的系統管理員帳戶。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要編輯訂閱者的地區。
3. 在導覽窗格中，選擇 [訂閱者]。

4. 在「訂戶」頁面上，使用圓鈕來選擇您要編輯的訂戶。所選用戶的數據訪問方法必須是 LAKEFORMAT ION。
5. 選擇編輯。
6. 輸入訂戶的新說明，然後選擇「儲存」。

若要編輯外部 ID

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   登入委派的系統管理員帳戶。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要編輯訂閱者詳細資料的地區。
3. 在導覽窗格中，選擇 [訂閱者]。
4. 在「訂戶」頁面上，使用圓鈕來選擇您要編輯的訂戶。所選用戶的數據訪問方法必須是 LAKEFORMAT ION。
5. 選擇編輯。
6. 輸入訂戶提供的新外部 ID，然後選擇「儲存」。

   儲存新的外部 ID 會自動移除先前的 AWS RAM 資源共用，並為訂閱者建立新的資源共用。
7. 訂閱者必須按照中的步驟 1 接受新的資源共用設定跨帳戶資料表共用 (訂閱者步驟)。確保出現在訂戶詳細信息中的 Amazon 資源名稱（ARN）與 Lake Formation 控制台中的相同。共用資料表的資源連結會保持原樣，因此訂閱者不需要建立新的資源連結。

若要編輯主參與者 (AWS 帳戶 ID)

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   登入委派的系統管理員帳戶。
2. 使用頁面右上角的選取 AWS 區域 器，選取您要編輯訂閱者詳細資料的地區。
3. 在導覽窗格中，選擇 [訂閱者]。
4. 在「訂戶」頁面上，使用圓鈕來選擇您要編輯的訂戶。所選用戶的數據訪問方法必須是 LAKEFORMAT ION。
5. 選擇編輯。
6. 輸入訂戶的新 AWS 帳戶 ID，然後選擇「儲存」。

儲存新帳號 ID 會自動移除先前的 AWS RAM 資源共用，因此先前的主參與者無法使用記錄檔和事件來源。安全湖創建一個新的資源共享。

7. 訂戶必須使用新主參與者的證明資料，接受新的資源共用，並建立共用表格的資源連結。這可讓新的主體存取共用資源。如需指示，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)。確保出現在用戶詳細信息中的 ARN 與 Lake Formation 控制台中的相同。

若要編輯記錄檔和事件來源

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

   登入委派的系統管理員帳戶。

2. 使用頁面右上角的選取 AWS 區域 器，選取您要編輯訂閱者詳細資料的地區。
3. 在導覽窗格中，選擇 [訂閱者]。
4. 在「訂戶」頁面上，使用圓鈕來選擇您要編輯的訂戶。所選用戶的數據訪問方法必須是 LAKEFORMAT ION。
5. 選擇編輯。
6. 取消選取現有來源，或選取您要新增的來源。如果您取消選取來源，則不需要進一步採取任何動作。如果您選取新增來源，則不會建立新的資源共用邀請。但是，安全湖根據添加的來源更新共享的 Lake Formation 表。訂閱者必須建立連至更新之共用資料表的資源連結，才能查詢來源資料。如需指示，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作業。如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行更新訂閱者命令。在您的要求中，使用支援的參數來指定訂戶的下列設定值：

- 對於`subscriberName`，指定新的訂戶名稱。
- 對於`subscriberDescription`，指定新描述。
- 在中`subscriberIdentity`，指定訂戶將用來查詢來源資料的主體 (AWS 帳戶 ID) 和外部識別碼。您必須同時提供主體識別碼和外部識別碼。如果您想要保持其中一個值相同，請傳入目前的值。

- 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。訂閱者必須按照中的步驟 1 接受新的資源共用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會保持原樣，因此訂閱者不需要建立新的資源連結。
- 僅更新主參與者 — 此動作會移除先前的 AWS RAM 資源共用，因此先前的主參與者無法使用記錄檔和事件來源。安全湖創建一個新的資源共享。訂戶必須使用新主參與者的證明資料，接受新的資源共用，並建立共用表格的資源連結。這可讓新的主體存取共用資源。如需指示，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 和主參與者，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)。

- 對於`sources`，移除現有來源或指定要新增的來源。如果您移除來源，則不需要進一步採取任何動作。如果您新增來源，則不會建立新的資源共用邀請。但是，安全湖根據添加的來源更新共享的 Lake Formation 表。訂閱者必須建立連至更新之共用資料表的資源連結，才能查詢來源資料。如需指示，請參閱中的步驟 2 設定跨帳戶資料表共用 (訂閱者步驟)。

安全湖查詢

您可以查詢安全湖泊儲存在資料 AWS Lake Formation 庫和資料表中的資料。您也可以在安全湖主控台、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表格的SELECT許可授與查詢資料的 IAM 身分。訂閱者也必須先在安全湖中建立，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，請參閱管理安全湖訂戶的查詢存取。

主題

- AWS 來源版本 1 (OCSF 1.0.0-rc.2) 的安全性湖泊查詢
- AWS 來源版本 2 的安全性湖泊查詢 (OCSF 1.1.0)

AWS 來源版本 1 (OCSF 1.0.0-rc.2) 的安全性湖泊查詢

下節提供從 Security Lake 查詢資料的指引，並包含一些原生支援來源的查詢範例。 AWS 這些查詢旨在檢索特定的數據 AWS 區域。這些範例使用 us-east-1 (美國東部 (維吉尼亞北部))。此外，範例查詢會使用LIMIT 25參數，該參數最多可傳回 25 筆記錄。您可以省略此參數，也可以根據自己的偏好進行調整。如需更多範例，請參閱 Amazon 安全湖 OCSF 查詢 GitHub 目錄。

記錄來源表格

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

```
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
```

記錄來源資料表的一般值包括下列項目：

- `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 路線 53 解析器查詢日誌
- `sh_findings_1_0`— AWS Security Hub 發現
- `vpc_flow_1_0`— Amazon Virtual Private Cloud（Amazon VPC）流程日誌

範例：us-east-1 區域中資料表**`sh_findings_1_0`**中的所有 Security Hub 發現項目

```
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

當您查詢 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。如需目前提供安全湖泊的完整資料庫區域清單，請參閱 Amazon 安全湖端點。

範例：列出來自來源 IP 的 AWS CloudTrail 活動

######### 20230301 (20 23 # 3 # 1 #) ######## IP 192.0.2.1 ### CloudTrail # ########## us-east-1 # Cloud_trail_mgmt_0# 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
```

分割日期

透過分割資料，您可以限制每個查詢掃描的資料量，進而改善效能並降低成本。安全湖實作透過eventDayregion、和accountid參數進行分割。 eventDay分區使用格式YYYYMMDD。

這是使用eventDay分區的示例查詢：

```
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
```

的一般值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)
```

最近 1 個月發生的事件

```
> 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)
```

最近 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：表格中 2023 年 3 月 1 **192.0.2.1** 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
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

範例：表格中過去 30 天來源 IP **192.0.2.1** 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
    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 資料查詢範例

AWS CloudTrail 追蹤中的使用者活動和 API 使用情況 AWS 服務。訂閱者可以查詢資 CloudTrail 料以瞭解下列類型的資訊：

以下是 CloudTrail 數據的一些示例查詢：

過去 7 天內未經授權的嘗試 AWS 服務

```
SELECT
      time,
      api.service.name,
      api.operation,
      api.response.error,
      api.response.message,
      unmapped['responseElements'],
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND api.response.error in (
        'Client.UnauthorizedOperation',
        'Client.InvalidPermission.NotFound',
        'Client.OperationNotPermitted',
        'AccessDenied')
    ORDER BY time desc
    LIMIT 25
```

過去 7 天來源 IP **192.0.2.1** 的所有 CloudTrail 活動清單

```
SELECT
      api.request.uid,
      time,
      api.service.name,
      api.operation,
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '127.0.0.1.'
```

```
    ORDER BY time desc
    LIMIT 25
```

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 天內使用認證**AIDACKCEVSQ6C2EXAMPLE**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 解析器查詢記錄檔的範例查詢

Amazon 路線 53 解析器查詢日誌跟踪您的 Amazon VPC 中的資源進行的 DNS 查詢。訂閱者可以查詢 Route 53 解析器查詢日誌，以了解以下類型的信息：

以下是 Route 53 解析器查詢日誌的一些示例查詢：

過去 7 天內的 DNS 查詢清單 CloudTrail

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

過去 7 天內相符**s3.amazonaws.com**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 天未解決的 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**192.0.2.1**的 DNS 查詢清單

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answer.rdata
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    CROSS JOIN UNNEST(answers) as st(answer)
    WHERE answer.rdata='192.0.2.1' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Security Hub 發現項目的範例查詢

Security Hub 為您提供中安全性狀態的全面檢視， AWS 並協助您根據安全性產業標準和最佳做法來檢查環境。Security Hub 會產生安全性檢查結果，並從協力廠商服務接收發現項目。

以下是 Security Hub 發現的一些示例查詢：

過去 7 天內嚴重性大於或等**MEDIUM**於的新發現項目

```
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 天內重複的發現項目

```
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 天內所有非資訊性發現

```
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
```

資源為 Amazon S3 儲存貯體的發現項目 (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 = 'AwsS3Bucket')
   LIMIT 25
```

常見弱點評分系統 (CVSS) 分數大於 **1** (無時間限制) 的發現項目

```
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
```

符合常見弱點和入侵程式 (CVE) 的發現項目 **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 天從 Security Hub 傳送發現項目的產品計數

```
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 天內發現項目中的資源類型計數

```
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
```

過去 7 天內發現的易受攻擊的套件

```
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
```

過去 7 天內已變更的發現項目

```
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 流程日誌的查詢範例

Amazon Virtual Private Cloud (Amazon VPC) 提供有關進出虛擬私人雲端網路界面的 IP 流量的詳細資 VPC。

以下是 Amazon VPC 流程日誌的一些查詢範例：

最近 7 天 AWS 區域 的特定流量

```
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
```

過去 7 天來自來源 IP `192.0.2.1` 和來源通訊埠22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 位址的計數

```
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
```

過去七天內自 198.51.100.0/24 之間的流量

```
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
```

過去 7 天**443**內目的地連線的封包數量排序

```
SELECT
      traffic.packets,
      dst_endpoint.ip
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      traffic.packets,
      dst_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

IP **192.0.2.1** 與過去 7 天之**192.0.2.2**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 天內的所有入站流量

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'ingress'
    LIMIT 25
```

過去 7 天內的所有輸出流量

```
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 的安全性湖泊查詢 (OCSF 1.1.0)

您可以查詢安全湖泊儲存在資料 AWS Lake Formation 庫和資料表中的資料。您也可以在安全湖主控台、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表格的SELECT許可授與查詢資料的 IAM 身分。訂閱者也必須先在安全湖中建立，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，請參閱管理安全湖訂戶的查詢存取。

下節提供從 Security Lake 查詢資料的指引，並包含一些原生支援來源的查詢範例。 AWS 這些查詢被設計為在一個特定的數據檢索 AWS 區域。這些範例使用 us-east-1 (美國東部 (維吉尼亞北部))。此

外，範例查詢會使用LIMIT 25參數，該參數最多可傳回 25 筆記錄。您可以省略此參數，也可以根據自己的偏好進行調整。如需更多範例，請參閱 Amazon 安全湖 OCSF 查詢 GitHub 目錄。

記錄來源表格

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

```
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
```

記錄來源資料表的一般值包括下列項目：

- `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 路線 53 解析器查詢日誌
- `sh_findings_2_0`— AWS Security Hub 調查結果
- `vpc_flow_2_0`— Amazon Virtual Private Cloud（Amazon VPC）流程日誌
- `eks_audit_2_0`— Amazon Elastic Kubernetes Service (Amazon EKS) 審核日誌

範例：us-east-1 區域中資料表**`sh_findings_2_0`**中的所有 Security Hub 發現項目

```
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

當您查詢 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。如需目前提供安全湖泊的完整資料庫區域清單，請參閱 Amazon 安全湖端點。

範例：列出來自來源 IP 的 Amazon Virtual Private Cloud 活動

```
######### 20230301 (2023 # 3 # 1 #) ####### IP 192.0.2.1 ### Amazon #######
######## us-west-2 # vpc_flow_2 _0# 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，進而改善效能並降低成本。與安全湖 1.0 相比，安全湖 2.0 中的分區工作方式略有不同。安全湖現在實作透過time_dtregion、和分割accountid。然而，安全湖 1.0 實現了通過 eventDayregion，和accountid參數進行分區。

查詢time_dt將自動從 S3 產生日期分區，並且可以像在 Athena 中任何基於時間的欄位一樣進行查詢。

以下是使用 time_dt分割區在 2023 年 3 月 1 日之後查詢記錄檔的範例查詢：

```
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
```

的一般值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
```

最近 1 個月發生的事件

```
  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
```

最近 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：表格中 2023 年 3 月 1 **192.0.2.1** 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
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

範例：表格中過去 30 天來源 IP **192.0.2.1** 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
    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
```

查詢安全湖觀察

可觀測值是安全湖 2.0 現在可用的新功能。可觀察到的對象是一個樞紐分析元素，其中包含在事件中的許多地方發現的相關信息。查詢可觀測項允許使用者從他們的資料集衍生出高層級的安全見解。

通過查詢可觀察值中的特定元素，您可以將數據集限制為諸如特定用戶名，資源 UID，IP，哈希和其他 IOC 類型信息之類的東西

這是一個範例查詢，使用可觀測值陣列查詢 VPC 流程和 Route53 資料表 (包含 IP 值 '172.01.02.03') 之間的記錄

```
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 資料查詢範例

AWS CloudTrail 追蹤中的使用者活動和 API 使用情況 AWS 服務。訂閱者可以查詢資 CloudTrail 料以瞭解下列類型的資訊：

以下是 CloudTrail 數據的一些示例查詢：

過去 7 天內未經授權的嘗試 AWS 服務

```
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
```

過去 7 天來源 IP **192.0.2.1** 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 天內使用認證**AIDACKCEVSQ6C2EXAMPLE**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 解析器查詢記錄檔的範例查詢

Amazon 路線 53 解析器查詢日誌跟踪您的 Amazon VPC 中的資源進行的 DNS 查詢。訂閱者可以查詢 Route 53 解析器查詢日誌，以了解以下類型的信息：

過去 7 天內的 DNS 查詢清單 CloudTrail

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
```

```
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

過去 7 天內相符**s3.amazonaws.com**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 天未解決的 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**192.0.2.1**的 DNS 查詢清單

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answer.rdata
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
UNNEST(answers) as st(answer)
WHERE answer.rdata='192.0.2.1'
AND time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Security Hub 發現項目的範例查詢

Security Hub 為您提供中安全性狀態的全面檢視， AWS 並協助您根據安全性產業標準和最佳做法來檢查環境。Security Hub 會產生安全性檢查結果，並從協力廠商服務接收發現項目。

以下是 Security Hub 發現的一些示例查詢：

過去 7 天內嚴重性大於或等**MEDIUM**於的新發現項目

```
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 天內重複的發現項目

```
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發現

```
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
```

資源為 Amazon S3 儲存貯體的發現項目 (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 = 'AwsS3Bucket')
LIMIT 25
```

常見弱點評分系統 (CVSS) 分數大於 **1** (無時間限制) 的發現項目

```
SELECT
    DISTINCT finding_info.uid
    time_dt,
    metadata,
    finding_info,
    vulnerabilities,
    resource
```

```
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
UNNEST(vulnerabilities) AS t(vulnerability),
UNNEST(vulnerability.cve.cvss) AS t(cvs)
WHERE cvs.base_score > 1.0
AND vulnerabilities is NOT NULL
LIMIT 25
```

符合常見弱點和入侵程式 (CVE) 的發現項目 **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 傳送發現項目的產品計數

```
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 天內發現項目中的資源類型計數

```
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
```

過去 7 天內發現的易受攻擊的套件

```
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
```

過去 7 天內已變更的發現項目

```
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 流程日誌查詢範例

Amazon Virtual Private Cloud (Amazon VPC) 提供有關進出虛擬私人雲端網路界面的 IP 流量的詳細資 VPC。

以下是 Amazon VPC 流程日誌的一些查詢範例：

最近 7 天 AWS 區域 的特定流量

```
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
```

過去 7 天來自來源 IP **192.0.2.1** 和來源通訊埠**22**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 位址的計數

```
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
```

過去七天內自 198.51.100.0/24 之間的流量

```
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
```

過去 7 天**443**內目的地連線的封包數量排序

```
SELECT
    traffic.packets,
    dst_endpoint.ip
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    traffic.packets,
    dst_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

IP **192.0.2.1** 與過去 7 天之**192.0.2.2**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 天內的所有入站流量

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Inbound'
LIMIT 25
```

過去 7 天內的所有輸出流量

```
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 的示例查詢

Amazon EKS 日誌追蹤控制平面活動可將稽核和診斷日誌直接從 Amazon EKS 控制平面提供到您帳戶中的 CloudWatch 日誌。這些記錄可讓您輕鬆保護和執行叢集。訂閱者可以查詢 EKS 記錄以了解下列類型的資訊：

以下是 EKS 日誌的一些示例查詢：

過去 7 天內對特定 URL 的要求

```
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
```

在過去 7 天內，來自「10.0.97.167」的更新要求

```
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' 相關聯的要求和回應

```
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
```

安全湖中的生命週期管理

您可以自訂 Security Lake，在您偏好 AWS 區域 的時間內儲存資料。生命週期管理可協助您遵循不同的法規遵循要求。

保留管理

若要管理資料以符合成本效益的方式儲存資料，您可以設定資料的保留設定。由於安全湖將您的資料作為物件存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中，因此保留設定對應於 Amazon S3 生命週期組態。透過設定這些設定，您可以指定偏好的 Amazon S3 儲存類別，以及 S3 物件在轉換到其他儲存類別或到期之前停留在該儲存類別中的時間段。如需 Amazon S3 生命週期組態的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的管理儲存生命週期。

在 [安全性湖泊] 中，您可以在 [區域] 層級指定保留設定。例如，您可以選擇在寫入資料湖 30 天後，AWS 區域 將特定於 S3 標準 — IA 儲存類別的所有 S3 物件轉移。預設的 Amazon S3 儲存類別為 S3 標準。

> **Important**
>
> 安全湖不支援 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。啟用具有預設保留模式的 S3 物件鎖定會中斷標準化日誌資料傳遞至資料湖。

在啟用安全性湖泊時設定保留設定

在您上線至 Security Lake 時，請依照下列指示設定一或多個區域的保留設定。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，並使用 S3 標準儲存類別無限期地存放資料。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 當您達到步驟 2: 定義上線工作流程的目標時，請選擇 [選取儲存類別] 下的 [新增轉換]。然後選擇您要將 S3 物件轉移到的 Amazon S3 儲存類別。(未列出的預設儲存類別為 S3 標準。) 同時指定該儲存空間類別的保留期間 (以天為單位)。若要在該時間之後將物件轉移到另一個儲存類別，請選擇 [新增轉移]，然後輸入後續儲存類別和保留期間的設定。

3. 若要指定 S3 物件到期的時間，請選擇新增轉移。然後，對於存儲類別，選擇過期。對於保留期，請在建立物件後，使用任何儲存類別，輸入您要在 Amazon S3 中存放物件的總天數。此時間週期結束時，物件會過期，Amazon S3 會刪除物件。
4. 完成後，請選擇下一步。

您的變更將套用至您在之前的上線步驟中啟用 Security Lake 的所有區域。

API

若要在上線安全湖時以程式設計方式設定保留設定，請使用安全湖 API 的CreateDataLake作業。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`，指定要在特定 Amazon S3 儲存類別中存放 S3 物件的總天數 (`storageClass`)。`days`
- 對於`expiration`，指定建立物件後，使用任何儲存類別在 Amazon S3 中存放物件的總天數。此時間週期結束時，物件會過期，Amazon S3 會刪除物件。

「安全湖」會將設定套用至您在`configurations`物件`region`欄位中指定的「區域」。

例如，下列命令會啟用「`us-east-1`區域」中的「安全湖」。在此區域中，物件會在 365 天後過期，物件會在 60 天後轉換至 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 之後，請依照下列指示更新一或多個區域的保留設定。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。

2. 在功能窗格中，選擇 [區域]
3. 選取「區域」，然後選擇「編輯」。
4. 在 [選取儲存空間類別] 區段中，輸入您想要的設定。對於儲存類別，請選擇您要將 S3 物件轉移到的 Amazon S3 儲存類別。(未列出的預設儲存類別為 S3 標準。) 針對保留期，請輸入您要在該儲存類別中儲存物件的天數。您可以指定多個轉變。

   若要指定 S3 物件的到期時間，請選擇儲存類別到期。然後，針對保留期，在建立物件後，使用任何儲存類別，輸入您要在 Amazon S3 中存放物件的總天數。此時間週期結束時，物件會過期，Amazon S3 會刪除物件。
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，請使用安全性湖泊 API 的UpdateDataLake作業。如果您正在使用 AWS CLI，請執行命update-data-lake令。在您的要求中，使用`lifecycleConfiguration`參數來指定新設定：

- 若要變更轉換設定，請使用`transitions`參數指定要在特定 Amazon S3 儲存類別中存放 S3 物件的每個新時間週期 (`days`)，以天為單位 (`storageClass`)。
- 若要變更整體保留期間，請在建立物件之後，使用`expiration`參數指定要使用任何儲存類別存放 S3 物件的總天數。此保留期結束時，物件會過期，Amazon S3 會刪除物件。

「安全湖」會將設定套用至您在`configurations`物件`region`欄位中指定的「區域」。

例如，下列 AWS CLI 命令會更新「`us-east-1`地區」的資料到期設定和儲存轉換設定。在此區域中，物件會在 500 天後過期，物件會在 30 天後轉換至 `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"
```

累計區域

彙總區域會合併來自一或多個貢獻區域的資料。這可協助您遵守區域資料合規性要求。

如需設定彙總區域的指示，請參閱設定彙總區域。

開放網路安全架構架構架構 (OCSF)

什麼是 OCSF？

開放網絡安全架構框架（OCSF）是網絡安全行業領先合作夥伴 AWS 和領先合作夥伴的協作開源工作。OCSF 提供常見安全性事件的標準結構描述、定義版本控制準則以促進結構描述演進，並包含安全性記錄檔產生者和取用者的自我控管程序。OCSF 的公開原始程式碼託管於 GitHub.

安全湖會自動將來自本機支援的記錄檔和事件轉換為 OCSF 結構 AWS 服務 描述。在轉換為 OCSF 之後，安全湖將資料存放在您的 Amazon Simple Storage Service (Amazon S3) 儲存貯體 (每個儲存貯體一個 AWS 區域) 儲存貯體 AWS 帳戶中。從自訂來源寫入安全湖的記錄檔和事件必須遵守 OCSF 結構描述和 Apache 實木地板格式。訂閱者可以將記錄和事件視為一般 Parquet 記錄，或套用 OCSF 結構描述事件類別，以更精確地解譯記錄中包含的資訊。

事件類別

來自指定安全湖泊來源的記錄檔和事件與 OCSF 中定義的特定事件類別相符。DNS 活動、SSH 活動和驗證是 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。

來源識別

OCSF 使用各種欄位來協助您判斷特定記錄檔集或事件來源的位置。這些是本機支援的相關欄位值 AWS 服務 ，做為 Security Lake 中的來源。

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

來源	中繼資料產品名稱	元數據產品. 供應商名稱	元數據產品. 功能. 名稱	類別名稱	元數據版本
CloudTrail Lambda 數據事件	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail 管理事件	CloudTrail	AWS	Management	API Activity、Au ation 或	1.0.0-rc.2

來源	中繼資料產品名稱	元數據產品.供應商名稱	元數據產品.功能. 名稱	類別名稱	元數據版本
				Account Change	
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 Security Hub ProductName 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	中繼資料產品名稱	元數據產品.供應商名稱	元數據產品.功能. 名稱	類別名稱	元數據版本
CloudTrail Lambda 數據事件	CloudTrail	AWS	Data	API Activity	1.1.0
CloudTrail 管理事件	CloudTrail	AWS	Management	API Activity、Authentication 或 Account Change	1.1.0
CloudTrail S3 資料事件	CloudTrail	AWS	Data	API Activity	1.1.0

來源	中繼資料產品名稱	元數據產品.供應商名稱	元數據產品.功能. 名稱	類別名稱	元數據版本
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
安全中樞	符合 AWS 安全性尋找格式 (ASFF) 值 ProductName	符合 AWS 安全性尋找格式 (ASFF) 值 CompanyName	符合 ASFF 的featureName 值 ProductFields	Vulnerability Finding, Compliance Finding, or Detection Finding	1.1.0
VPC 流量日誌	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0
EKS 稽核記錄檔	Amazon EKS	AWS	Elastic Kubernetes Service	API Activity	1.1.0

與安全湖集成

Amazon 安全湖與其他 AWS 服務 和第三方產品集成。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。下列主題說明哪些產品以 AWS 服務 及協力廠商產品與 Security Lake 整合。

主題

AWS 服務 與安全湖集成

Amazon 安全湖集成與其他 AWS 服務. 服務可以作為來源整合、訂閱者整合或兩者運作。

來源整合具有下列屬性：

- 將資料傳送至安全湖
- 資料到達結開放網路安全架構架構架構 (OCSF)構描述
- 數據到達阿帕奇鑲木地板格式

訂閱者整合具有下列屬性，可從 HTTPS 端點或 Amazon Simple Queue Service (Amazon SQS) 的安全湖讀取來源資料，或直接查詢來源資料 AWS Lake Formation

下節將說明與哪些 AWS 服務 Security Lake 整合，以及每個整合的運作方式。

與整合 AWS AppFabric

整合類型：來源

AWS AppFabric這是一項無程式碼服務，可連接整個組織的軟體即服務 (SaaS) 應用程式，因此 IT 和安全團隊可以使用標準結構描述和中央儲存庫來管理和保護應用程式。

安全湖如何接收 AppFabric 發現

您可以將 AppFabric 稽核日誌資料傳送到安全湖，方法是選取 Amazon Kinesis Data Firehose 做為目的地，然後設定 Kinesis 資料防火管，將 OCSF 結構描述和 Apache 鑲木地板格式的資料傳送至安全湖。

必要條件

您必須先將 OCSF 標準化 AppFabric 稽核記錄輸出至 Kinesis Data Firehose 串流，才能將稽核記錄傳送至安全湖。然後，您可以設定 Kinesis Data Firehose，將輸出傳送到您的安全湖 Amazon S3 儲存貯體。如需詳細資訊，請參閱 Amazon Kinesis 開發人員指南中的目的地選擇 Amazon S3。

將您的發 AppFabric 現發現發送到安全湖

若要在完成前述必要條件之後將 AppFabric 稽核記錄檔傳送至 Security Lake，您必須同時啟用這兩項服務，並在 Security Lake 中新增 AppFabric 為自訂來源。如需新增自訂來源的指示，請參閱從自訂來源收集資料。

停止接收安全湖中的 AppFabric 記錄

若要停止接收 AppFabric 稽核記錄，您可以使用 Security Lake 主控台、Security Lake API，或 AWS CLI 將其 AppFabric 作為自訂來源進行刪除。如需說明，請參閱刪除自訂來源。

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。

當您整合安全湖和 Detective 時，您可以從 Detective 查詢安全湖儲存的原始記錄資料。如需詳細資訊，請參閱與 Amazon 安全湖整合。

與 Amazon 服 OpenSearch 務集成

整合類型：訂閱者

Amazon Ser OpenSearch vice 是一種受管服務，可讓您輕鬆部署、操作和擴展 OpenSearch AWS 雲端. 使用 OpenSearch 服務擷取將資料導入您的 OpenSearch Service Service 叢集，您可以更快地獲得深入解析，以進行時間敏感的安全性調查。您可以迅速回應安全性事件，協助保護您的業務關鍵資料和系統。

OpenSearch 服務儀表板

將 OpenSearch 服務與 Security Lake 整合後，您可以設定 Security Lake，透過無伺 OpenSearch 服器服務擷取將不同來源的安全性資料傳送至 OpenSearch 服務服務。如需如何設定 OpenSearch 服

務擷取以處理安全資料的詳細資訊，請參閱使用 Amazon 服 OpenSearch 務擷取從 Amazon Security Lake 資料產生安全洞見。

OpenSearch 服務擷取開始將資料寫入您的 OpenSearch 服務服務網域之後。要使用預先構建的儀表板可視化數據，Nnvigate 到儀表板並選擇任何一個已安裝的儀表板。

與 Amazon 集成 QuickSight

整合類型：訂閱者

Amazon QuickSight 是雲端規模商業智慧 (BI) 服務，您可以使用它向與您合作的人員提供 easy-to-understand 洞察，無論他們身在何處。Amazon 會 QuickSight 連線到雲端中的資料，並結合來自許多不同來源的資料。Amazon QuickSight 讓決策者有機會在互動式視覺環境中探索和解譯資訊。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。

Amazon QuickSight 儀表

若要在 Amazon 中視覺化您的 Amazon Security Lake 資料 QuickSight，建立所需的 AWS 物件，並將基本資料來源、資料集、分析、儀表板和使用者群組部署到 Amazon QuickSight 相關的安全湖。如需詳細指示，請參閱與 Amazon 整合 QuickSight。

與 Amazon 集成 SageMaker

整合類型：訂閱者

Amazon SageMaker 是全受管的機器學習 (ML) 服務。透過 Security Lake，資料科學家和開發人員可以快速且自信地建置、訓練機器學習模型，並將其部署到生產就緒的託管環境中。它提供執行 ML 工作流程的 UI 體驗，讓 SageMaker ML 工具可在多個整合式開發環境 (IDE) 中使用。

SageMaker 洞察

您可以使用 SageMaker Studio 產生安全湖的機器學習深入解析。 SageMaker Studio 是用於機器學習的 Web 整合式開發環境 (IDE)，可為資料科學家提供準備、建置、訓練和部署機器學習模型的工具。有了這個解決方案，您就可以快速部署一組 Python 筆記本，著重於 Security Lake 中的 AWS Security Hub 發現項目，也可以擴充以在 Security Lake 中合併其他來 AWS 源或自訂資料來源。如需詳細資訊，請參閱使用 Amazon 產生 Amazon 安全湖資料的機器學習深入解析 SageMaker。

與 Amazon 基岩集成

Amazon 基岩是一項全受管服務，可透過統一的 API，讓領先的 AI 新創公司和 Amazon 提供的高效能基礎模型 (FMs) 供您使用。透過 Amazon Bedrock 的無伺服器體驗，您可以快速開始使用、使用自己

的資料私人自訂基礎模型，並使用 AWS 工具輕鬆安全地將基礎模型整合並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 Amazon 基岩的生成 AI 功能和 SageMaker Studio 中的自然語言輸入來分析 Security Lake 中的資料，並致力於降低組織的風險並提高安全狀態。您可以自動識別適當的資料來源、產生和叫用 SQL 查詢，以及將調查中的資料視覺化，以減少進行調查所需的時間。有關詳情，請參閱使用 Amazon SageMaker 工作室和 Amazon 基岩為 Amazon 安全湖生成 AI 驅動的見解。

與整合 AWS Security Hub

整合類型：來源

AWS Security Hub提供您中安全性狀態的全面檢視， AWS 並協助您根據安全性產業標準和最佳實務來檢查環境。Security Hub 會從各 AWS 帳戶種服務和支援的協力廠商合作夥伴產品中收集安全性資料，並協助您分析安全性趨勢並找出最優先順序的安全性問題。

當您啟用安全性中樞，並將 Security Hub 發現項目新增為安全性湖泊中的來源時，Security Hub 會開始將新的發現項目和更新傳送至安全湖現有的發現項目。

安全湖如何接收 Security Hub 發現項目

在 Security Hub 中，將安全問題作為問題清單進行追蹤。某些發現項目來自其他 AWS 服務或協力廠商合作夥伴偵測到的問題。Security Hub 也會針對規則執行自動且持續的安全性檢查，藉此產生自己的發現項目。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。

安全湖接收 Security Hub 發現並將其轉換為開放網路安全架構架構架構 (OCSF).

將您的 Security Hub 發現發現傳送至安全湖

若要將 Security Hub 發現項目傳送至安全性湖泊，您必須啟用這兩項服務，並將 Security Hub 發現項目新增為安全性湖泊中的來源 如需新增來 AWS 源的說明，請參閱新增 AWS 服務 為來源。

如果您希望 Security Hub 產生控制項發現項目並將其傳送至 Security Lake，您必須啟用相關的安全性標準，並在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 使用指南》 AWS Config中的「啟用和設定」。

停止接收安全湖中的安全中心發現項目

若要停止接收 Security Hub 發現項目，您可以使用 Security Hub 主控台、Security Hub API 或 AWS CLI.

請參閱AWS Security Hub 使用者指南中的〈停用和啟用整合 (主控台) 的發現項目流程或停用整合 (Security Hub API、AWS CLI) 的發現項目流程。

與安全湖的第三方集成

Amazon 安全湖與多個第三方供應商整合。提供者可能會提供來源整合、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：

- 將資料傳送至安全湖
- 數據到達阿帕奇鑲木地板格式
- 資料到達結開放網路安全架構架構架構 (OCSF)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) 的安全湖讀取來源資料，或直接查詢來源資料 AWS Lake Formation
- 能夠讀取阿帕奇鑲木地板格式的數據
- 能夠讀取 OCSF 模式中的數據

服務整合可協助您 AWS 服務 在組織中實作安全湖和其他功能。他們還可以在報告、分析和其他使用案例方面提供協助。

若要搜尋特定合作夥伴供應商，請參閱 P artner Solutions Finder 案尋找器。若要購買第三方產品，請參閱 AWS Marketplace。

若要要求新增為合作夥伴整合或成為安全湖合作夥伴，請傳送電子郵件至 <securitylake-partners@amazon.com>。

如果您使用將發現項目傳送至的協力廠商整合 AWS Security Hub，如果已啟用 Security Lake 的 Security Hub 整合，您也可以在 Security Lake 中檢閱這些發現項目。如需啟用整合的指示，請參

閱與整合 AWS Security Hub。如需將發現項目傳送至 Security Hub 的第三方整合清單，請參閱AWS Security Hub 使用指南中的可用第三方合作夥伴產品整合。

在設定訂閱者之前，請先驗證訂閱者的 OCSF 記錄支援。如需最新詳細資訊，請參閱訂閱者的文件。

查詢整合

您可以查詢安全湖泊儲存在資料 AWS Lake Formation 庫和資料表中的資料。您也可以在安全湖主控台、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表格的SELECT許可授與查詢資料的 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，請參閱管理安全湖訂戶的查詢存取。

您可以為下列第三方合作夥伴設定與 Security Lake 的查詢整合。

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

Accenture – MxDR

整合類型：訂閱者、服務

Accenture's與 Security Lake 整合的 MXDR 可提供記錄和事件的即時資料擷取、管理異常偵測、威脅搜尋和安全性作業。這有助於分析和託管式偵測與回應 (MDR)。

作為服務整合，也Accenture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安全湖。稽核事件會轉換成 OCSF 結構描述和實木地板格式。

整合文件

Barracuda – Email Protection

整合類型：來源

Barracuda Email Protection偵測到新的網路釣魚電子郵件攻擊時，可以傳送事件至 Security Lake。您可以與資料湖中的其他安全性資料一起接收這些事件。

整合文件

Booz Allen Hamilton

整合類型：服務

作為服務整合，Booz Allen Hamilton透過將資料和分析與 Security Lake 服務融合在一起，使用資料導向的網路安全方法。

夥伴鏈接

ChaosSearch

整合類型：訂閱者

ChaosSearch提供多模型資料存取權給具有開放 API (例如 Elasticsearch 和 SQL) 的使用者，或使用原生包含的 Kibana 和超集使用者介面。您可以在ChaosSearch沒有保留限制的情況下使用 Security Lake 資料，以監控、警示和威脅搜尋。這有助於您面對現今複雜的安全環境和持續性威脅。

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充的方式儲存防火牆記錄檔。思科的 EnCore 用戶端會從防火牆管理中心串流防火牆記錄檔，執行結構描述轉換為 OCSF 結構描述，並將其儲存在 Security Lake 中。

整合文件

Claroty – xDome

整合類型：來源

Claroty xDome以最少的組態將在網路內偵測到的警示傳送至 Security Lake。彈性快速的部署選項有助於xDome保護網路內的延伸物聯網 (XIOT) 資產 (包含 IoT、IIoT 和 BMS 資產)，同時自動偵測早期威脅指標。

整合文件

CMD Solutions

整合類型：服務

CMD Solutions透過設計、自動化和持續的保證程序及早持續整合安全性，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。

夥伴鏈接

Confluent – Amazon S3 Sink Connector

整合類型：來源

Confluent使用完全受管的預先建置連接器，自動連接、設定和協調資料整合。Confluent S3 Sink Connector可讓您取得原始資料，並以原生鑲木地板格式將其大規模地沉入安全湖中。

整合文件

Contrast Security

整合類型：來源

用於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 應用程序，API 和微服務中提供實時漏洞檢測。評估與 Security Lake 整合，以協助提供所有工作負載的集中能見度。

整合文件

Cribl – Search

整合類型：訂閱者

您可以使Cribl Search用搜尋安全湖資料。

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支援的協力廠商來源傳送至 OCSF 結構描述中的安全湖。

整合文件

CrowdStrike – Falcon Data Replicator

整合類型：來源

此整合會以連續串流為基礎提取資料，將資料轉換為 OCSF 結構描述，然後將其傳送至 Security Lake。CrowdStrike Falcon Data Replicator

整合文件

CyberArk – Unified Identify Security Platform

整合類型：來源

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

整合文件

Darktrace – Cyber AI Loop

整合類型：來源

Darktrace與安全湖整合為安全湖帶來了Darktrace自我學習的力量。來自的洞察Cyber AI Loop可以與組織安全性堆疊中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性發現項目。

整合文件 (登入入Darktrace口網站以檢閱文件)

Datadog

整合類型：訂閱者

Datadog Cloud SIEM偵測雲端環境的即時威脅，包括 Security Lake 中的資料，並在單一平台上統一 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協助您快速儲存、分析和視覺化您的標準化安全性資料。CAE 套件的自訂分析、人工智慧和機器學習功能會根據 Security Lake 中 OCF 格式資料執行的模型，自動提供可行的見解。

作為服務整合，也Deloitte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

AWS 支援從安全湖擷取的Devo收集器。此整合可協助您分析並處理各種安全使用案例，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 收集安全事件並對其進行監控，以偵測和警示潛在的安全威脅。這有助於組織更好地了解其安全狀況，並主動識別和回應威脅。

作為服務整合，也DXC可以協助您在組織中實作 Security Lake。

整合文件

Eviden— AIsaac (以前Atos)

整合類型：訂閱者

此AIsaac MDR平台會使用 Security Lake 中 OCSF 結構描述擷取的 VPC 流程記錄，並利用 AI 模型偵測威脅。

整合文件

ExtraHop – Reveal(x) 360

整合類型：來源

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

整合文件

Falcosidekick

整合類型：來源

Falcosidekick收集法爾科事件並將其發送到安全湖。此整合會使用 OCSF 結構描述匯出安全性事件。

整合文件

Gigamon – Application Metadata Intelligence

整合類型：來源

Gigamon Application Metadata Intelligence (AMI)透過重要的中繼資料屬性，為您提供可觀察性、SIEM 和網路效能監控工具。這有助於提供更深入的應用程式能見度，讓您可以精確找出效能瓶頸、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、排定優先順序、資料來源上線，並透過 Security Lake 提供的現有工具和整合，協助客戶查詢其資料。

夥伴鏈接

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，可識別並預防混合雲中的威脅。此整合支援資料存取和查詢存取。

有關使用 AWS CloudTrail 日誌的集成文檔

使用 Amazon Athena 進行查詢的整合文件

Infosys

整合類型：服務

Infosys協助您根據組織需求自訂 Security Lake 實作，並提供自訂深入解析。

夥伴鏈接

Insbuilt

整合類型：服務

Insbuilt專門從事雲端諮詢服務，可協助您瞭解如何在組織中實作 Security Lake。

夥伴鏈接

Kyndryl – AIOps

整合類型：訂閱者、服務

Kyndryl與 Security Lake 整合，提供網路資料、威脅情報和人工智慧型分析的互通性。身為資料存取訂閱者，會從 Security Lake Kyndryl 擷取 AWS CloudTrail 管理事件以供分析之用。

作為服務整合，也Kyndryl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與 Security Lake 整合為資料來源，並針對您 AWS 環境中的弱點、錯誤設定以及已知和未知威脅提供安全性發現。

整合文件

Laminar

整合類型：來源

Laminar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專門從事雲端諮詢服務，可協助您瞭解如何在組織中實作 Security Lake。我們將 Security Lake 與整合式 ISV 解決方案連接起來，以建置自訂任務，並建立與客戶需求相關的客製化見解。

整合文件

Monad

整合類型：來源

Monad自動將您的資料轉換為 OCSF 結構描述，並將其傳送至您的安全湖資料湖。

整合文件

NETSCOUT – Omnis Cyber Intelligence

整合類型：來源

透過與 Security Lake 整合，可NETSCOUT成為安全性發現項目的自訂來源，以及針對企業發生的情況 (例如網路威脅、安全風險和攻擊面變更) 的詳細安全性深入解。這些發現項目是由NETSCOUT CyberStreams和在客戶帳戶中產生Omnis Cyber Intelligence，然後傳送至 OCSF 結構描述中的安全湖。擷取的資料也符合 Security Lake 來源的其他需求和最佳做法，包括格式、結構描述、磁碟分割和效能相關層面。

整合文件

Netskope – CloudExchange

整合類型：來源

Netskope透過與 Security Lake 共用安全性相關記錄檔和安全威脅資訊，協助您強化安全狀態。Netskope發現結果會使用外掛程式傳送至 Security Lake，該CloudExchange外掛程式可在本機資料中心內 AWS 或本機資料中心中以 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New Relic使用New Relic授權金鑰將資料傳送到

整合文件

Okta – Workforce Identity Cloud

整合類型：來源

Okta透過 Amazon EventBridge 整合，將身分記錄傳送至 OCSF 結構描述中的安全湖。 Okta System Logs在 OCSF 模式中，將幫助安全和數據科學家團隊按開源標準查詢安全事件。從 Okta 產生標準化的 OCSF 記錄可協助您在一致的結構描述下執行稽核活動，並產生與驗證、授權、帳戶變更和實體變更相關的報告。

整合文件

AWS CloudFormation 要在安全湖中新增Okta為自訂來源的範本

Orca – Cloud Security Platform

整合類型：來源

透過在 OCSF 架構中傳送雲端偵測 AWS 與回應 (CDR) 事件，與安全湖整合的Orca無代理雲端安全平台。

整合文件 (登入入Orca口網站以檢閱文件)

Palo Alto Networks – Prisma Cloud

整合類型：來源

Palo Alto Networks Prisma Cloud彙總雲端原生環境中虛擬機器的弱點偵測資料，並將其傳送至 Security Lake。

整合文件

Palo Alto Networks – XSOAR

整合類型：來源

Palo Alto Networks XSOAR已經建立了與 XSOAR 和安全湖的用戶集成。

整合文件

Ping Identity – PingOne

整合類型：來源

PingOne以 OCSF 結構描述和實木複合地板格式傳送帳戶修改警示至安全湖，讓您能夠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

普華永道帶來的知識和專業知識，以幫助客戶建立融合中心，以滿足他們的個人需求。融合中心建立在 Amazon Security Lake 上，能夠合併來自各種來源的資料，以建立近乎即時的集中式檢視。

整合文件

Rapid7 – InsightIDR

整合類型：訂閱者

InsightIDRRapid7SIEM/XDR 解決方案可擷取 Security Lake 中的記錄檔，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以資料融合為基礎，提供全企業的大規模威脅探索方法，並提供精細的安全性、適應性強的工作流程和報告。

整合文件

Sailpoint

整合類型：來源

整合的合作夥伴產品：SailPoint IdentityNow

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

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，並擴展其偵測與回應能力。

整合文件

SentinelOne

整合類型：訂閱者

該SentinelOne Singularity™ XDR平台將即時偵測和回應延伸到在現場部署和公有雲基礎設施上執行的端點、身分和雲端工作負載，包括 Amazon 彈性運算雲端 (Amazon EC2)、亞馬遜彈性容器服務 (Amazon ECS) 和亞馬遜彈性 Kubernetes 服務 (Amazon EKS)。

整合文件 (登入入SentinelOne口網站以檢閱文件)

Sentra – Data Lifecyle Security Platform

整合類型：來源

在您的帳戶中部署Sentra掃描基礎結構之後，Sentra擷取發現項目並將其導入您的 SaaS 中。這些發現項目是中繼資料，可在 OCSF 結構描述中Sentra儲存並稍後將串流至安全湖以供查詢。

整合文件

SOC Prime

整合類型：訂閱者

SOC Prime透過 Amazon OpenSearch 服務和亞馬 Amazon Athena 與安全湖整合，以便根據零信任里程碑進行智慧資料協調和威脅追捕。 SOC Prime使安全團隊能夠提高威脅可見性並調查事件，而不會出現大量警報。您可以使用可重複使用的規則和查詢，在 OCSF 結構描述中自動轉換為 Athena 和 OpenSearch Service，節省開發時間。

整合文件

Splunk

整合類型：訂閱者

Amazon Web Services (AWS) 的Splunk AWS 附加元件支援從安全湖擷取。此整合可透過從 Security Lake 訂閱 OCSF 結構描述中的資料，協助您加速威脅偵測、調查和回應速度。

整合文件

Stellar Cyber

整合類型：訂閱者

Stellar Cyber使用來自安全湖泊的記錄檔，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消耗來自 Security Lake 的資料 AWS，並在內部部署和混合雲環境中提供廣泛的可見性。Sumo Logic 為安全團隊提供所有安全工具的全面可見性、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，並透過低程式碼教戰手冊和案例管理傳送資料，以加快威脅偵測、調查和事件回應速度。

整合文件 (登入入Swimlane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，以最大限度地提高監督、簡化調查並簡化合規性。

整合文件

Talon

整合類型：來源

適用於整合的合作夥伴產品：Talon 企業瀏覽器

Talon's Enterprise Browser這是一個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，提供可見度和選項，以便在偵測、鑑識和調查之間進行交叉關聯的事件。

整合文件 (登入入Talon口網站以檢閱文件)

Tanium

整合類型：來源

Tanium Unified Cloud Endpoint Detection, Management, and Security平台將庫存資料提供給 OCSF 架構中的安全湖。

整合文件

TCS

整合類型：服務

提TCS AWS Business Unit供創新，經驗和人才。這種整合由十年的共同價值創造、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，可協助您快速偵測並調查潛在的安全威脅。通過將廣泛的時間框架和日誌來源的各種威脅指標相關聯，Tego Cyber 發現了隱藏的威脅。該平台具有高度情境的威脅情報，可在威脅檢測和調查方面提供精確和洞察力。

整合文件

Tines – No-code security automation

整合類型：訂閱者

Tines No-code security automation運用 Security Lake 中集中的安全性資料，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、訂戶

Torq作為自訂來源和訂閱者，與安全湖無縫整合。 Torq透過簡單的無程式碼平台，協助您實作企業級自動化和協調作業。

整合文件

Trellix – XDR

整合類型：來源、訂戶

作為開放式 XDR 平台，Trellix XDR支援安全湖整合。 Trellix XDR可以利用 OCSF 結構描述中的資料進行安全性分析使用案例。您也可以在中使用超過 1,000 個安全事件來源來增強您的安全湖資料湖。Trellix XDR這可協助您擴充 AWS 環境的偵測與回應功能。擷取的資料與其他安全風險相關，為您提供必要的教戰手冊，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從您的 Amazon Elastic Compute Cloud (EC2) 執行個體傳送下列資訊到安全湖：

- DNS 查詢活動
- 檔案活動
- 網路活動
- 處理活動
- 登錄值作業
- 使用者帳戶活動

整合文件

Uptycs – Uptycs XDR

整合類型：來源

Uptycs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安全湖。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

通過使用Vectra Detect for AWS，您可以使用專用 AWS CloudFormation 模板將高保真度警報作為自定義源發送到 Security Lake。

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旨在安全地處理用戶數據，為每個源提供查詢訪問權限，並優化查詢成本。

整合文件

Wipro

整合類型：來源、服務

這項整合可讓您從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性態勢。

作為服務整合，也Wipro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 之間的整合利用 OCSF 結構描述 (專為可延伸和標準化安全性資料交換而設計的開放原始碼標準)，有助於在單一安全性資料湖中收集雲端安全性資料。

整合文件 (登入入Wiz口網站以檢閱文件)

Zscaler – Zscaler Posture Control

整合類型：來源

Zscaler Posture Control™雲端原生應用程式保護平台，會將安全發現項目傳送至 OCSF 結構描述中的安全性湖。

整合文件

亞馬遜安全湖中的安全

雲端安全是 AWS 最重視的一環。身為 AWS 的客戶，您將能從資料中心和網路架構中獲益，這些都是專為最重視安全的組織而設計的。

安全是 AWS 與您共同肩負的責任。共同的責任模式將其稱為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護執行 AWS 雲端 內 AWS 服務的基礎設施。AWS 提供的服務，也可讓您安全使用。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 AWS 合規計劃的一部分。若要了解適用於 Amazon Security Lake 的合規計劃，請參閱AWS合規計劃合規計劃AWS服務範的服務。
- 雲端內部的安全：您的責任取決於所使用的 AWS 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。

本文件可協助您瞭解如何在使用 Security Lake 時套用共同的責任模型。下列主題說明如何設定 Security Lake 以符合安全性和合規性目標。您也會學到如何使用其他可AWS協助您監控和保護 Security Lake 資源的服務。

主題

- Amazon 安全湖的身分和存取管理
- Amazon 安全湖中的資料保護
- Amazon 安全湖的合規驗證
- 安全性湖泊的安全性最佳做法
- 亞馬遜安全湖的彈性
- 亞馬遜安全湖的基礎設施安全
- 安全湖中的組態和弱點分析
- 監控 Amazon Security Lake ake ake

Amazon 安全湖的身分和存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Security Lake 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，視您在安全湖中所做的工作而定。

服務使用者 — 如果您使用 Security Lake 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Security Lake 功能來完成工作時，您可能需要額外的權限。瞭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。如果您無法存取安全湖中的功能，請參閱疑難排解 Amazon 安全湖身分和存取。

服務管理員 — 如果您負責公司的安全湖資源，您可能擁有安全湖的完整存取權。決定您的服務使用者應該存取哪些 Security Lake 功能和資源是您的工作。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。若要深入瞭解貴公司如何搭配安全湖使用 IAM，請參閱Amazon 安全湖如何與 IAM 搭配使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理 Security Lake 存取權的詳細資訊。若要檢視可在 IAM 中使用的安全湖身分型政策範例，請參閱。Amazon 安全湖的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司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識別的範例。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 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，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 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

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) 來增加帳戶的安全性。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》中的在 AWS 中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務 和資源。此身分稱為 AWS 帳戶 root 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作業。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

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

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，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，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。如需詳細資訊，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。您無法以群組身分登入。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過程變得更為容易。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，但角色僅提供暫時憑證。如需進一步了解，請參閱《IAM 使用者指南》中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色方法的相關資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色。

使用暫時憑證的 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，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。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。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。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 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。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。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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給 AWS 服務 服務。
- 服務連結角色 — 服務連結角色是連結至. AWS 服務 服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。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 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。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 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。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暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱《IAM 使用者指南》中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的相關資訊，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哪些內容。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。若要授與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。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。如需瞭解如何在受管政策及內嵌政策間選擇，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。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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 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 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 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原則類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。如需許可邊界的相關資訊，請參閱《IAM 使用者指南》中的 IAM 實體許可邊界。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個

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 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的相關資訊，請參閱《AWS Organizations 使用者指南》中的 SCP 運作方式。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon 安全湖如何與 IAM 搭配使用

在您使用 IAM 管理安全湖的存取權限之前，請先了解哪些 IAM 功能可與安全湖搭配使用。

您可以搭配 Amazon 安全湖使用的 IAM 功能

IAM 功能	安全湖支持
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
主體許可	是

IAM 功能	安全湖支持
服務角色	否
服務連結角色	是

若要深入瞭解安全湖和其他 AWS 服務如何搭配大多數 IAM 功能運作，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

安全湖泊的身分型原則

支援身分型政策	是

身分型政策是可以連接到身分 (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。若要瞭解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。若要了解您在 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。

安全湖支援以身分識別為基礎的原則。如需詳細資訊，請參閱 Amazon 安全湖的身分型政策範例。

安全湖中以資源為基礎的政策

支援以資源基礎的政策	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。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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。AWS 服務

若要啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作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。當主體和資源不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策附

加到實體來授予許可。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 角色與資源型政策有何差異。

安全湖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。您不會將這些以資源為基礎的政策附加到 S3 儲存貯體。安全湖會代表您自動建立這些原則。

範例資源是具有 Amazon 資源名稱 (ARN) 的 `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}` S3 儲存貯體。在此範例中，`region`是您已啟用 Security Lake 的特定 AWS 區域 位置，而且`bucket-identifier`是 Security Lake 指派給值區的唯一區域字母數字字串。安全湖會建立 S3 儲存貯體來存放該區域的資料。資源策略定義了哪些主參與者可以對值區執行動作。以下是 Security Lake 附加到存儲桶的基於資源的策略（存儲桶策略）示例：

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

```
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-east-1:{DA-AccountID}:*"
                }
            }
        }
    ]
}
```

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識別為基礎的政策和資源型政策。

安全湖的政策動作

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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

如需安全湖動作的清單，請參閱服務授權參考中的 Amazon Security Lake 定義的動作。

Security Lake 中的原則動作會在動作之前使用下列前置詞：

```
securitylake
```

例如，若要授與使用者存取特定訂戶相關資訊的權限，請在指派給該使用者的策略中加入`securitylake:GetSubscriber`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Security Lake 會定義自己的一組動作，用來描述您可以使用此服務執行的工作。

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視以身分識別為基礎的原則範例，請參閱。Amazon 安全湖的身分型政策範例

安全湖的原則資源

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哪些內容。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 (例如列出作業)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

Security Lake 會定義下列資源類型：特定的訂閱者和資 AWS 帳戶 料湖組態 AWS 區域。您可以使用 ARN 在策略中指定這些類型的資源。

如需安全湖資源類型和每種資源類型的 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資源類型指定哪些動作，請參閱服務授權參考中由 Amazon Security Lake 定義的動作。

若要檢視以身分識別為基礎的原則範例，請參閱。Amazon 安全湖的身分型政策範例

安全湖泊的原則條件金鑰

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哪些內容。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，請使用邏輯OR運算來 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與該 IAM 使用者。如需詳細資訊，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條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

如需安全湖條件金鑰的清單，請參閱服務授權參考中的 Amazon Security Lake 的條件金鑰。若要了解可將條件金鑰與哪些動作和資源搭配使用，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原則範例，請參閱Amazon 安全湖的身分型政策範例。

安全湖中的存取控制清單 (ACL)

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。

安全湖不支援 ACL，這表示您無法將 ACL 附加至安全湖資源。

以屬性為基礎的存取控制 (ABAC) 搭配安全湖泊

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。您可以將標籤附加到 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。

若要根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件金鑰，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 的相關資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。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)。

您可以將標籤附加到 Security Lake 資源 — 訂閱者，以及個 AWS 帳戶 別的資料湖組態。 AWS 區域 您也可以透過在策略的Condition元素中提供標籤資訊來控制對這些類型資源的存取。如需標記安全湖資源的資訊，請參閱標記 Amazon 安全湖資源。如需以身分識別為基礎的政策範例，該策略可根據該資源的標籤控制對資源的存取，請參閱。Amazon 安全湖的身分型政策範例

搭配安全湖使用臨時登入資料

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。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。如需切換角色的相關資訊，請參閱《IAM 使用者指南》中的切換至角色 (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。

安全湖支援使用臨時登入資料。

安全湖的轉寄存取工作階段

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，您會被視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS

服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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》。

某些安全湖動作需要其他相依動作的權限才能執行其他動作 AWS 服務。如需這些動作的清單，請參閱服務授權參考中由 Amazon Security Lake 定義的動作。

安全湖泊的服務角色

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給 AWS 服務 服務。

安全湖不會假設或使用服務角色。但是，當您使用安全湖時 EventBridge AWS Lambda，Amazon 和 Amazon S3 等相關服務會承擔服務角色。若要代表您執行動作，Security Lake 會使用服務連結角色。

> **Warning**
>
> 變更服務角色的權限可能會在您使用 Security Lake 時造成作業上的問題。只有當 Security Lake 提供指引時，才編輯服務角色。

安全湖泊的服務連結角色

支援服務連結角色	是

服務連結角色是連結至. AWS 服務 服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

安全湖使用名為AWSServiceRoleForAmazonSecurityLake的 IAM 服務連結角色。Security Lake 服務連結角色授與代表客戶操作安全性資料湖服務的權限。此服務連結角色是直接連結至安全湖的 IAM 角色。它是由安全湖預先定義的，它包括安全湖代表您呼叫其他人所需 AWS 服務 的所有權限。安全湖泊會在所有可用安全湖泊的 AWS 區域 地方使用此服務連結角色。

如需有關建立或管理 Security Lake 服務連結角色的詳細資訊，請參閱亞馬遜安全湖的服務連結角色。

Amazon 安全湖的身分型政策範例

依預設，使用者和角色沒有建立或修改 Security Lake 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授與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。

若要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。

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 ARN 格式，請參閱服務授權參考中的 Amazon Security Lake 的動作、資源和條件金鑰。

主題

政策最佳實務

以身分識別為基礎的原則會決定某人是否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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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權。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 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，可協助您編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 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。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 使用者指南中的設定 MFA 保護的 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。

使用安全湖控制台

若要存取 Amazon 安全湖主控台，您必須擁有一組最低限度的許可。這些權限必須允許您列出並檢視您的 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。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。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。

為確保使用者和角色可以使用 Security Lake 主控台，請建立 IAM 政策，為他們提供主控台存取權。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 身分。

如果您建立的策略允許使用者或角色使用 Security Lake 主控台，請確定該策略針對這些使用者或角色需要在主控台上存取的資源包含適當的動作。否則，他們將無法在控制台上導航到或顯示有關這些資源的詳細信息。

例如，若要使用主控台新增自訂來源，必須允許使用者執行下列動作：

- `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 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

範例：允許組織管理帳戶指定及移除委派的管理員

此範例顯示如何建立原則，以允許 AWS Organizations 管理帳戶的使用者指定和移除其組織的委派 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

在以身分識別為基礎的原則中，您可以使用條件根據標籤來控制 Security Lake 資源的存取。此範例顯示如何建立政策，以允許使用者使用 Security Lake 主控台或 Security Lake API 檢閱訂閱者。不過，只有當訂閱者的`Owner`標籤值是使用者的使用者名稱時，才會授與權限。

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

```
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

在此範例中，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料，則必須標記訂閱者`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。如需有關使用條件金鑰的詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的條件。如需標記安全湖資源的資訊，請參閱標記 Amazon 安全湖資源。

AWS Amazon 安全湖的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 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。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略： AmazonSecurityLakeMetastoreManager

Amazon 安全湖使用 AWS Lambda 函數來管理資料湖中的中繼資料。透過使用此功能，Security Lake 可以將包含您的資料和資料檔案的 Amazon 簡單儲存服務 (Amazon S3) 分區編入資 AWS Glue 料目錄表格的索引。此受管政策包含 Lambda 函數的所有許可，可將 S3 分割區和資料檔案索引到資料 AWS Glue 表中。

許可詳細資訊

此政策包含以下許可：

- logs— 允許校長將 Lambda 函數的輸出記錄到 Amazon CloudWatch 日誌。
- glue— 允許主參與者對「 AWS Glue 資料目錄」表格執行特定寫入動作。這也可讓 AWS Glue 搜尋器識別資料中的分割區。
- sqs— 允許主體對 Amazon SQS 佇列執行特定的讀取和寫入動作，這些佇列會在物件新增至資料湖或更新物件時傳送事件通知。
- s3— 允許主體對包含您資料的 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 受管理的策略： 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，並讓第三方自訂訂閱者使用資料湖中的資料，並在建立這些角色時使用此政策來定義其許可的界限。您不需要採取行動即可使用此原則。如果使用客戶管理的 AWS KMS 金鑰加密資料湖，`kms:Decrypt`並新增`kms:GenerateDataKey`權限。

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

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

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

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

AWS 受管理的策略： AmazonSecurityLakeAdministrator

您可以將AmazonSecurityLakeAdministrator政策附加到主體，然後才能為其帳戶啟用 Amazon 安全湖。此原則會授與允許主體完整存取所有 Security Lake 動作的管理權限。然後，主體可以上線到安全湖，然後在安全湖中設定來源和訂閱者。

此原則包括 Security Lake 系統管理員可透過安全性湖泊在其他 AWS 服務上執行的動作。

該AmazonSecurityLakeAdministrator政策不支援建立 Security Lake 管理 Amazon S3 跨區域複寫、在 AWS Glue中註冊新資料分區、對新增至自訂來源的資料執行 Glue 爬蟲程式，或通知 HTTPS 端點訂閱者有關新資料的公用程式角色。您可以提前建立這些角色，如中所述開始使用 Amazon 安全湖。

除了AmazonSecurityLakeAdministrator受管理的原則之外，Security Lake 還需要上線和設定功能的lakeformation:PutDataLakeSettings權限。 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iam:CreateRole permission具有附加AmazonSecurityLakeAdministrator原則。

Lake Form 管理員擁有對 Lake Formation 控制台的完全訪問權限，並控制初始數據配置和訪問權限。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、註冊新分割區，以及設定資料表的權限。您必須在 Security Lake 系統管理員使用者或角色的原則中包含下列權限：

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

許可詳細資訊

此政策包含以下許可。

- `securitylake`— 允許主參與者完整存取所有安全湖動作。
- `organizations`— 允許主參與者從「組 Organ AWS izations」擷取有關組織中帳號的資訊。如果帳戶屬於某個組織，則這些權限允許 Security Lake 主控台顯示帳戶名稱和帳號。
- `iam`— 允許主參與者建立 Security Lake、和的服務連結角色 AWS Lake Formation Amazon EventBridge，作為啟用這些服務時的必要步驟。此外，還允許建立和編輯訂戶和自訂來源角色的原則，而這些角色的權限僅限於`AmazonSecurityLakePermissionsBoundary`原則所允許的項目。
- `ram`— 允許主參與者設定訂閱者對 Security Lake 來源的 Lake Formation基礎查詢存取權。
- `s3`— 允許主參與者建立和管理 Security Lake 值區，以及讀取這些值區的內容。
- `lambda`— 可讓主參與者管理在 AWS 來源傳遞和跨區域複寫之後 Lambda 用來更新 AWS Glue 表格分割區的項目。
- `glue`— 可讓主參與者建立及管理 Security Lake 資料庫與表格。

- lakeformation— 允許主參與者管理「安全性湖泊」表格的 Lake Formation 權限。
- events— 允許主參與者管理用來通知訂閱者 Security Lake 來源中新資料的規則。
- sqs— 允許主參與者建立和管理 Amazon SQS 佇列，該佇列可用來通知訂閱者 Security Lake 來源中的新資料。
- kms— 允許主體授與 Security Lake 使用客戶管理的金鑰寫入資料的存取權。
- secretsmanager— 允許主體透過 HTTPS 端點管理用來通知訂閱者安全湖來源中新資料的密碼。

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowActionsWithAnyResource",
    "Effect": "Allow",
    "Action": [
      "securitylake:*",
      "organizations:DescribeOrganization",
      "organizations:ListDelegatedServicesForAccount",
      "organizations:ListAccounts",
      "iam:ListRoles",
      "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
    "Effect": "Allow",
    "Action": [
      "glue:CreateCrawler",
      "glue:StopCrawlerSchedule",
      "lambda:CreateEventSourceMapping",
      "lakeformation:GrantPermissions",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "lakeformation:GetDatalakeSettings",
      "events:ListConnections",
      "events:ListApiDestinations",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "kms:DescribeKey"
```

```
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowManagingSecurityLakeS3Buckets",
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketNotification",
      "s3:PutBucketTagging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetBucketNotification"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaCreateFunction",
    "Effect": "Allow",
    "Action": [
      "lambda:CreateFunction"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
```

```
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaAddPermission",
    "Effect": "Allow",
    "Action": [
      "lambda:AddPermission"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringEquals": {
        "lambda:Principal": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "glue:CreateTable",
      "glue:GetTable"
    ],
    "Resource": [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
```

```
    "Sid": "AllowEventBridgeActions",
    "Effect": "Allow",
    "Action": [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
      "events:DeleteConnection",
      "events:DeleteApiDestination",
      "events:ListTargetsByRule",
      "events:RemoveTargets",
      "events:DeleteRule"
    ],
    "Resource": [
      "arn:aws:events:*:*:rule/AmazonSecurityLake*",
      "arn:aws:events:*:*:rule/SecurityLake*",
      "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
      "arn:aws:events:*:*:connection/AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowSQSActions",
    "Effect": "Allow",
    "Action": [
      "sqs:CreateQueue",
      "sqs:SetQueueAttributes",
      "sqs:GetQueueURL",
      "sqs:AddPermission",
      "sqs:GetQueueAttributes",
      "sqs:DeleteQueue"
    ],
    "Resource": [
      "arn:aws:sqs:*:*:SecurityLake*",
      "arn:aws:sqs:*:*:AmazonSecurityLake*"
    ],
    "Condition": {
```

```
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowKmsCmkGrantForSecurityLake",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "GenerateDataKey",
          "RetireGrant",
          "Decrypt"
        ]
      }
    }
  },
  {
    "Sid": "AllowEnablingQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "ram:ResourceArn": [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
```

```
      }
    }
  },
  {
    "Sid": "AllowConfiguringQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
      "ram:DeleteResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ram:ResourceShareName": "LakeFormation*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringCredentialsForSubscriberNotification",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
```

```
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": [
          "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
          "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
```

```
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCrossRegionReplicationS3Arn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
```

```
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:subscriber/*"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:events:*:*:rule/AmazonSecurityLake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowOnboardingToSecurityLakeDependencies",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
```

```
    "Resource": [
      "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
      "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition": {
      "StringLike": {
        "iam:AWSServiceName": [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
          "apidestinations.events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "AllowRolePolicyActionsforSubscibersandSources",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "StringEquals": {
        "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowRegisterS3LocationInLakeFormation",
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam:GetRolePolicy"
    ],
```

```
    "Resource": "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowIAMActionsByResource",
    "Effect": "Allow",
    "Action": [
      "iam:ListRolePolicies",
      "iam:DeleteRole"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "S3ReadAccessToSecurityLakes",
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid": "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid": "S3ResourcelessReadOnly",
    "Effect": "Allow",
    "Action": [
```

```
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  }
]
}
```

AWS 受管理的策略： SecurityLakeServiceLinkedRole

您無法將受SecurityLakeServiceLinkedRole管政策附加到 IAM 實體。此原則附加至服務連結角色，可讓 Security Lake 代表您執行動作。如需詳細資訊，請參閱 亞馬遜安全湖的服務連結角色。

AWS 受管理的策略： AWS GlueServiceRole

AWS GlueServiceRole受管理的原則會叫用爬行 AWS Glue 者程式，並允許 AWS Glue 編目自訂來源資料並識別分割區中繼資料。此中繼資料對於在「資料目錄」中建立和更新表格是必要的。

如需詳細資訊，請參閱 從自訂來源收集資料。

AWS 受管理原則的安全性湖泊更新

檢視有關 Security Lake AWS 受管理原則更新的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱安全湖文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AmazonSecurityLakeMetastoreManager – 更新現有政策	Security Lake 已更新原則，以新增中繼資料清理動作，可讓您刪除資料湖中的中繼資料。	2024年3月27日
AmazonSecurityLakeAdministrator – 更新現有政策	Security Lake 已更新原則以允許使iam:PassRole 用新AmazonSecurityLakeMetastoreManagerV2 角色，並可讓 Security Lake 部署或更新資料湖元件。	2024年2月23 日

變更	描述	日期
AmazonSecurityLake MetastoreManager – 新政策	Security Lake 新增了一項新的受管理政策，授予 Security Lake 管理資料湖中繼資料的權限。	2024 年 1 月 23 日
AmazonSecurityLakeAdministrator – 新政策	Security Lake 新增了一項新的受管理政策，可授與主體對所有 Security Lake 動作的完整存取權。	2023 年 5 月 30 日
安全湖開始跟踪更改	安全湖開始追蹤其 AWS 受管理原則的變更。	2022 年 11 月 29 日

亞馬遜安全湖的服務連結角色

安全湖使用名AWSServiceRoleForSecurityLake為的 AWS Identity and Access Management (IAM) 服務連結角色。此服務連結角色是直接連結至安全湖的 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 服務人並操作安全性資料湖服務所需的所有權限。安全湖泊會在所有可用安全湖泊的AWS 區域地方使用此服務連結角色。

服務連結角色無需在設定 Security Lake 時手動新增必要的權限。Security Lake 會定義此服務連結角色的權限，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。只有在刪除服務連結角色的相關資源後，才能刪除該角色。這可保護您的資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務資訊，請參閱《可搭配 IAM 運作的 AWS 服務》，尋找 Service-linked roles (服務連結角色) 欄中顯示為 Yes (是) 的服務。選擇具有連結的 [是]，以檢閱該服務的服務連結角色文件。

主題

- 安全性湖泊的服務連結角色權限
- 建立資訊安全湖服務連結角色
- 編輯資訊安全湖服務連結角色

- 刪除資訊安全湖服務連結角色
- 支援AWS 區域安全性湖泊服務連結角色

安全性湖泊的服務連結角色權限

安全湖泊使用名為AWSServiceRoleForSecurityLake的服務連結角色。此服務連結角色會信任securitylake.amazonaws.com服務擔任該角色。

角色的權限原則是名為的AWS受管理原則SecurityLakeServiceLinkedRole，可讓 Security Lake 建立和操作安全性資料湖。它還允許安全湖對指定的資源執行以下任務：

- 使用AWS Organizations動作擷取關聯帳號的資訊
- 使用亞馬遜彈性運算雲端 (Amazon EC2) 擷取有關 Amazon VPC 流程日誌的資訊
- 使用AWS CloudTrail動作擷取有關服務連結角色的資訊

角色設定為下列權限原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationsPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "DescribeOrgAccounts",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount"
            ],
            "Resource": [
                "arn:aws:organizations::*:account/o-*/*"
            ]
```

```
        },
        {
            "Sid": "AllowManagementOfServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateServiceLinkedChannel",
                "cloudtrail:DeleteServiceLinkedChannel",
                "cloudtrail:GetServiceLinkedChannel",
                "cloudtrail:UpdateServiceLinkedChannel"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
        },
        {
            "Sid": "AllowListServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:ListServiceLinkedChannels"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DescribeAnyVpc",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListDelegatedAdmins",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securitylake.amazonaws.com"
                }
            }
        }
    ]
```

```
}
```

您必須設定許可，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。

建立資訊安全湖服務連結角色

您不需要為安全湖泊手動建立AWSServiceRoleForSecurityLake服務連結角色。當您為您啟用安全湖泊時AWS 帳戶，安全湖會自動為您建立服務連結角色。

編輯資訊安全湖服務連結角色

安全湖泊不允許您編輯AWSServiceRoleForSecurityLake服務連結的角色。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照該角色。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》中的編輯服務連結角色。

刪除資訊安全湖服務連結角色

您無法從資訊安全湖中刪除服務連結角色。相反地，您可以從 IAM 主控台、API 或AWS CLI刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

刪除服務連結角色之前，您必須先確認角色沒有使用中的工作階段，並移除任何AWSServiceRoleForSecurityLake正在使用的資源。

> **Note**
>
> 當您嘗試刪除資源時，如果 Security Lake 正在使用此AWSServiceRoleForSecurityLake角色，則刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試該操作。

如果您刪除AWSServiceRoleForSecurityLake服務連結角色並需要重新建立，您可以為您的帳戶啟用 Security Lake，以再次建立該角色。當您再次啟用安全湖時，安全性湖泊會自動為您再次建立服務連結角色。

支援AWS 區域安全性湖泊服務連結角色

安全湖支援在所有可用安全湖泊的AWS 區域地方使用AWSServiceRoleForSecurityLake服務連結角色。如需目前提供安全湖泊的區域清單，請參閱Amazon Security Lake Security Lake Security Lake。

Amazon 安全湖中的資料保護

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 AWS 雲端 的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務 的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，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，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 憑證，並設定個人使用者。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 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務 內的所有預設安全控制項。
- 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。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，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) 140-2 概觀。

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 Name (名稱) 欄位。這包括當您使用主控台、API 或 AWS SDK AWS 服務 使用安全湖或其他工作時。AWS CLI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 安全湖使用AWS加密解決方案安全地存放您的靜態資料。原始安全日誌和事件資料存放在 Security Lake 管理的帳戶中的多租戶 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體中。安全湖使用AWS擁有的密鑰AWS Key Management Service（AWS KMS）對此原始數據進行加密。 AWS擁有的金鑰是一組AWS KMS金鑰，AWS服務 (在本例中為 Security Lake) 擁有並管理，以供多個帳戶使用。AWS

安全湖對原始日誌和事件資料執行擷取、轉換和載入 (ETL) 工作。處理過的資料會在安全湖服務帳戶中保持加密狀態。

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 (每個已在其中啟用 Security Lake AWS 區域 的儲存貯體有一個儲存貯體)。資料只會暫時存放在多租用戶 S3 儲存貯體中，直到 Security Lake 能夠可靠地將資料傳遞到單租戶 S3 儲存貯體。單租用戶值區包含以資源為基礎的政策，可授予 Security Lake 將記錄檔和事件資料寫入值區的權限。若要加密 S3 儲存貯體中的資料，您可以選擇 S3 受管加密金鑰或客戶管理金鑰 (來源AWS KMS)。這兩個選項都使用對稱加密。

使用 KMS 金鑰加密您的資料

根據預設，安全湖交付到 S3 儲存貯體的資料會使用 Amazon 伺服器端加密使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。若要提供您直接管理的安全層，您可以改為針對安全湖資料使用金AWS KMS鑰 (SSE-KMS) 的伺服器端加密。

安全湖泊主控台不支援 SSE-KMS。若要搭配安全性湖 API 或 CLI 使用 SSE-KMS，請先建立 KMS 金鑰或使用現有金鑰。您可以將原則附加至金鑰，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。對於客戶管理的金鑰，Security Lake 會將`CreateGrant`要求傳送至，以代表您建立授權AWS KMS。中的授權AWS KMS用於授予安全湖存取客戶帳戶中 KMS 金鑰的權限。

Security Lake 需要授權，才能在下列內部作業中使用您的客戶管理金鑰：

- 傳送`GenerateDataKey`要求AWS KMS以產生由客戶管理金鑰加密的資料金鑰。
- 將請`RetireGrant`求發送到AWS KMS。當您對資料湖進行更新時，此作業可讓新增至 AWS KMS 金鑰以進行 ETL 處理的授權淘汰。

安全湖不需要`Decrypt`權限。當授權的金鑰使用者讀取 Security Lake 資料時，S3 會管理解密，授權的使用者能夠以未加密的形式讀取資料。不過，訂閱者需要使用來源資料的`Decrypt`權限。如需有關訂閱者權限的詳細資訊，請參閱管理安全湖訂戶的資料存取。

當您建立金鑰原則或使用具有適當權限的現有金鑰原則時，您的 KMS 金鑰可以接受授與要求，讓 Security Lake 存取金鑰。如需建立金鑰原則的指示，請參閱AWS Key Management Service開發人員指南中的建立金鑰政策。將下列金鑰原則附加至您的 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 所需建立的 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，而訂閱者則可使用資料湖中的資料。名為的AWS受管理策略會`AmazonSecurityLakePermissionsBoundary`設定這些角色的權限界限。

加密 Amazon SQS 佇列

建立資料湖時，Security Lake 會在委派的安全湖管理員帳戶中建立兩個未加密的 Amazon 簡單佇列服務 (Amazon SQS) 佇列。您應該加密這些佇列以保護您的資料。Amazon 簡單佇列服務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來加密佇列，並授予 Amazon S3 服務主體許可以處理加密佇列。如需授與這些許可的指示，請參閱為什麼 Amazon S3 事件通知沒有傳送到使用伺服器端加密的 Amazon SQS 佇列？ 在AWS知識中心。

由於安全湖用AWS Lambda於支援資料上的擷取、傳輸和載入 (ETL) 任務，因此您還必須授與 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權限。

傳輸中加密

安全湖會加密AWS服務之間傳輸中的所有資料。Security Lake 會使用傳輸層安全性 (TLS) 1.2 加密通訊協定，自動加密所有網路間資料，藉此保護傳輸中的資料 (往返服務)。傳送至安全湖 API 的直接 HTTPS 要求是使用簽AWS章版本 4 演算法來簽署，以建立安全連線。

選擇不使用您的資料以改善服務

您可以使用AWS Organizations退出政策，選擇不讓您的資料用於開發和改善 AWS Security Lake 和其他安全服務。即使安全湖目前未收集任何此類資料，您也可以選擇退出。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性資料，也不會收集您上傳至此服務建立之安全性資料湖的安全性資料。為了開發和改善 Security Lake 服務以及其他AWS安全服務的功

能，Security Lake future 可能會收集此類資料，包括您從第三方資料來源上傳的資料。當 Security Lake 打算收集任何此類數據並描述其工作方式時，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，您的 AWS 帳戶必須由 AWS Organizations 集中管理。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 將在您選擇退出（如果有的話）之前刪除其收集和存儲的數據。
- 選擇退出後，安全湖將不再收集或儲存此資料。

Amazon 安全湖的合規驗證

要瞭解 AWS 服務 是否在特定法規遵循方案範圍內，請參閱法規遵循方案範圍內的 AWS 服務，並選擇您感興趣的法規遵循方案。如需一般資訊，請參閱 AWS 法規遵循方案。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您使用 AWS 服務 時的法規遵循責任取決於資料的敏感度、您的公司的合規目標，以及適用的法律和法規。AWS 提供以下資源協助您處理法規遵循事宜：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心的基準環境的架構考量和步驟。
- Amazon Web Services 的 HIPAA 安全與法規遵循架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規定的應用程式。

> **Note**
>
> 並非全部的 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源：這組手冊和指南可能適用於您的產業和位置。
- AWS 客戶合規指南：透過合規的角度瞭解共同的責任模式。這份指南橫跨多個架構 (包含國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準組織 (ISO))，總結保護 AWS 服務的最佳實務並將指導方針對應至安全控制。

- AWS Config 開發人員指南中的使用規則評估資源：AWS Config 服務可評估您的資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務 可供您全面檢視 AWS 中的安全狀態。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 controls reference。
- AWS Audit Manager – 此 AWS 服務 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。

安全性湖泊的安全性最佳做法

請參閱下列使用亞馬遜安全湖的最佳實務。

授予安全湖使用者可能的最低權限

為您的 AWS Identity and Access Management (IAM) 使用者、使用者群組和角色授予一組最低存取政策許可，以遵循最低權限原則。例如，您可能允許 IAM 使用者檢視 Security Lake 中的記錄來源清單，但不能建立來源或訂閱者。如需詳細資訊，請參閱 Amazon 安全湖的身分型政策範例

您也可以使用AWS CloudTrail在安全湖中追蹤 API 使用情況。CloudTrail提供使用者、群組或角色在安全湖中所採取之 API 動作的記錄。如需詳細資訊，請參閱使用記錄亞馬遜安全湖 API 呼叫 AWS CloudTrail。

檢視「摘要」頁面

Security Lake 主控台的 [摘要] 頁面提供過去 14 天影響安全湖服務和資料儲存貯體之 Amazon S3 儲存貯體的問題概觀。您可以進一步調查這些問題，以協助您減輕可能的安全性相關影響。

與安全中心整合

整合安全湖，並AWS Security Hub接收安全性湖泊中的安全中心發現。安全中心從許多不同AWS 服務和第三方集成生成發現。接收 Security Hub 發現項目可協助您取得合規狀態的概觀，以及您是否符合AWS安全性最佳做法。

如需詳細資訊，請參閱與整合 AWS Security Hub。

監控安全湖泊事件

您可以使用亞馬遜CloudWatch指標監控安全湖。CloudWatch每分鐘從安全湖收集原始數據，並將其處理為指標。您可以設定警示，在測量結果符合指定臨界值時觸發通知。

如需詳細資訊，請參閱 CloudWatchAmazon Security Lake 的指標。

亞馬遜安全湖的彈性

AWS 全球基礎架構是以 AWS 區域 與可用區域為中心建置的。AWS 區域 提供多個分開且隔離的實際可用區域，並以具備低延遲、高輸送量和高度備援特性的聯網相互連結。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、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

安全湖的可用性與區域可用性有關。跨多個可用區域發佈可協助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 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

除了AWS全球基礎設施之外，Security Lake 還提供資料由 Amazon Simple Storage Service (Amazon S3) 提供支援的多種功能，協助您支援資料彈性和備份需求。

生命週期組

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非預期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。

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。

亞馬遜安全湖的基礎設施安全

作為一項受管服務，Amazon 安全湖受到AWS全球網路安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 AWS 雲端安全。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的基礎設施保護。

您可以使用AWS已發佈的 API 呼叫透過網路存取安全湖。用戶端必須支援下列項目：

- 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，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

安全湖中的組態和弱點分析

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。

監控 Amazon Security Lake ake ake

Security Lake 整合了AWS CloudTrail，後者是一項服務，可提供由使用者、角色或其他角色所採取之動作的記錄AWS 服務。這包括來自安全湖控制台的動作，以及對安全湖 API 操作進行程式設計調用。通過使用收集的信息CloudTrail，您可以確定向安全湖發出了哪些請求。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，請參閱使用記錄亞馬遜安全湖 API 呼叫 AWS CloudTrail。

整合了，後者CloudWatch是一項服務，可讓您收集、檢視和分析 Security Lake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake ake CloudWatchSecurity Lake 資料湖的指標會以一分鐘的間隔自動收集並推送到CloudWatch。您也可以設定警示，以便在符合 Security Lake 量度的指定臨界值時傳送通知給您。如需安全性湖泊傳送至的所有指標清單 CloudWatch，請參閱安全 Lake 指標和維度。

CloudWatchAmazon Security Lake 的指標

您可以使用 Amazon Security Lake 監控CloudWatch，Amazon 會收集原始資料並將該資料處理成可讀且近乎即時的指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚資料 Lake 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

安全 Lake 指標和維度

AWS/SecurityLake 命名空間包含下列指標。

指標	描述
ProcessedSize	目前儲存在資料湖中的原生AWS 服務支援資料量。 單位：位元組

下列維度適用於安全湖度量。

維度	描述
Account	ProcessedSize 特定的量度AWS 帳戶。只有當您檢視Per-Account Source Version Metrics開啟的時，才能使用此維度CloudWatch。
Region	ProcessedSize 特定的量度AWS 區域。
Source	ProcessedSize 特定AWS日誌來源的測量結果。

維度	描述
SourceVersion	ProcessedSize 特定AWS日誌來源版本的測量結果。

您可以檢視特定 AWS 帳戶 (Per-Account Source Version Metrics) 或組織中所有帳戶的量度 (Per-Source Version Metrics)。

檢視安全湖的CloudWatch測量結果

您可以使用CloudWatch主控台、CloudWatch本身的命令列界面 (CLI) 或使用 CloudWatch API 的程式設計方式。選擇您偏好的方法，然後按照步驟存取 Security Lake 指標。

CloudWatch console

1. 開啟 CloudWatch 主控台，網址為：https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格上，選擇指標，所有指標，所有指標。
3. 在 [瀏覽] 索引標籤上，選擇 [安全湖]。
4. 選擇每個帳戶的來源版本量度或每個來源版本量度。
5. 選取測量結果以詳細檢視。您也可以選擇執行以下作業：
   - 若要排序指標，請使用欄標題。
   - 若要將指標圖形化，請選取指標名稱，並選擇圖形化。
   - 若要依測量結果篩選，請選取測量結果名稱，然後選擇新增以搜尋。

CloudWatch API

若要使用 CloudWatch API 存取安全湖度量，請使用GetMetricStatistics動作。

AWS CLI

若要使用存取安全湖度量AWS CLI，請執行get-metric-statistics命令。

有關使用指標進行監控的詳細資訊，請參閱 Amazon 使用CloudWatch者指南中的使用 Amazon 指CloudWatch標。

設定安全湖度量的CloudWatch警示

CloudWatch 亦可讓您設定到達指標的閾值時的警示。例如，您可以為ProcessedSize指標設定警示，以便在特定來源的資料量超過特定臨界值時收到通知。

如需設定鬧鐘的指示，請參閱 Amazon 使用CloudWatch者指南中的使用 Amazon CloudWatch 警示。

使用記錄亞馬遜安全湖 API 呼叫 AWS CloudTrail

Amazon Security Lake 與這項服務整合AWS CloudTrail，可提供安全湖中使用者、角色或服務所採取的動作記錄的AWS服務。CloudTrail將安全湖泊的 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 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付CloudTrail事件到 Amazon S3 儲存貯體，包括 Security Lake 的事件。如果您不設定追蹤記錄，仍然可以透過 CloudTrail 主控台中的 Event history (事件歷史記錄) 檢視最新的事件。使用收集的資訊 CloudTrail，您可以判斷向 Security Lake 提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間，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。

安全湖資訊 CloudTrail

當您建立帳戶時，系統會在您的 AWS 帳戶 中啟用 CloudTrail。當活動發生在 Security Lake 中時，該活動會與CloudTrail事件歷史記錄中的其他AWS服務事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄您AWS 帳戶的事件 (包括安全湖的事件)，請建立追蹤。追蹤可讓您CloudTrail將事件以日誌檔的形式傳遞到您指定的 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。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。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 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

安全湖動作會由安全性湖泊 API 參考記錄，CloudTrail並記錄在安全湖 API 參考中。例如，對 `UpdateDataLake`、`ListLogSources` 及 `CreateSubscriber` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌項目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：

- 該請求是否使用根或 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。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

瞭解安全性湖泊記錄檔項目

CloudTrail 日誌檔案包含一個或多個日誌項目。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 日誌檔案並非依公有 API 呼叫追蹤記錄的堆疊排序，因此不會以任何特定順序出現。

下列範例顯示「安全湖」GetSubscriber 動作的CloudTrail記錄項目。

```
{
   "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 Amazon 安全湖資源

標籤是可選的標籤，您可以定義並指派給 AWS 資源，包括特定類型的 Amazon Security Lake 資源。標籤可協助您以不同的方式識別、分類及管理資源，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原則、分配成本、區分資源，或識別支援特定合規性需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，以及個別 AWS 帳戶 的資料湖組態 AWS 區域。

主題

標記基本面

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」。標籤關鍵字是一般標示，可做為更特定標籤值的品類。標籤值是標籤金鑰的描述項。

例如，如果您新增訂閱者以分析來自不同環境的安全性資料 (一組雲端資料的訂閱者，另一組用於內部部署資料)，則可以將`Environment`標籤金鑰指派給這些訂閱者。關聯的標籤值可能`Cloud`適用於分析來源資料的訂閱者 AWS 服務，以及其他`On-Premises`用戶。

當您定義和指派標籤給 Amazon 安全湖資源時，請牢記下列事項：

- 每個資源的上限為 50 個標籤。
- 對於每個資源，每個標籤鍵必須是唯一的，並且只能有一個標籤值。
- 標籤鍵與值皆區分大小寫。最佳做法是，我們建議您定義策略，以便將標籤資本化，並在資源中一致地實作該策略。
- 一個標籤鍵最多可包含 128 個 UTF-8 字元。一個標籤值最多可包含 256 個 UTF-8 字元。字符可以是字母，數字，空格或以下符號：_。：/= +-@

- 前aws:綴保留供使用 AWS。您不能在您定義的任何標籤鍵或值中使用它。此外，您無法變更或移除使用此前置詞的標籤鍵或值。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標籤， AWS 帳戶 且僅適用於您指派標籤的標籤。 AWS 區域
- 如果您使用 Security Lake 將標籤指派給資源，標籤只會套用至直接儲存在適用的 Security Lake 中的資源 AWS 區域。這些資源不會套用至 Security Lake 在其他地方為您建立、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，則標籤僅會套用至指定區域的 Security Lake 中的資料湖組態。它們不適用於存放日誌和事件資料的 Amazon 簡易儲存服務 (Amazon S3) 儲存貯體。若要將標籤指派給關聯的資源，您可以使用 AWS Resource Groups 或存放資源 AWS 服務 的標籤，例如 Amazon S3 用於 S3 儲存貯體。將標籤指派給關聯資源可協助您識別資料湖的支援資源。
- 如果刪除資源，也會刪除指定給該資源的任何標籤。

有關其他限制、提示和最佳做法，請參閱標記資 AWS 源使用指南中的標記 AWS 資源。

> **Important**
>
> 請勿在標籤中儲存機密或其他類型的敏感資料。標籤可以從許多人訪問 AWS 服務，包括 AWS Billing and Cost Management。它們不打算用於敏感數據。

若要新增和管理安全湖資源的標籤，您可以使用安全湖主控台或安全湖 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。透過這種方式使用標籤，您可以對您中的哪些使用者和角色 AWS 帳戶 有權建立和標記資源，以及哪些使用者和角色有權更一般地新增、編輯和移除標籤。若要根據標籤控制存取，您可以在 IAM 政策的「條件」元素中使用與標籤相關的條件金鑰。

例如，如果資源的Owner標籤指定了使用者名稱，您可以建立一個政策，允許使用者完全存取所有 Amazon Security Lake 資源：

```
{
    "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 AWS 資源的存取。

將標籤新增至 Amazon 安全湖資源

若要將標籤新增至 Amazon 安全湖資源，您可以使用安全湖主控台或安全湖 API。

> **Important**
>
> 將標籤新增至資源可能會影響資源的存取。在將標籤新增至資源之前，請先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

當您為某個訂閱者啟用 Security Lake AWS 區域 或建立訂閱者時，Security Lake 主控台會提供新增標籤至資源的選項，也就是區域或訂閱者的資料湖組態。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，請依照下列步驟執行。

將標籤加入資源

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 根據您要新增標籤的資源類型，執行下列其中一個動作：
   - 對於資料湖組態，請在導覽窗格中選擇 [區域]。然後，在「區域」表中，選取「區域」。
   - 對于訂戶，請在導航窗格中選擇「訂戶」。然後，在「我的訂閱者」表格中，選取訂閱者。

如果訂閱者未出現在表格中，請使用頁面右上角的選取 AWS 區域 器來選取您建立訂閱者的地區。此表格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。此區段列出目前指定給資源的所有標籤。
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。字符可以是字母，數字，空格或以下符號：_。：/= +-@
7. 若要將其他標籤新增至資源，請選擇 [新增標籤]，然後重複上述步驟。您最多可以為資源指派 50 個標籤。
8. 完成新增標籤後，請選擇 [儲存]。

API

若要建立資源並以程式設計方式為其新增一或多個標籤，請針對您要建立的資源類型使用適當的`Create`作業：

- 資料湖配置 — 使用CreateDataLake作業，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，則執行create-data-lake命令。
- 訂閱者 — 使用CreateSubscriber作業，或者，如果您正在使用 AWS CLI，則執行建立訂閱者命令。

在您的請求中，使用`tags`參數來為每個要新增至資源的標籤指定標籤鍵 (`keyvalue`) 和可選標籤值 ()。該`tags`參數指定對象的數組。每個物件都會指定一個標籤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，請使用安全湖 API 的TagResource作業，或者，如果您使用的是 AWS CLI，請執行標籤資源命令。在您的請求中，指定要新增標籤的資源的 Amazon 資源名稱 (ARN)。使用`tags`參數可為要加入的每個標籤指定標籤鍵 (`keyvalue`) 和可選標籤值 ()。與`Create`操作和命令的情況一樣，該`tags`參數指定對象的數組，每個標籤鍵及其相關聯的標籤值一個對象。

例如，下列 AWS CLI 命令會將含有`Environment`標籤值的標籤索引鍵新增至指定的訂閱者。`Cloud`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戶的 ARN。
- *`Environment`*是要新增至訂閱者之標籤的標籤索引鍵。
- *`Cloud`*是指定標籤鍵的標籤值 (*`Environment`*)。

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，`key`和引`value`數都是必需的。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鍵建立關聯，請不要指定`value`引數的值。例如，下列命令會加入沒有關聯`Owner`標籤值的標籤鍵：

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

如果標記作業成功，安全湖會傳回空的 HTTP 200 回應。否則，安全湖會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

查看 Amazon 安全湖資源的標籤

您可以使用安全湖主控台或安全湖 API，檢閱 Amazon 安全湖資源的標籤 (標籤金鑰和標籤值)。

Console

請依照下列步驟，使用 Security Lake 主控台檢閱資源的標籤。

若要檢閱資源的標籤

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 根據您要檢閱其標籤的資源類型，執行下列其中一項作業：

   - 對於資料湖組態，請在導覽窗格中選擇 [區域]。在「區域」表格中，選取「區域」，然後選擇「編輯」。然後展開標籤部分。
   - 對于訂戶，請在導航窗格中選擇「訂戶」。然後，在「我的訂閱者」表格中，選擇訂閱者的名稱。

     如果訂閱者未出現在表格中，請使用頁面右上角的選取 AWS 區域 器來選取您建立訂閱者的地區。此表格僅列出目前區域的現有訂閱者。

「標籤」區段會列出目前指定給資源的所有標籤。

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作業。在您的請求中，使用`resourceArn`參數來指定資源的 Amazon 資源名稱 (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
```

在前面的例子中，*ARN#AW#########-1#123456789012####/1234 ## -34AB-56EF-12345*67890ab 是一個現有的用戶的 ARN。

如果操作成功，安全湖返回一個`tags`數組。陣列中的每個物件都會指定目前指派給資源的標籤 (標籤鍵和標籤值)。例如：

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
```

```
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

其中EnvironmentCostCenter、和Owner是指派給資源的標籤鍵。 Cloud是與標籤鍵相關聯的標Environment籤值。 12345是與標籤鍵相關聯的標CostCenter籤值。標Owner籤鍵沒有關聯的標籤值。

編輯 Amazon 安全湖資源的標籤

若要編輯 Amazon 安全湖資源的標籤 (標記金鑰或標籤值)，您可以使用安全湖主控台或安全湖 API。

> **Important**
>
> 編輯資源的標籤可能會影響資源的存取。在編輯資源的標籤金鑰或值之前，請先檢閱任何可能使用標籤來控制資源存取權的 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。

若要編輯資源的標籤

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 根據您要編輯其標籤的資源類型，執行下列其中一項作業：
   - 對於資料湖組態，請在導覽窗格中選擇 [區域]。然後，在「區域」表中，選取「區域」。
   - 對于訂戶，請在導航窗格中選擇「訂戶」。然後，在「我的訂閱者」表格中，選取訂閱者。

     如果訂閱者未出現在表格中，請使用頁面右上角的選取 AWS 區域 器來選取您建立訂閱者的地區。此表格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。「標籤」區段會列出目前指定給資源的所有標籤。

5. 執行下列任何一項：

   - 若要將標籤值加入至現有的標籤關鍵字，請在標籤關鍵字旁的「值」方塊中輸入值。
   - 若要變更現有的標籤關鍵字，請選擇標籤旁邊的「移除」。然後選擇「新增標籤」。在出現的「關鍵字」方塊中，輸入新的標籤關鍵字。選擇性地在「值」方塊中輸入關聯的標籤值。
   - 若要變更現有標籤值，請在包含該值的「值」方塊中選擇「X」。然後在「值」方塊中輸入新標籤值。
   - 若要移除現有的標籤值，請在包含該值的「值」方塊中選擇「X」。
   - 若要移除現有標籤 (包括標籤鍵值和標籤值)，請選擇標籤旁邊的「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。字符可以是字母，數字，空格或以下符號：_。：/= +-@

6. 編輯完標籤後，請選擇 [儲存]。

API

當您以程式設計方式編輯資源的標籤時，您可以使用新值覆寫現有標籤。因此，編輯標籤的最佳方式取決於您要編輯標籤關鍵字、標籤值還是兩者。若要編輯標籤關鍵字，請移除目前的標籤並新增標籤。

若只要編輯或移除與標籤金鑰相關聯的標籤值，請使用 Security Lake API 的TagResource作業覆寫現有值。如果您使用的是 AWS Command Line Interface (AWS CLI)，請運行標籤資源命令。在您的請求中，指定您要編輯或移除其標籤值的資源的 Amazon 資源名稱 (ARN)。

若要編輯標籤值，請使用`tags`參數來指定要變更其標籤值的標籤鍵。同時指定鍵的新標籤值。例如，下列 AWS CLI 命令會`Cloud`將指派給指定訂閱者之`Environment`標籤索引鍵的標籤值從變更`On-Premises`為。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`指定訂戶的 ARN。

- *Environment*是與要變更的標籤值相關聯的標籤鍵。
- *On-Premises*是指定標籤鍵的新標籤值 (*Environment*)。

若要從標籤鍵移除標籤值，請勿為參數中索value引鍵的引tags數指定值。例如：

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

如果作業成功，安全湖會傳回空的 HTTP 200 回應。否則，安全湖會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

從 Amazon 安全湖資源中刪除標籤

若要從 Amazon 安全湖資源移除標籤，您可以使用安全湖主控台或安全湖 API。

> **Important**
>
> 從資源中移除標籤可能會影響對資源的存取。移除標籤之前，請先檢閱任何可能使用標籤控制資源存取權的 AWS Identity and Access Management (IAM) 政策。

Console

請依照下列步驟，使用 Security Lake 主控台移除資源中的一或多個標籤。

若要從資源中移除標籤

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 根據您要從中移除標籤的資源類型，執行下列其中一個動作：
   - 對於資料湖組態，請在導覽窗格中選擇 [區域]。然後，在「區域」表中，選取「區域」。
   - 對于訂戶，請在導航窗格中選擇「訂戶」。然後，在「我的訂閱者」表格中，選取訂閱者。

     如果訂閱者未出現在表格中，請使用頁面右上角的選取 AWS 區域 器來選取您建立訂閱者的地區。此表格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。「標籤」區段會列出目前指定給資源的所有標籤。
5. 執行下列任何一項：
   - 若只要移除標籤的標籤值，請在包含要移除的值的「值」方塊中選擇「X」。
   - 若要同時移除標籤的標籤鍵和標籤值 (以配對形式)，請選擇要移除的標籤旁邊的「移除」。
6. 若要從資源中移除其他標籤，請針對每個要移除的其他標籤重複上述步驟。
7. 完成移除標籤後，請選擇 [儲存]。

API

若要以程式設計方式從資源中移除一或多個標籤，請使用 Security Lake API 的UntagResource作業。在您的請求中，使用`resourceArn`參數指定要從中移除標籤的資源的 Amazon 資源名稱 (ARN)。使用`tagKeys`參數指定要移除之標籤的標籤鍵。若要移除多個標籤，請為每個要移除的標籤附加`tagKeys`參數和引數，並以 & 符號分隔，例如。`tagKeys=`*`key1`*`&tagKeys=`*`key2`*若只要從資源中移除特定標籤值 (而非標籤鍵)，請編輯標籤，而不要移除標籤。

如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 untag-resource 命令以從資源中移除一或多個標籤。對於`resource-arn`參數，請指定要從中移除標籤的資源 ARN。使用`tag-keys`參數指定要移除之標籤的標籤鍵。例如，下列命令會從指定的訂閱者移除標`Environment`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`指定要從中刪除標籤的用戶的 ARN，並且*`Environment`*是要刪除的標籤的標籤鍵。

要從資源中刪除多個標籤，請添加每個額外的標籤鍵作為`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
```

如果作業成功，安全湖會傳回空的 HTTP 200 回應。否則，安全湖會傳回 HTTP 4 xx 或 500 回應，指出作業失敗的原因。

疑難排解 Amazon 安全

如果您在使用安全性湖泊時遇到問題，請參閱下列主題。

疑難排解資料湖狀態

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 就無法啟用 AWS CloudTrail 管理事件的記錄收集。「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說明和建議的補救步驟。

若要以程式設計方式存取問題摘要，您可以使用安全湖 API 的ListDataLakeExceptions作業。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 (例如美國東部 (維吉尼亞北部) 區域，`us-east-1`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。如需區域代碼的清單，請參閱 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"
```

若要通知安全湖使用者有關問題或錯誤，請使用安全湖 API 的CreateDataLakeExceptionSubscription作業。使用者可以透過電子郵件收到通知、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。

例如，下列 AWS CLI 命令會透過 SMS 傳送，將安全湖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"
```

若要檢視有關例外訂閱的詳細資訊，您可以使用此GetDataLakeExceptionSubscription作業。若要更新例外訂閱，您可以使用此UpdateDataLakeExceptionSubscription作業。若要刪除例外訂閱並停止通知，您可以使用此DeleteDataLakeExceptionSubscription作業。

解決 Lake Formation 問題

使用下列資訊可協助您診斷並修正使用 Security Lake 和資 AWS Lake Formation 料庫或表格時可能會遇到的常見問題。如需更多 Lake Formation 疑難排解主題，請參閱AWS Lake Formation 開發人員指南的疑難排解一節。

找不到資料表

您可能會在嘗試建立訂閱者時收到這個錯誤訊息。

若要解決此錯誤，請確定您已在「地區」中新增來源。如果您在 Security Lake 服務處於預覽版本時新增來源，則必須在建立訂閱者之前再次新增來源。如需新增來源的詳細資訊，請參閱Amazon Security Lake ake ake ake ake ake ake ake 鍵。

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訊息。

若要解決此錯誤，請檢閱您的 Lake Formation 權限。呼叫 API 的 IAM 角色應具有安全湖資料庫的「建立」資料表權限。如需詳細資訊，請參閱使用 Lake Formation 主控台授與資料庫權限，以及AWS Lake Formation 開發人員指南中的具名資源方法。

語法錯誤：行 1:8：不允許從沒有列的關係中選擇 *

第一次在 Lake Formation 中查詢來源資料表時，您可能會收到此錯誤訊息。

若要解決錯誤，請在登入時`SELECT`授與您正在使用的 IAM 角色的權限 AWS 帳戶。有關如何授予權限的說明，請參閱《AWS Lake Formation 開發人員指南》中的使用 Lake Formation 控制台授予表格權限和具名資源方法。`SELECT`

安全湖未能將呼叫者的主要 ARN 添加到 Lake Formation 數據湖管理員。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 為記錄來源時，您可能會收到此錯誤。

若要解決錯誤，請依照下列步驟執行：

1. 開啟 Lake Formation 主控台，網址為 https://console.aws.amazon.com/lakeformation/。
2. 以系統管理使用者身分登入。

3. 在功能窗格的 [權限] 下，選擇 [系統管理角色和工作]。
4. 在 [資料湖管理員] 區段中，選擇 [選擇管理員]。
5. 清除標示為在 IAM 中找不到的主參與者，然後選擇 [儲存]。
6. 請再次嘗試安全湖作業。

安全湖 CreateSubscriber 與 Lake Formation 沒有創建一個新的 RAM 資源共享邀請被接受

如果您在安全湖建立 Lake Form 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 第 2 版和第 3 版跨帳戶共用會將多個跨帳戶權限授與對應至一個 AWS RAM 資源共用，藉此最佳化 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 與回應中的 ARN 相符。`CreateSubscriber`

Amazon Athena 的疑難排解

使用下列資訊可協助您診斷並修正使用 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 使用者指南中的 Athena 疑難排解一節。

查詢不會傳回資料湖中的新物件

即使 Security Lake 的 S3 儲存貯體包含這些物件，您的 Athena 查詢也可能不會傳回資料湖中的新物件。如果您已停用安全性湖泊，然後再次啟用，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物件。

若要解決錯誤，請依照下列步驟執行：

1. 請在以下位置開啟 AWS Lambda 主控台。 https://console.aws.amazon.com/lambda/
2. 從導覽列的區域選取器上，選擇已啟用安全湖泊但 Athena 查詢不會傳回結果的區域。
3. ********* [##]##### [SecurityLake_Glue_ ********* _ Lambda_ # ## > ###
4. 在組態索引標籤上，選擇觸發器。
5. 選取函數旁邊的選項，然後選擇「編輯」。
6. 選取啟動觸發器，然後選擇儲存。這會將函數狀態轉為「已啟用」。

無法存取 AWS Glue 表格

查詢存取訂閱者可能無法存取包含 Security Lake 資料的資料 AWS Glue 表。

首先，請確保您已按照中列出的步驟進行操作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，請依照下列步驟執行：

1. 請在以下位置開啟 AWS Glue 主控台。 https://console.aws.amazon.com/glue/
2. 在導覽窗格中，選擇 [資料目錄和目錄設定]。
3. 授予訂閱者以資源為基礎的策略存取 AWS Glue 表格的權限。如需有關建立以資源為基礎的政策的詳細資訊，請參閱AWS Glue 開發人員指南 AWS Glue中的資源型政策範例

排解 Organizations 問題

使用下列資訊可協助您診斷及修正使用 Security Lake 和時可能會遇到的常見問題 AWS Organizations。如需更多 Organizations 疑難排解主題，請參閱AWS Organizations 使用指南中的「疑難排解」一節。

呼叫 CreateDataLake 作業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系統管理員帳戶。

如果您刪除委派系統管理員帳戶所屬的組織，然後嘗試使用 Security Lake 主控台或 CreateDataLakeAPI 使用該帳戶來設定 Security Lake，則可能會收到此錯誤。

若要解決錯誤，請使用不同組織或獨立帳戶的委派管理員帳戶。

疑難排解 Amazon 安全湖身分和存取

使用下列資訊可協助您診斷和修正使用安全湖和 IAM 時可能會遇到的常見問題。

我沒有在安全湖執行動作的授權

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是提供您認證的人員。

當 `mateojackson` IAM 使用者嘗試使用主控台來檢視虛構*`subscriber`*但沒有虛構`SecurityLake:`*`GetSubscriber`*許可的詳細資料時，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 會要求管理員更新原則，以允許他使用SecurityLake:*GetSubscriber*動作存取*subscriber*資訊。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞至 Security Lake。

有些 AWS 服務 允許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 使用者marymajor嘗試使用主控台在 Security Lake 中執行動作時，就會發生下列範例錯誤。但是，該動作要求服務具備服務角色授與的許可。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 系統管理員。您的管理員提供您的登入憑證。

我想允許我以外的人存 AWS 帳戶 取我的安全湖資源

您可以建立一個角色，讓其他帳戶中的使用者或您的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：

- 若要瞭解安全性湖泊是否支援這些功能，請參閱Amazon 安全湖如何與 IAM 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源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第三方 AWS帳戶 擁有的存取權。
- 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)。

- 若要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 角色與資源型政策的差異。

如何確定安全湖定價

Amazon 安全湖定價以兩個維度為基礎：資料擷取和資料轉換。安全湖也與其他工作AWS 服務儲存和共用您的資料，而您可能會針對這些活動產生個別費用。

當您第一次開啟記錄收集時AWS 帳戶在任何AWS 區域安全湖支持，該帳戶將自動註冊安全湖的 15 天免費試用。在免費試用期間，您可能仍會向其他服務產生費用。

數據擷取

這些成本來自攝入量AWS CloudTrail日誌和其他AWS 服務日誌和事件 (Amazon Roule 53) 解析程式查詢日誌、事件。AWS Security Hub調查結果以及 Amazon VPC 流程日誌。

資料轉換

這些成本來自的體積AWS 服務安全湖正常化的日誌和事件開放網路安全架構架構架構 (OCSF)架構和轉換為阿帕奇鑲木地板格式。

相關服務的成本

以下是您可能會從其他產生的一些費用AWS 服務用於儲存和共用安全性資料湖中的資料：

- Amazon S3 — 這些成本來自於在 Security Lake 帳戶中維護 Amazon S3 儲存貯體、在該處存放資料，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 — 這些成本來自於建立用於訊息傳遞的 Amazon SQS 佇列。如需詳細資訊，請參閱Amazon SQS 定價。
- 亞馬遜 EventBridge — 這些成本來自亞馬遜 EventBridge 傳送物件通知至訂閱端點。如需詳細資訊，請參閱亞馬遜 EventBridge價錢。

訂閱者自行負責從 Security Lake 查詢資料並儲存查詢結果而產生的費用。

如需詳細資訊，請參閱安全湖定價。

檢閱安全湖使用情況和預估成本

該用法Amazon Security Lake 主控台的頁面可讓您檢閱目前的安全湖使用情況，以及 future 的使用情況和成本估算。如果您目前正在參與 15 天的免費試用期，試用期間的使用量可協助您估算免費試用期結束後使用 Security Lake 的費用。如需安全湖定價的概觀，請參閱如何確定安全湖定價。如需詳細資訊和費用範例，請參閱Amazon 安全湖定價。

在安全湖中，估計的使用成本以美元報告，並僅適用於當前AWS 區域。費用涵蓋組織中所有帳戶的安全湖使用情況，並包括轉換為開放網路安全架構架構 (OCSF) 和 Apache Parquet 格式。不過，預測成本不包含其他服務 (例如 Amazon Simple Storage Service (Amazon S3) 和 Amazon Simple Storage Service (Amazon S3) 和 Amazon Simple Storage Service (Amazon S3) 和AWS Glue。

在「」用法頁面上，您可以選擇要檢視使用情況和成本資料的期間。預設時段為最後 1 個行事曆日。您必須至少有 1 天的安全湖使用量，才能查看成本預測。

頁面頂端會顯示所有帳戶的預估成本。這是您當前預測的安全湖成本AWS 區域根據您在所選時間範圍內的實際使用情況，接下來的 30 個日曆日。實際使用量和預測成本會以非同步方式調用的所有帳戶。

在頁面的其餘部分，使用情況和成本資料分為兩個表格，如下所示：

- 按來源劃分的用量和成本— 這是依資料來源劃分的目前 Security Lake 使用量，以及根據所選時間範圍內的實際使用情況，接下來 30 個日曆天的預估使用情況和成本。實際使用量、預測使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，則會開啟分割面板，顯示哪些帳戶從該來源產生記錄檔和事件。對於每個帳戶，分割面板包含來自該來源的實際使用情況，以及預測的使用情況和成本。
- 按帳戶劃分的使用和費用— 這是按帳戶劃分的當前 Security Lake 使用情況，以及根據您在所選時間範圍內的實際使用情況，接下來的 30 個日曆天的估計使用情況和成本。如果您選取帳戶，則會開啟分割面板，其中顯示有助於該帳戶使用的來源。對於每個貢獻來源，分割面板包含實際使用情況和預測使用量和成本。

所有支援AWS即使您尚未在 Security Lake 中新增特定來源，資料來源也會顯示在上述資料表中。我們建議您將所有AWS來源（如果您參與免費試用版），以獲取全套日誌和事件的成本估算。有關添加的說明AWS來源，請參閱收集資料 AWS 服務。使用量或成本計算中不包含自訂來源。

請依照下列步驟在 Security Lake 主控台中檢閱您的使用情況和成本資料。

檢閱安全湖使用量和預測成本 (主控台)

1. 開啟安全湖主控台，位於：https://console.aws.amazon.com/securitylake/。
2. 通過使用AWS 區域選取頁面右上角的選取器，選取您要檢視其使用量和成本的區域。
3. 在導覽窗格中，選擇設定然後用法。
4. 選取您要檢視其使用情況和成本資料的期間。預設值為最後 1 天。
5. 請選取依資料來源或者按帳戶標籤，以詳細複查使用量與成本。

Amazon Security Lake Security Lake Security Lake

如需安全湖支援的區域和服務端點清單，請參閱中的 Amazon 安全湖端點AWS 一般參考。

建議您針對所有支援啟用 Security Lake 的 Security LakeAWS 區域。這可讓您使用 Security Lake 偵測並調查未經授權或不尋常的活動，即使在您未主動使用的區域也是如此。

禁用 Amazon 安全湖

停用 Amazon 安全湖時，安全湖停止從您的 AWS 來源收集日誌和事件。現有的安全性湖泊設定和在您的中建立的資源 AWS 帳戶 都會保留。此外，您儲存或發佈到其他 AWS 服務資料 (例如資料 AWS Lake Formation 表和 AWS CloudTrail 記錄檔中的機密資料) 仍可使用。根據您的 Amazon S3 儲存生命週期，存放在 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體中的資料仍可供使用。

從 Security Lake 主控台的 [設定] 頁面停用 Security Lake 會停止收集目前已啟用 Security Lake AWS 區域 的所有 AWS 記錄檔和事件。您可以使用主控台的 [區域] 頁面來停止特定區域的記錄收集。安全湖 API， AWS CLI 並停止您在請求中指定的區域中的日誌收集。

如果您使用與整合， AWS Organizations 且您的帳戶屬於集中管理多個 Security Lake 帳戶的組織，則只有委派的 Security Lake 系統管理員可以針對本身和成員帳戶停用 Security Lake。不過，離開組織會停止收集成員帳戶的記錄檔。

當您針對組織停用 Security Lake 時，如果您遵循此頁面上提供的停用指示，則會保留委派的管理員指定。您不需要再次指定委派的系統管理員，才能重新啟用 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。無法停用整合將導致來源整合繼續將日誌傳送到 Amazon S3。此外，您必須停用訂閱者整合，否則訂閱者仍然可以使用 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，請參閱個別提供者的說明文件。

本主題說明如何使用安全湖主控台、安全湖 API 或停用安全湖泊 AWS CLI。

Console

1. 開啟安全湖主控台，網址為 https://console.aws.amazon.com/securitylake/。
2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。
3. 選擇禁用安全湖。
4. 當系統提示您確認時，請輸入**`Disable`**，然後選擇 [停用]。

API

若要以程式設計方式停用安全湖泊，請使用安全湖 API 的DeleteDataLake作業。如果您使用的是 AWS CLI，請執行delete-date-lake命令。在您的要求中，使用`regions`清單來指定您要停用 Security Lake 之每個區域的地區代碼。如需區域代碼的清單，請參閱 AWS 一般參考.

對於使用的 Security Lake 部署 AWS Organizations，只有組織委派的 Security Lake 系統管理員可以針對組織中的帳戶停用 Security Lake。

例如，下列 AWS CLI 命令會停用`ap-northeast-1`和`eu-central-1`區域中的安全性湖泊。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 安全湖用戶指南的文檔歷史記錄

下表說明自上次發行 Amazon 安全湖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。

最新文件更新：2024 年 3 月 27 日

變更	描述	日期
更新至現有的受管理策略	Security Lake 已更新AmazonSecurityLake MetastoreManager原則，以新增中繼資料清理動作，可讓您刪除資料湖中的中繼資料。	2024年3月27日
新的來源版本	更新您的角色權限，以從新的資料來源版本擷取資料。	2024 年 2 月 29 日
新的 AWS 記錄檔來源	安全湖將 EKS 稽核記錄新增為記 AWS 錄來源。EKS 稽核記錄可協助您在 Amazon Elastic Kubernetes Service 中偵測 EKS 叢集中潛在的可疑活動。	2024 年 2 月 29 日
更新至現有的受管理策略	Security Lake 已更新原則以允許使`iam:PassRole` 用新`AmazonSecurityLake MetastoreManagerV2` 角色，並可讓 Security Lake 部署或更新資料湖元件。	2024年2月23 日
新的受管理策略	安全湖添加了一個新的AWS受管理策略，即`AmazonSecurityLakeMetastore Manager` 策略。此原則授與權限讓 Security Lake 管理資料湖中的中繼資料。	2024 年 1 月 23 日

區域可用性	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)。如需目前提供安全湖泊的完整區域清單，請參閱中的 Amazon 安全湖端點AWS 一般參考。	2023 年 10 月 26 日
新功能	您現在可以為具有查詢存取權的訂閱者編輯特定設定。您也可以為您的 AWS 帳戶.	2023 年 7 月 20 日
新的受管理策略	安全湖添加了一個新的AWS受管理策略，即AmazonSecurityLakeAdministrator 策略。此原則會授與允許主體完整存取所有 Security Lake 動作的管理權限。	2023 年 5 月 30 日
一般可用性	安全湖現已正式推出。	2023 年 5 月 30 日
新功能	安全湖現在將指標發送到 Amazon CloudWatch。	2023 年 5 月 4 日
區域可用性	Security Lake 現已在以下地區提供 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	當您使用安全湖主控台啟用並開始使用安全湖時，Security Lake 現在會代表您建立 AWS Identity and Access Management (IAM) 角色。	2023 年 2 月 15 日
初始版本	這是 Amazon 安全湖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。