使用者指南

AWS CloudTrail

版本 1.0

AWS CloudTrail: 使用者指南

Table of Contents

什麼是 AWS CloudTrail？

AWS CloudTrail AWS 服務 是可協助您啟用您的 AWS 帳戶. 使用者、角色或 AWS 服務所執行的動作會記錄為中的事件 CloudTrail。事件包括在 AWS Management Console、 AWS Command Line Interface和 AWS SDK 和 API 中採取的動作。

CloudTrail 在您創建它 AWS 帳戶 時處於活動狀態。當您的活動發生時 AWS 帳戶，該活動會記錄在 CloudTrail 事件中。

CloudTrail 提供三種記錄事件的方法：

- 事件歷史記錄 – 事件歷史記錄提供過去 90 天發生的 AWS 區域管理事件的可檢視、可搜尋、可下載而且不可變的記錄。您可以透過篩選單個屬性搜尋事件。創建帳戶時，您將自動獲得事件歷史記錄的存取權。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。

  查看活動歷史記錄不 CloudTrail 收取任何費用。

- CloudTrail Lake — AWS CloudTrail Lake 是一個受管理的資料湖，用於擷取、儲存、存取和分析上的使用者和 API 活動，以 AWS 供稽核和安全用途。 CloudTrail 湖將基於行的 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。如果您選擇一年可延長保留定價選項，則可將事件資料保留在事件資料存放區中最多 3,653 天 (約 10 年)；如果您選擇七年保留定價選項，則最多可保留 2,557 天 (約 7 年)。您可以使用為單一 AWS 帳戶 或多個事件資料倉庫建立事件 AWS 帳戶 資料倉庫 AWS Organizations。您可以將 S3 儲存貯體中的任何現有 CloudTrail 日誌匯入現有或新的事件資料存放區。您還可以使用 Lake 儀表板將熱門 CloudTrail 事件趨勢視覺化。如需詳細資訊，請參閱 工作, 由于, AWS CloudTrail 湖。

  CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。在 Lake 中執行查詢時，您需要依據掃描的資料量付費。如需有關 CloudTrail 定價和管理 Lake 成本的資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

- 追蹤 — 追蹤可擷取 AWS 活動記錄，在 Amazon S3 儲存貯體中交付和存放這些事件，並可選擇交付到CloudWatch 日誌和 Amazon EventBridge。您可以輸入這些事件到您的安全監控解決方案。您也可以使用自己的第三方解決方案或解決方案 (例如 Amazon Athena) 來搜尋和分析 CloudTrail 日誌。您可以使用建立單一 AWS 帳戶 或多個 AWS 帳戶 系統線 AWS Organizations。您可以記錄 Insights 事件，以 API 呼叫量和錯誤率分析您的管理事件是否存在異常行為。如需詳細資訊，請參閱為您的建立追蹤 AWS 帳戶。

您可以透 CloudTrail 過建立追蹤，免費將一份正在進行的管理事件副本傳遞到 S3 儲存貯體，但是 Amazon S3 儲存會產生費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

可見度您的 AWS 帳戶活動是安全性和營運最佳實踐的關鍵方面。您可以用 CloudTrail 來檢視、搜尋、下載、封存、分析和回應 AWS 基礎結構中的帳戶活動。您可以識別誰或採取了哪些動作、採取了哪些資源處理、事件發生時間，以及其他詳細資料，以協助您分析和回應 AWS 帳戶中的活動。

您可以使用 API 整合 CloudTrail 到應用程式中、為組織自動建立追蹤或事件資料存放區、檢查您建立的事件資料存放區和追蹤的狀態，以及控制使用者檢視 CloudTrail 事件的方式。

存取 CloudTrail

您可以使用下 CloudTrail 列任何一種方式使用。

主題

- CloudTrail 控制台
- AWS CLI
- CloudTrail API
- AWS 開發套件

CloudTrail 控制台

請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。

CloudTrail 控制台提供用於執行許多 CloudTrail 任務的用戶界面，例如：

- 查看您 AWS 帳戶的最近事件和事件歷史記錄。
- 從事件歷史記錄下載過去 90 天管理事件的過濾或完整文件。
- 建立和編輯 CloudTrail 系統線。
- 建立和編輯 CloudTrail Lake 事件資料存放區。
- 對事件資料存放區執行查詢。
- 設定 CloudTrail 追蹤，包括：
  - 為追蹤選取 Amazon S3 儲存貯體。

- 設定前綴。
- 設定傳送至 CloudWatch 記錄檔。
- 使用密 AWS KMS 鑰對跟踪數據進行加密。
- 啟用在追蹤的日誌檔案交付之後的 Amazon SNS 通知。
- 為您的追蹤新增和管理標籤。

- 設定 CloudTrail Lake 事件資料存放區，包括：
  - 將事件資料存放區與合 CloudTrail 作夥伴或您自己的應用程式整合，以記錄來自外部來源的事件 AWS。
  - 聯合事件資料存放區，以便從 Amazon Athena 執行查詢。
  - 使用 AWS KMS 金鑰加密事件資料存放區資料。
  - 為您的事件資料存放區新增和管理標籤。

如需有關的更多資訊 AWS Management Console，請參閱AWS Management Console。

AWS CLI

這 AWS Command Line Interface 是一個統一的工具，您可以使用它 CloudTrail 來從命令行進行交互。如需詳細資訊，請參閱 AWS Command Line Interface 使用者指南。如需 CloudTrail CLI 命令的完整清單，請參閱《命令參考》中的 cloudtrail 和雲路資料。AWS CLI

CloudTrail API

除了控制台和 CLI 之外，您還可以使用 CloudTrail RESTful API CloudTrail 直接進行編程。如需詳細資訊，請參閱 AWS CloudTrail API 參考資料和 CloudTrail-Data API 參考資料。

AWS 開發套件

作為使用 CloudTrail API 的替代方法，您可以使用其中一個 AWS SDK。每種開發套件皆包含多種程式設計語言與平台的程式庫與範本程式碼。SDK 提供了一種方便的方式來創建程序化訪問. CloudTrail 例如，您可以使用開發套件以密碼編譯方式來簽署請求、管理錯誤，以及自動重試請求。如需詳細資訊，請參閱要建置的工具 AWS頁面。

如何 CloudTrail 工作

您可以 CloudTrail 在建立您的 AWS 帳戶. 事件歷史記錄提供過去 90 天發生的已記錄 AWS 區域管理事件的可檢視、可搜尋、可下載而且不可變的記錄。

如需過 AWS 帳戶 去 90 天內持續的事件記錄，請建立追蹤或 CloudTrail Lake 事件資料存放區。

主題

CloudTrail 事件歷史

您可以前往 [事件歷史記錄] 頁面，在 CloudTrail 主控台中輕鬆檢視過去 90 天的管理事件。您還可以透過執行 aws cloudtrail lookup-events 命令或 `LookupEvents` API 操作檢視事件歷史記錄。您可以篩選單一屬性上的事件，以搜尋事件歷史記錄中的事件。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。

事件歷史記錄不會連接到存在於帳戶中的任何追蹤或事件資料存放區，因此您對追蹤和事件資料存放區所做的組態變更不會對其產生影響。

檢視 [事件歷史記錄] 頁面或執行`lookup-events`命令無 CloudTrail 須付費。

CloudTrail 湖泊和事件資料倉庫

您可以建立事件資料存放區來記錄CloudTrail 事件 (管理事件、資料事件)、CloudTrailInsights 事件、AWS Audit Manager 證據、AWS Config 設定項目或外部的事件 AWS。

事件資料存放區可以記錄目前事件 AWS 區域，或從您 AWS 帳戶 AWS 區域 中記錄所有事件。用於從外部記錄整合事件的事件資料存放區 AWS 必須僅適用於單一區域；它們不能是多區域事件資料存放區。

如果您已在中建立組織 AWS Organizations，則可以建立一個組織事件資料存放區，以記錄該組織中所有 AWS 帳戶的所有事件。組織事件資料存放區可套用至所有 AWS 區域或目前的區域。組織事件資料存放區必須透過使用管理帳戶或委派的管理員帳戶建立，且在獲指定套用到組織時，將會自動套用到組織中的所有成員帳戶。成員帳戶無法查看組織事件資料存放區，也無法進行修改或刪除。組織事件資料存放區無法用於從外部收集事件 AWS。如需詳細資訊，請參閱 組織事件資料存放區。

依預設，事件資料存放區中的所有事件均由加密 CloudTrail。設定事件資料存放區時，您可以選擇使用自己的資料存放區 AWS KMS key。使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將

事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。如需詳細資訊，請參閱 使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)。

下表提供您可以在事件資料存放區上執行之工作的相關資訊。

任務	描述
檢視湖泊儀表板	您可以使用 CloudTrail Lake 儀表板，以視覺化方式呈現事件資料存放區中收集管理事件、S3 資料事件或 Insights 事件的事件。
記錄檔管理事件	將您的事件資料存放區設定為記錄唯讀、唯寫或所有管理事件。依預設，事件資料會儲存記錄管理事件。
記錄資料事件	設定事件資料存放區以記錄資料事件。您可以使用進階事件選取器篩選`eventName` 、和`resources.ARN` 欄位`readOnly`，以僅記錄感興趣的事件。
日誌見解事件	將事件資料存放區設定為記錄 Insights 事件，以協助您識別和回應與管理 API 呼叫相關的異常活動。如需詳細資訊，請參閱 記錄 Insights 事件。 Insights 事件會產生額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。
複製追蹤事件	您可以將追蹤事件複製到新的或現有的事件資料存放區，以建立記錄至追蹤的事件 point-in-time 快照。
在事件資料存放區上啟用聯合	您可以聯合事件資料存放區，以在資料目錄中查看與事件資料存放區相關聯的中繼 AWS Glue 資料，並使用 Amazon Athena 對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。
停止或啟動事件資料存放區的事件擷取	您可以在收集 CloudTrail 管理和資料事件或 AWS Config 設定項目的事件資料存放區上停止和啟動事件擷取。
建立與事件來源以外的整合 AWS	您可以使用 CloudTrail Lake 整合功能，從混合式環境中的 AWS 任何來源記錄和儲存使用者活動資料，例如內部部署或雲端中託

任務	描述
	管的 SaaS 應用程式、虛擬機器或容器。如需可用整合合作夥伴的資訊，請參閱 AWS CloudTrail Lake 整合。
在 CloudTrail 主控台中檢視 Lake 範例查詢	主 CloudTrail 控台提供許多範例查詢，可協助您開始撰寫自己的查詢。
建立或編輯查詢	中的查詢 CloudTrail 是以 SQL 編寫的。您可以從頭開始以 SQL 撰寫查詢，或開啟已儲存或範例查詢並進行編輯，在 CloudTrail Lake Editor 索引標籤上建立查詢。
將查詢結果儲存至 S3 儲存貯體	執行查詢時，您可以將查詢結果儲存至 S3 儲存貯體。
下載儲存的查詢結果	您可以下載包含已儲存的 CloudTrail Lake 查詢結果的 CSV 檔案。
驗證儲存的查詢結果	您可以使用 CloudTrail 查詢結果完整性驗證來判斷查詢結果 CloudTrail 傳遞至 S3 儲存貯體後，查詢結果是否已修改、刪除或未變更。

如需 CloudTrail Lake 的更多資訊，請參閱〈〉工作, 由于, AWS CloudTrail 湖。

CloudTrail Lake 事件資料存放區和查詢會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。在 Lake 中執行查詢時，您需要依據掃描的資料量付費。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

CloudTrail 小徑

追蹤是一種組態，能讓事件交付到您指定的 Amazon S3 儲存貯體。您還可以使用 Amazon CloudWatch 日誌和 Amazon 在跟踪中交付和分析事件 EventBridge。

追蹤可以記錄 CloudTrail 管理事件、資料事件和見解事件。

您可以為一個建立兩種類型的系統線 AWS 帳戶：多區域系統線和單一區域系統線。

多區域步道

當您建立多區域追蹤時，會將事件 CloudTrail 記錄在您正 AWS 區域 在使用的AWS 分割區中的所有事件，並將 CloudTrail 事件日誌檔案傳送到您指定的 S3 儲存貯體。如果 AWS 區域 在您建立多區域追蹤後新增，則會自動包含該新區域，並記錄該區域中的事件。由於您要擷取帳戶所有區域內的活動，因此建立多區域追蹤是建議的最佳實務。您使用 CloudTrail 主控台建立的所有路徑都是多區域。您可以使用將單一區域系統軌跡轉換為多區域系統線。 AWS CLI如需詳細資訊，請參閱 在主控台中建立追蹤 及 將套用至一個區域的追蹤轉換成套用至所有區域。

單一區域步道

當您建立單一區域追蹤時，只會 CloudTrail 記錄該區域中的事件。然後，它會將 CloudTrail 事件日誌檔傳送到您指定的 Amazon S3 儲存貯體。您只能使用 AWS CLI建立單一區域追蹤。如果您建立額外的單一追蹤，您可以讓這些追蹤將 CloudTrail 事件日誌檔傳遞至相同的 S3 儲存貯體或個別儲存貯體。當您使用 AWS CLI 或 CloudTrail API 建立追蹤時，這是預設選項。如需詳細資訊，請參閱 建立、更新和管理追蹤 AWS CLI。

> **Note**
>
> 對於這兩種類型的追蹤，您可以指定來自任何區域的 Amazon S3 儲存貯體。

如果您已在中建立組織 AWS Organizations，則可以建立組織追蹤記錄該組織中所有 AWS 帳戶的所有事件。組織追蹤可套用至所有「區 AWS 域」或目前的「區域」。組織追蹤必須透過管理帳戶或委派的管理員帳戶建立，且在獲指定套用到組織時，將會自動套用到組織中的所有成員帳戶。成員帳戶可以看到組織軌跡，但無法修改或刪除它。在預設情況下，成員帳戶無法存取 Amazon S3 儲存貯體中組織追蹤的日誌檔案。

根據預設，當您在 CloudTrail 主控台中建立追蹤時，您的事件記錄檔會使用 KMS 金鑰加密。如果您選擇不啟用 SSE-KMS 加密，您的事件日誌會使用 Amazon S3 伺服器端加密 (SSE) 加密。您可以將日誌檔案存放在 儲存貯體中，沒有時間限制。您也可以定義 Amazon S3 生命週期規則以自動封存或刪除日誌檔案。如果您要日誌檔案交付和驗證的通知，可以設定 Amazon SNS 通知。

CloudTrail 每小時多次發佈記錄檔，大約每 5 分鐘一次。這些記錄檔包含來自支援帳戶中服務的 API 呼叫 CloudTrail。如需詳細資訊，請參閱 CloudTrail 支援的服務與整合。

> **Note**
>
> CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內提供記錄檔。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
> 如果您錯誤設定追蹤 (例如，無法連線 S3 儲存貯體)， CloudTrail將嘗試將日誌檔重新傳送到 S3 儲存貯體 30 天，而且這些 attempted-to-deliver 事件將收取標準費用。 CloudTrail 若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。
> CloudTrail 捕獲用戶直接或 AWS 服務代表用戶進行的操作。例如， AWS CloudFormation `CreateStack`呼叫可能會根據範 AWS CloudFormation 本的要求，對 Amazon EC2、Amazon RDS、Amazon EBS 或其他服務進行額外的 API 呼叫。這是正常且預期的行為。您可以識別動作是否由 CloudTrail事件中具有`invokedby`欄位的 AWS 服務採取。

下表提供您可在追蹤記錄上執行之工作的相關資訊。

任務	描述
記錄管理事件	將追蹤設定為記錄唯讀、唯寫或所有管理事件。
記錄資料事件	您可以使用進階事件選取器來建立精細的選取器，以僅記錄感興趣的資料事件。使用進階事件選取器時，您可以篩選`eventName` 欄位以包含或排除特定 API 呼叫的記錄，這有助於控制成本。
日誌見解事件	將追蹤設定為記錄 Insights 事件，以協助您識別和回應與 管理 API 呼叫相關的異常活動。 Insights 事件會產生額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。
查看見解事件	在追蹤上啟用 CloudTrail 深入解析之後，您可以使用主 CloudTrail 控台或 AWS CLI.
下載洞察活動	在追蹤上啟用 CloudTrail 深入解析後，您可以下載 CSV 或 JSON 檔案，其中包含最多 90 天的追蹤見解事件。

任務	描述
將路徑活動複製到 CloudTrail 湖泊	您可以將現有追蹤事件複製到 CloudTrail Lake 事件資料存放區，以建立記錄至追蹤的事件 point-in-time 快照。
建立並訂閱 Amazon SNS 主題	訂閱主題以接收交付到您儲存貯體之日誌檔案的相關通知。Amazon SNS 可透過多種方式來通知您，包括以 Amazon Simple Queue Service 透過編寫程式的方式。 **Note** 如果您想要收到從所有區域傳遞之日誌檔案的相關 SNS 通知，請為您的追蹤指定唯一的 SNS 主題。如果您想要透過編寫程式的方式處理所有事件，請參閱「使用 CloudTrail 處理程式庫」。
檢視您的記錄檔	從 S3 儲存貯體尋找並下載您的日誌檔。
使用 CloudWatch 記錄監控事件	您可以將追蹤設定為將事件傳送至 CloudWatch 記錄檔。然後，您可以使用 CloudWatch Logs 來監控您的帳戶是否有特定的 API 呼叫和事件。 **Note** 如果您將套用至所有區域的追蹤設定為將事件傳送至 CloudWatch 記錄日誌群組，則會將所有區域的事件 CloudTrail 傳送至單一記錄群組。
啟用記錄檔加密	日誌檔案加密為您的日誌檔案多加一層安全性防護。
啟用記錄檔完整性	記錄檔完整性驗證可協助您確認記錄檔自 CloudTrail 傳送以來是否保持不變。

任務	描述
與其他人共用記錄檔 AWS 帳戶	您可以在帳戶之間共享日誌檔案。
彙總來自多個帳戶的記錄	您可以將多個帳戶的日誌檔案彙整至單一儲存貯體。
使用夥伴解決方案	使用整合的合作夥伴解決方案分析您的 CloudTrail 輸出 CloudTrail。合作夥伴解決方案提供一組廣泛的功能，例如變更追蹤、故障診斷和安全分析。

您可以透 CloudTrail 過建立追蹤，免費將一份正在進行的管理事件副本傳遞到 S3 儲存貯體，但是 Amazon S3 儲存會產生費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail 洞察活動

AWS CloudTrail 透過持續分析 CloudTrail 管理事件，深入解析可協助 AWS 使用者識別並回應與 API 呼叫和 API 錯誤率相關的異常活動。 CloudTrail Insights 會分析您的 API 呼叫量和 API 錯誤率 (也稱為基準) 的正常模式，並在呼叫量或錯誤率超出正常模式時產生 Insights 事件。其會針對 `write` 管理 API 產生 API 呼叫量的 Insights 事件，並針對 `read` 和 `write` 管理 API 產生 API 錯誤率的 Insights 事件。

根據預設， CloudTrail 追蹤和事件資料存放區不會記錄見解事件。您必須設定追蹤或事件資料存放區，才能記錄 Insights 事件。如需詳細資訊，請參閱 記錄見解事件 AWS Management Console 及 記錄見解事件 AWS Command Line Interface。

Insights 事件會產生額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

檢視追蹤和事件資料存放區的見解事件

CloudTrail 同時支援追蹤和事件資料存放區的 Insights 事件，不過，您檢視和存取 Insights 事件的方式有所不同。

檢視追蹤的 Insights 事件

如果您在追蹤上啟用了 Insights 事件，並 CloudTrail 偵測到異常活動，Insights 事件會記錄到目的地 S3 儲存貯體中的其他資料夾或前置詞，以供追蹤使用。您也可以在 CloudTrail 主控台上檢視 Insights

事件時，查看見解的類型和事件期間。如需詳細資訊，請參閱 在 CloudTrail 主控台中檢視追蹤的 CloudTrail 深入解析事件。

在追蹤上首次啟用「 CloudTrail 深入解析」之後，如果偵測到異常活動，最多可能需 CloudTrail 要 36 小時才能傳遞第一個「見解」事件。

檢視事件資料存放區的 Insights 事件

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要記錄 Insights 事件的目標事件資料存放區，以及啟用見解和記錄管理事件的來源事件資料存放區。如需詳細資訊，請參閱 使用主控台為 CloudTrail Insights 事件建立事件資料存放區。

在來源事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能將第一個 Insights 事件傳送至目的地事件資料存放區。

如果您在來源事件資料存放區上啟用了 CloudTrail Insights 並 CloudTrail 偵測到異常活動，則會將 Insights 事件 CloudTrail 傳送至目的地事件資料存放區。然後，您可以查詢目的地事件資料存放區以取得 Insights 事件的相關資訊，並可選擇性地將查詢結果儲存至 S3 儲存貯體。如需詳細資訊，請參閱 建立或編輯查詢 及 在 CloudTrail 主控台中檢視範例查詢。

您可以檢視「見解事件」儀表板，以視覺化方式呈現目標事件資料存放區中的見解事件。如需有關 Lake 儀表板的詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

CloudTrail 渠道

CloudTrail 支援兩種類型的通道：

CloudTrail Lake 與外部事件來源整合的管道 AWS

> CloudTrail Lake 使用頻道將活動從外部與外部合作夥伴合作 CloudTrail，或從您自己的來源帶 AWS 入 CloudTrail Lake。建立通道時，您可以選擇一或多個事件資料存放區，以儲存從通道來源到達的事件。只要目的地事件資料存放區設定為記錄活動事件，您就可以視需要變更通道的目的地事件資料存放區。當您為來自外部合作夥伴的事件建立通道時，您會將通道 ARN 提供給合作夥伴或來源應用程式。連接至通道的資源政策允許來源透過通道傳輸事件。如需詳細資訊，請參閱建立與事件來源以外的整合 AWS和 AWS CloudTrail API 參考中的 `CreateChannel`。

服務連結通道

> AWS 服務可以建立與服務連結的頻道，以代表您接收 CloudTrail 事件。建立 AWS 服務連結通道的服務會針對頻道設定進階事件選取器，並指定該頻道是套用至所有區域，還是目前的區域。

您可以使用CloudTrail 控制台或AWS CLI查看有關由 AWS 服務創建的任何 CloudTrail 服務鏈接渠道的信息。

CloudTrail 概念

本節總結了與之相關的基本概念 CloudTrail。

概念：

- CloudTrail 事件
- 事件歷史記錄
- 線索
- 組織軌跡
- CloudTrail 湖泊和事件資料倉庫
- CloudTrail 洞察
- 標籤
- AWS Security Token Service 和 CloudTrail
- 全球服務事件

CloudTrail 事件

中的事件 CloudTrail 是 AWS 帳戶中活動的記錄。此活動可以是 IAM 身分或可監控的服務所 CloudTrail採取的動作。 CloudTrail事件提供透過 AWS Management Console、 AWS SDK、命令列工具和其他 AWS 服務進行的 API 和非 API 帳戶活動的歷史記錄。

CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此事件不會以任何特定順序顯示。

CloudTrail 記錄三種類型的事件：

- 管理事件
- 資料事件
- 洞察活動

所有事件類型都使用 CloudTrail JSON 記錄格式。

依預設，追蹤和事件資料存放區會記錄管理事件，但不會記錄資料或 Insights 事件。

如需與之 AWS 服務 整合的相關資訊 CloudTrail，請參閱AWS 的服務主題 CloudTrail。

管理事件

管理事件提供有關對您 AWS 帳戶中資源執行之管理作業的相關資訊。這些也稱為控制平面操作。

範例管理事件包含：

- 設定安全性 (例如 AWS Identity and Access Management `AttachRolePolicy` API 作業)。
- 註冊裝置 (例如，Amazon EC2 `CreateDefaultVpc` API 操作)。
- 設定規則以路由資料 (例如，Amazon EC2 `CreateSubnet` API 操作)。
- 設定記錄 (例如 AWS CloudTrail `CreateTrail` API 作業)。

管理事件也可以包含您帳戶中發生的非 API 事件。例如，當使用者登入您的帳戶時，會 CloudTrail 記錄`ConsoleLogin`事件。如需詳細資訊，請參閱 擷取的非 API 事件 CloudTrail。

依預設， CloudTrail 追蹤和 CloudTrail Lake 事件資料會儲存記錄管理事件。如需記錄管理事件的詳細資訊，請參閱記錄管理事件。

資料事件

資料事件提供在資源上執行或於資源中執行之資源操作的相關資訊。這些也稱為資料平面操作。資料事件通常是大量資料的活動。

範例資料事件包含：

- S3 儲存貯體中物件上的 Amazon S3 物件層級 `PutObject` API 活動 (例如`DeleteObject`，和 API 操作)。`GetObject`
- AWS Lambda 函數執行活動（ `Invoke`API ）。
- CloudTrail `PutAuditEvents`CloudTrail Lake 頻道上的活動，用於從外部記錄事件 AWS。
- 主題上的 Amazon SNS `Publish` 和 `PublishBatch` API 操作。

下表顯示可用於追蹤和事件資料存放區的資料事件類型。資料事件類型 (主控台) 欄顯示主控台中的適當選取項目。resource .type 值欄會顯示您要指定以使用或 API 將該類型的資料事件納入追蹤或事件資料存放區中的`resources.type` AWS CLI 值。 CloudTrail

對於追蹤，您可以使用基本或進階事件選取器來記錄 Amazon S3 物件、Lambda 函數和 DynamoDB 表格的資料事件 (顯示在表格的前三列中)。您只能使用進階事件選取器來記錄剩餘列中顯示的資料事件類型。

對於事件資料存放區，您只能使用進階事件選取器來包含資料事件。

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon DynamoDB	資料表上的 Amazon DynamoDB 項目層級 API 活動 (例如PutItemDeleteItem 、和 UpdateItem API 操作)。 **Note** 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table 。如果您指定 AWS::DynamoDB::Table 作為 resources.type ，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB	DynamoDB	AWS::DynamoDB::Table

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	串流事件。若要排除串流事件，請在eventName 欄位上新增篩選器。		
AWS Lambda	AWS Lambda 函數執行活動（InvokeAPI）。	Lambda	AWS::Lambda::Function
Amazon S3	S3 儲存貯體中物件上的 Amazon S3 物件層級 PutObject API 活動 (例如DeleteObject ，和 API 操作)。GetObject	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 設定作業的 API 活動，例如呼叫StartConfiguration Session 和GetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration
AWS 數據交換	用於轉換器作業的 B2B 資料交換 API 活動，例如呼叫 GetTransformerJob 和 StartTransformerJob 。	B2B 資料交換	AWS::B2BI::Transformer

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon Bedrock	代理程式別名上的 Amazon Bedrock API 活動。	Bedrock 代理程式別名	`AWS::Bedrock::AgentAlias`
	知識庫中的 Amazon Bedrock API 活動。	Bedrock 知識庫	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront 上的 API 活動 KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map 命名空間上的 API 活動。	AWS Cloud Map 命名空間	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map 服務上的 API 活動。	AWS Cloud Map 服務	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` CloudTrail Lake 頻道上的活動，用於從外部記錄事件 AWS。	CloudTrail 渠道	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	在自定義 Amazon CodeWhisperer API 活動。	CodeWhisperer 定制	`AWS::CodeWhisperer::Customization`
	設定檔上的 Amazon CodeWhisperer API 活動。	CodeWhisperer	`AWS::CodeWhisperer::Profile`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon Cognito	Amazon Cognito 身分集區上的 Amazon Cognito API 活動。	Cognito 身分池	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	串流上的 Amazon DynamoDB API 活動。	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) direct API，例如 Amazon EBS 快照上的 `PutSnapshotBlock` 、`GetSnapshotBlock` ，以及 `ListChangedBlocks` 。	Amazon EBS direct API	`AWS::EC2::Snapshot`
Amazon EMR	預寫日誌工作區上的 Amazon EMR API 活動。	EMR 預寫日誌工作區	`AWS::EMRWAL::Workspace`
Amazon FinSpace	環境上的 Amazon FinSpace API 活動。	FinSpace	`AWS::FinSpace::Environment`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
AWS Glue	AWS Glue 由 Lake Formation 創建的表上的 API 活動。 **Note** AWS Glue 目前僅在下列區域支援資料表的資料事件： • 美國東部 (維吉尼亞北部) • 美國東部 (俄亥俄) • 美國西部 (奧勒岡) • 歐洲 (愛爾蘭) • 亞太 (東京) 區域	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	檢測器的 Amazon GuardDuty API 活動。	GuardDuty 探測器	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging 資料存放區上的 API 活動。	醫學影像資料存放區	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT 憑證上的 API 活動。	IoT 證書	`AWS::IoT::Certificate`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	AWS IoT 事物上的 API 活動。	IoT 的事	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	來自組件版本的 Greengrass 核心設備的 API 活動。 Note Greengrass 不會記錄訪問被拒絕的事件。	IoT Greengrass 件版本	`AWS::GreengrassV2::ComponentVersion`
	部署上來自 Greengrass 核心裝置的 API 活動。 Note Greengrass 不會記錄訪問被拒絕的事件。	IoT 環境部署	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	資產上的 IoT SiteWise API 活動。	IoT SiteWise 資產	`AWS::IoTSiteWise::Asset`
	時間序列上的 IoT SiteWise API 活動。	IoT SiteWise 時間序列	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	實體上的 IoT TwinMaker API 活動。	IoT TwinMaker 實體	`AWS::IoTTwinMaker::Entity`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	工作區上的 IoT TwinMaker API 活動。	IoT TwinMaker 工作區	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	重新評分執行計畫上的 Amazon Kendra Intelligent Ranking API 活動。	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (適用於 Apache Cassandra)	表上的 Amazon Keyspaces API 活動。	卡桑德拉表	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	串流上的 Kinesis Data Streams 流 API 活動。	Kinesis 流	`AWS::Kinesis::Stream`
	串流取用者的室運動資料串流 API 活動。	Kinesis 流消費者	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	Kinesis Video Streams 片串流上的 API 活動，例如呼叫`GetMedia`和`PutMedi`	Kinesis 視訊串流	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	網路上的 Amazon Managed Blockchain API 活動。	Managed Blockchain 網路	`AWS::ManagedBlockchain::Network`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Ethereum 節點上的 Amazon Managed Blockchain JSON-RPC 呼叫，例如 `eth_getBalance` 或 `eth_getBlockByNumber` 。	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Neptune 圖形	Neptune 圖形上的資料 API 活動，例如查詢、演算法或向量搜尋。	Neptune 圖形	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA 作用中目錄 API 活動的連接器。	AWS Private CA 作用中目錄的連接器	`AWS::PCAConnectorAD::Connector`
Amazon Q 應用	Amazon Q 應用程式上的資料 API 活動。	Amazon Q 應用	`AWS::QApps:QApp`
Amazon Q Business	應用程式上的 Amazon Q Business API 活動。	Amazon Q Business 應用程式	`AWS::QBusiness::Application`
	資料來源上的 Amazon Q Business API 活動。	Amazon Q Business 資料來源	`AWS::QBusiness::DataSource`
	索引上的 Amazon Q Business API 活動。	Amazon Q Business 索引	`AWS::QBusiness::Index`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Web 體驗上的 Amazon Q Business API 活動。	Amazon Q Business Web 體驗	`AWS::QBusiness::WebExperience`
Amazon RDS	資料庫叢集上的 Amazon RDS API 活動。	RDS 數據 API-數據庫集群	`AWS::RDS::DBCluster`
Amazon S3	存取點上的 Amazon S3 API 活動。	S3 存取點	`AWS::S3::AccessPoint`
	Amazon S3 物件 Lambda 存取點 API 活動，例如呼叫`CompleteMultipartUpload` 和`GetObject`。	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Outposts 上 Amazon S3 物件層級的 API 活動。	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	端點上的 Amazon SageMaker `InvokeEndpointWithResponseStream` 活動。	SageMaker 端點	`AWS::SageMaker::Endpoint`
	功能商店上的 Amazon SageMaker API 活動。	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	實驗試用元件上的 Amazon SageMaker API 活動。	SageMaker 度量實驗試驗元件	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	平台端點上的 Amazon SNS `Publish` API 操作。	SNS 平台端點	`AWS::SNS::PlatformEndpoint`
	主題上的 Amazon SNS `Publish` 和 `PublishBatch` API 操作。	SNS 主題	`AWS::SNS::Topic`
Amazon SQS	訊息上的 Amazon SQS API 活動。	SQS	`AWS::SQS::Queue`
AWS Step Functions	Step Functions 狀態機上的 API 活動。	Step Functions 狀態機器	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain 執行個體上的 API 活動。	供應鏈	`AWS::SCN::Instance`
Amazon SWF	網域上的 Amazon SWF API 活動。	SWF 網域名稱	`AWS::SWF::Domain`
AWS Systems Manager	控制通道上的 Systems Manager API 活動。	Systems Manager	`AWS::SSMMessages::ControlChannel`
	受管節點上的系統管理員 API 活動。	系統管理員管理節點	`AWS::SSM::ManagedNode`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon Timestream	資料庫上的 Amazon Timestream Query API 活動。	Timestream 資料庫	AWS::Timestream::Database
	資料庫上的 Amazon Timestream Query API 活動。	Timestream 資料表	AWS::Timestream::Table
Amazon Verified Permissions	政策存放區上的 Amazon Verified Permissions API 活動。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces 瘦客戶端	WorkSpaces 裝置上的精簡型用戶端 API 活動。	精簡型客戶端裝置	AWS::ThinClient::Device
	WorkSpaces 環境上的精簡型用戶端 API 活動。	精簡型客戶端環境	AWS::ThinClient::Environment
AWS X-Ray	軌跡上的 X-Ray API 活動。	X-Ray 軌跡	AWS::XRay::Trace

依預設，在您建立追蹤或事件資料存放區時，不會記錄資料事件。若要記錄資 CloudTrail 料事件，您必須明確新增要收集活動的支援資源或資源類型。如需有關記錄資料事件的詳細資訊，請參閱 記錄資料事件。

記錄資料事件需支付額外的費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

洞察活動

CloudTrail 洞察事件會透過分析 CloudTrail 管理活動，擷取您 AWS 帳戶中異常的 API 呼叫率或錯誤率活動。Insights 事件會提供相關資訊，例如關聯的 API、錯誤代碼、事件時間及統計資料，以協助您了解並針對異常活動採取行動。與 CloudTrail 追蹤或事件資料存放區中擷取的其他類型事件不

同，Insights 事件只有在 CloudTrail 偵測到帳戶 API 使用情況或錯誤率記錄的變更時，才會記錄與帳戶的一般使用模式明顯不同。

可能產生 Insights 事件的活動範例包括：

- 您的帳戶通常每分鐘記錄不超過 20 個 Amazon S3 `DeleteBucket` API 呼叫，但是您的帳戶開始記錄到每分鐘平均 100 個 `DeleteBucket` API 呼叫。異常活動開始時會記錄 Insights 事件，並記錄另一個 Insights 事件以標示異常的活動結束。
- 您的帳戶通常每分鐘記錄 20 個 Amazon EC2 `AuthorizeSecurityGroupIngress` API 呼叫，但您的帳戶開始記錄到零個 `AuthorizeSecurityGroupIngress` 呼叫。異常活動開始時會記錄 Insights 事件，並在十分鐘後，當異常活動結束時，記錄另一個 Insights 事件以標示異常的活動結束。
- 您的帳戶於 7 天內在 AWS Identity and Access Management API 上記錄通常少於一個的 `AccessDeniedException` 錯誤，`DeleteInstanceProfile`。您的帳戶開始在 `DeleteInstanceProfile` API 呼叫中記錄每分鐘 12 個 `AccessDeniedException` 錯誤的平均值。異常錯誤率活動開始時會記錄 Insights 事件，並記錄另一個 Insights 事件以標示異常活動的結束。

這些範例僅供說明之用。您的結果可能會根據您的使用案例而有所不同。

若要記錄 CloudTrail Insights 事件，您必須在新的或現有的追蹤或事件資料存放區上明確啟用 Insights 事件。如需有關記錄 Insights 事件的詳細資訊，請參閱 記錄 Insights 事件。

Insights 事件會產生額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

檢視追蹤和事件資料存放區的見解事件

CloudTrail 同時支援追蹤和事件資料存放區的 Insights 事件，不過，您檢視和存取 Insights 事件的方式有所不同。

檢視追蹤的 Insights 事件

如果您在追蹤上啟用了 Insights 事件，並 CloudTrail 偵測到異常活動，Insights 事件會記錄到目的地 S3 儲存貯體中的其他資料夾或前置詞，以供追蹤使用。您也可以在 CloudTrail 主控台上檢視 Insights 事件時，查看見解的類型和事件期間。如需詳細資訊，請參閱 在 CloudTrail 主控台中檢視追蹤的 CloudTrail 深入解析事件。

檢視事件資料存放區的 Insights 事件

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要記錄 Insights 事件的目標事件資料存放區，以及啟用見解和記錄管理事件的來源事件資料存放區。如需詳細資訊，請參閱 使用主控台為 CloudTrail Insights 事件建立事件資料存放區。

如果您在來源事件資料存放區上啟用了 CloudTrail Insights 並 CloudTrail 偵測到異常活動，則會將 Insights 事件 CloudTrail 傳送至目的地事件資料存放區。然後，您可以查詢目的地事件資料存放區以取得 Insights 事件的相關資訊，並可選擇性地將查詢結果儲存至 S3 儲存貯體。如需詳細資訊，請參閱 建立或編輯查詢 及 在 CloudTrail 主控台中檢視範例查詢。

您可以檢視「見解事件」儀表板，以視覺化方式呈現目標事件資料存放區中的見解事件。如需詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

事件歷史記錄

CloudTrail 事件歷史記錄提供了過去 90 天的 CloudTrail 管理事件的可查看，可搜索，可下載和不可變的記錄。 AWS 區域您可以使用此歷史記錄來查看在 AWS 帳戶中執行的操作 AWS Management Console， AWS SDK，命令行工具和其他 AWS 服務。您可以在 CloudTrail 主控台中自訂事件歷史記錄的檢視，方法是選取要顯示的欄。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。

線索

追蹤是允許將 CloudTrail 事件交付到 S3 儲存貯體的組態，並可選擇將事件交付到CloudWatch 日誌和 Amazon EventBridge。您可以使用追蹤選擇要傳遞的 CloudTrail 事件、使用 AWS KMS 金鑰加密 CloudTrail 事件日誌檔，以及設定 Amazon SNS 通知以進行日誌檔交付。如需建立及管理追蹤的詳細資訊，請參閱為您的建立追蹤 AWS 帳戶。

多區域和單一區域路徑

您可以為一個建立兩種類型的系統線 AWS 帳戶：多區域系統線和單一區域系統線。

多區域步道

> 當您建立多區域追蹤時，會將事件 CloudTrail 記錄在您正 AWS 區域 在使用的AWS 分割區中的所有事件，並將 CloudTrail 事件日誌檔案傳送到您指定的 S3 儲存貯體。如果 AWS 區域 在您建立多區域追蹤後新增，則會自動包含該新區域，並記錄該區域中的事件。由於您要擷取帳戶所有區域內的活動，因此建立多區域追蹤是建議的最佳實務。您使用 CloudTrail 主控台建立的所有路徑都是多區域。您可以使用將單一區域系統軌跡轉換為多區域系統線。 AWS CLI如需詳細資訊，請參閱 在主控台中建立追蹤 及 將套用至一個區域的追蹤轉換成套用至所有區域。

單一區域步道

當您建立單一區域追蹤時，只會 CloudTrail 記錄該區域中的事件。然後，它會將 CloudTrail 事件日誌檔傳送到您指定的 Amazon S3 儲存貯體。您只能使用 AWS CLI建立單一區域追蹤。如果您建立額外的單一追蹤，您可以讓這些追蹤將 CloudTrail 事件日誌檔傳遞至相同的 S3 儲存貯體或個別儲存貯體。當您使用 AWS CLI 或 CloudTrail API 建立追蹤時，這是預設選項。如需詳細資訊，請參閱 建立、更新和管理追蹤 AWS CLI。

> **Note**
>
> 對於這兩種類型的追蹤，您可以指定來自任何區域的 Amazon S3 儲存貯體。

多區域追蹤具有以下優點：

- 追蹤的組態設定會一致地套用至所有項目 AWS 區域。
- 您可以在單一 Amazon S3 儲存貯體 AWS 區域 中接收所有 CloudTrail 事件，並選擇性地在 CloudWatch 日誌日誌群組中接收事件。
- 您可以 AWS 區域 從一個位置管理所有人的追蹤組態。

當您將追蹤套用至所有區 AWS 域時， CloudTrail 會使用您在特定「區域」中建立的追蹤，在您正在使用的AWS 分割區中的所有其他區域中，建立具有相同組態的追蹤。

如此會帶來下列效果：

- CloudTrail 將帳戶活動的日誌檔從所有 AWS 區域傳遞到您指定的單一 Amazon S3 儲存貯體，並選擇性地傳送至 CloudWatch 日誌日誌群組。
- 如果您為追蹤設定 Amazon SNS 主題，則所有 AWS 區域中日誌檔交付的 SNS 通知都會傳送至該單一 SNS 主題。

無論追蹤是多區域還是單一區域，傳送至 Amazon 的事件 EventBridge 都會在每個區域的事件匯流排中接收，而不是在單一事件匯流排中接收。

每個區域的多個追蹤

如果您有不同但相關的使用者群組 (例如開發人員、安全人員和 IT 稽核員)，則可以為每個區域建立多個追蹤。這可讓每個群組收到各自的日誌檔案副本。

CloudTrail 每個區域支援五個追蹤。多區域追蹤計為每個區域的一個追蹤。

以下是具有五條軌跡的「區域」範例：

- 您在美國西部 (加利佛尼亞北部) 區域中建立只套用至此區域的兩個追蹤。
- 您可以在美國西部 (加利佛尼亞北部) 區域建立兩個多區域追蹤。
- 您在亞太區域 (雪梨) 區域建立另一個多區域路線。此追蹤在美國西部 (加利佛尼亞北部) 區域中也以追蹤形式存在。

您可以在 CloudTrail 主控台的 [追蹤] 頁面 AWS 區域 中檢視追蹤清單。如需詳細資訊，請參閱 更新追蹤。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

組織軌跡

組織追蹤是一種組態，可將管理帳戶中的 CloudTrail 事件和 AWS Organizations 組織中的所有成員帳戶交付到相同的 Amazon S3 儲存貯體、 CloudWatch 日誌和 Amazon EventBridge。建立組織追蹤，有助於您為組織定義一個統一的事件記錄策略。

使用主控台建立的所有組織追蹤都是多區域組織追蹤，可記錄組織 AWS 區域 中每個成員帳戶中已啟用的事件。若要記錄組織中所有 AWS 分割區中的事件，請在每個分割區中建立多區域組織追蹤。您可以使用建立單一區域或多區域組織追蹤。 AWS CLI如果您建立單一區域追蹤，則只會在追蹤記錄 AWS 區域 (也稱為「本地區」) 中記錄活動。

雖然大 AWS 區域 多數預設為啟用 AWS 帳戶，但您必須手動啟用某些區域 (也稱為選擇加入區域)。如需預設啟用哪些區域的相關資訊，請參閱《AWS Account Management 參考指南》中的啟用和停用區域之前的考量事項。如需 CloudTrail支援的區域清單，請參閱CloudTrail 支援的地區。

當您建立組織軌跡時，系統會在屬於您組織的成員帳戶中建立一份具有您指定名稱之追蹤檔的複本。

- 如果組織追蹤是針對單一區域，且追蹤檔的本位目錄「區域」不是「選擇區域」，則會在每個成員帳戶的組織軌跡的本位目錄「區域」中建立追蹤副本。
- 如果組織追蹤檔是針對單一區域，且追蹤檔的本位目錄「區域」是「選擇區域」，則會在已啟用該「區域」的成員帳戶中，在組織軌跡的本位目錄「區域」中建立軌跡副本。
- 如果組織追蹤為「多區域」，且追蹤的主「區域」不是選擇加入「區域」，則會在每個成員帳戶 AWS 區域 中啟用的每個追蹤建立副本。當成員帳戶啟用選擇加入區域時，會在該區域啟動完成後，在該成員帳戶的新選擇中為該成員帳戶建立多區域追蹤的副本。
- 如果組織追蹤為「多區域」，且主「區域」是選擇加入的「區域」，則除非成員帳戶選擇加入建立多區域追蹤的 AWS 區域 位置，否則不會將活動傳送至組織追蹤。例如，如果您建立多區域追蹤，並

選擇「歐洲 (西班牙) 區域」作為軌跡的本位目錄區域，則只有為其帳戶啟用「歐洲 (西班牙) 區域」的成員帳戶才會將其帳戶作業傳送至組織追蹤檔。

> **Note**
>
> CloudTrail 即使資源驗證失敗，仍會在成員帳號中建立組織追蹤。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 存儲桶政策
> - 不正確的 Amazon SNS 主題政策
> - 無法傳遞至 CloudWatch 記錄檔記錄群組
> - 使用 KMS 金鑰加密權限不足
>
> 具有 CloudTrail 權限的成員帳戶可以在 CloudTrail 主控台上檢視追蹤的詳細資料頁面或執行 AWS CLI get-trail-status命令，來查看組織追蹤的任何驗證失敗。

在成員帳戶中具有 CloudTrail 權限的使用者將能夠看到組織追蹤 (包括追蹤 ARN)，當他們從其 AWS 帳戶登入 AWS CloudTrail 主控台時，或執行 AWS CLI 命令 `describe-trails` (雖然成員帳戶必須使用 ARN 作為組織追蹤，而不是使用名稱時)。 AWS CLI不過，成員帳戶中的使用者將沒有足夠的權限來刪除組織追蹤、開啟或關閉記錄、變更記錄的事件類型，或以任何方式變更組織追蹤。如需使用 AWS Organizations的詳細資訊，請參閱 Organizations 術語與概念。如需建立與使用組織追蹤的詳細資訊，請參閱建立組織追蹤。

CloudTrail 湖泊和事件資料倉庫

CloudTrail Lake 可讓您針對事件執行精細的 SQL 查詢，並記錄來自外部來源的事件，包括來自您自己的應用程式 AWS，以及與之整合的合作夥伴的事件。 CloudTrail您不需要在帳戶中設定追蹤即可使用 CloudTrail Lake。

系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。如果您選擇一年可延長保留定價選項，則可將事件資料保留在事件資料存放區中最多 3,653 天 (約 10 年)；如果您選擇七年保留定價選項，則最多可保留 2,557 天 (約 7 年)。您可以儲存 Lake 查詢以供將來使用，並可查看最多七天的查詢結果。您也可以將查詢結果儲存至 S3 儲存貯體。 CloudTrail Lake 也可以將組織的事件儲存 AWS Organizations 在事件資料存放區中，或將來自多個區域和帳戶的事件儲存。 CloudTrail Lake 是稽核解決方案的一部分，可協助您執行安全性調查和疑難排解。如需詳細資訊，請參閱 工作, 由于, AWS CloudTrail 湖 及 CloudTrail 湖泊概念和術語。

CloudTrail 洞察

CloudTrail 透過持續分析 CloudTrail 管理事件，深入解析可協助 AWS 使用者識別和回應異常大量的 API 呼叫或記錄在 API 呼叫中的錯誤。Insights 事件是 `write` 管理 API 活動之異常層級或針對管理 API 活動傳回之異常層級錯誤的記錄。根據預設，追蹤和事件資料存放區不會記錄 CloudTrail 見解事件。在主控台中，您可以在建立或更新追蹤或事件資料存放區時選擇記錄 Insights 事件。使用 CloudTrail API 時，您可以使用 `PutInsightSelectors`API 編輯現有追蹤或事件資料存放區的設定來記錄 Insights 事件。記錄 CloudTrail 見解事件需支付額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 記錄 Insights 事件 和 AWS CloudTrail 定價。

標籤

標籤是客戶定義的金鑰和選用值，可指派給 AWS 資源，例如 CloudTrail 追蹤、事件資料存放區和通道、用於存放 CloudTrail 日誌檔的 S3 儲存貯體、組 AWS Organizations 織和組織單位等等。透過將相同的標籤新增至追蹤和用於存放追蹤記錄的日誌檔的 S3 儲存貯體，您可以更輕鬆地使用這些資源來管理、搜尋和篩選這些資源AWS Resource Groups。您可以實作標記策略以協助您持續、有效、輕鬆地尋找和管理您的資源。如需詳細資訊，請參閱標記 AWS 資源的最佳做法。

AWS Security Token Service 和 CloudTrail

AWS Security Token Service (AWS STS) 是具有全域端點且也支援區域特定端點的服務。端點指的是用做 Web 服務請求之進入點的 URL。例如，`https://cloudtrail.us-west-2.amazonaws.com`是 AWS CloudTrail 服務的美國西部 (奧勒岡) 區域進入點。區域端點將有助於降低應用程式的延遲。

當您使用區 AWS STS 域特定端點時，該區域中的追蹤只會傳遞該區域中發生的 AWS STS 事件。例如，如果您要使用端點 `sts.us-west-2.amazonaws.com`，則 us-west-2 中的追蹤只會交付源自 us-west-2 的 AWS STS 事件。如需區 AWS STS 域端點的詳細資訊，請參閱 IAM 使用者指南AWS STS 中的在 AWS 區域中啟用和停用。

如需AWS 地 AWS 區端點的完整清單，請參閱 AWS 一般參考. 如需全域 AWS STS 端點之事件的詳細資訊，請參閱 全球服務事件。

全球服務事件

> **Important**
>
> 截至 2021 年 11 月 22 日，AWS CloudTrail 改變了追蹤捕捉全球服務事件的方式。現在，由 Amazon 建立的事件 CloudFront AWS Identity and Access Management，並記錄 AWS STS 在其建立的區域中，美國東部 (維吉尼亞北部) 區域 us-east-1。這使得這 CloudTrail 些服務如何與其他 AWS 全球服務一致。若要繼續接收美國東部 (維吉尼亞北部) 以外的全域服務事件，請務必將使用美國東部 (維吉尼亞北部) 以外全域服務事件的單一區域追蹤轉換為多區域追蹤。如需擷取全球服務事件的詳細資訊，請參閱本節下文的「啟用及停用全球服務事件記錄」。相反，CloudTrail 控制台中的事件歷史記錄和aws cloudtrail lookup-events命令將顯示這些事件發生的 AWS 區域 位置。

對於大多數服務，事件會記錄在動作所發生的區域。對於全球服務 AWS Identity and Access Management (IAM) 和 Amazon AWS STS CloudFront，事件會傳遞至包含全球服務的任何追蹤。

對於大部分的全域服務，事件會記錄在事件發生的美國東部 (維吉尼亞北部) 區域中，但部分全域服務事件會記錄在事件發生的其他區域中，例如美國東部 (俄亥俄) 區域或美國西部 (奧勒岡) 區域。

為了避免收到重複的全球服務事件，請記住下列項目：

- 全域服務事件預設會傳遞給使用 CloudTrail 主控台建立的追蹤。事件會交付至追蹤的儲存貯體。
- 如果您有多個單一區域追蹤，請考慮設定追蹤，使之只會傳遞一個追蹤的全域服務事件。如需詳細資訊，請參閱 啟用及停用全球服務事件記錄。
- 如果您將追蹤的組態從記錄所有區域變更為記錄單一區域，則會自動關閉該追蹤的全域服務事件記錄。同樣地，如果您將追蹤的組態從記錄單一區域變更為記錄所有區域，則會自動開啟該追蹤的全域服務事件記錄。

  如需變更追蹤之全球服務事件記錄日誌的詳細資訊，請參閱 啟用及停用全球服務事件記錄。

範例：

1. 您可以在 CloudTrail 主控台中建立追蹤。根據預設，此追蹤會記錄全球服務事件。
2. 您有多個單一區域追蹤。
3. 您不需要在單一區域追蹤中包含全域服務。會交付第一個追蹤的全球服務事件。如需詳細資訊，請參閱 建立、更新和管理追蹤 AWS CLI。

> **Note**
>
> 使用 AWS CLI、 AWS SDK 或 CloudTrail API 建立或更新追蹤時，您可以指定是否包含或排除追蹤的全域服務事件。您無法從主控台設定全域服務事件記 CloudTrail 錄。

CloudTrail 支援的地區

> **Note**
>
> 如需 CloudTrail 湖泊支援區域的相關資訊，請參閱CloudTrail 湖泊支持的地區。
> 如需有關資料平面端點的資訊，請參閱中的資料平面端點AWS 一般參考。

區域名稱	區域	控制平面端點	通訊協定	支援日期
美國東部 (維吉尼亞北部)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	11/13/2013
美國東部 (俄亥俄)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	2016/10/17
美國西部 (加利佛尼亞北部)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	2014/05/13
美國西部 (奧勒岡)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	11/13/2013
非洲 (開普敦)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	04/22/2020
亞太區域 (香港)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	2019/04/24
亞太區域 (海德拉巴)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	11/22/2022

區域名稱	區域	控制平面端點	通訊協定	支援日期
亞太區域 (雅加達)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	12/13/2021
亞太區域 (墨爾本)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	01/23/2023
亞太區域 (孟買)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	2016/06/27
亞太區域 (大阪)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	2018/02/12
亞太區域 (首爾)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	2016/01/06
亞太區域 (新加坡)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	2014/06/30
亞太區域 (悉尼)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	2014/05/13
亞太區域 (東京)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	2014/06/30
加拿大 (中部)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	2016/12/08
加拿大西部 (卡加利)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	12/20/2023
中國 (北京)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	2014/03/01
中國 (寧夏)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	2017/12/11
歐洲 (法蘭克福)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	2014/10/23

區域名稱	區域	控制平面端點	通訊協定	支援日期
歐洲 (愛爾蘭)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	2014/05/13
歐洲 (倫敦)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	2016/12/13
歐洲 (米蘭)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	2020/04/27
歐洲 (巴黎)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	2017/12/18
歐洲 (西班牙)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	11/16/2022
歐洲 (斯德哥爾摩)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	2018/12/11
歐洲 (蘇黎世)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
以色列 (特拉維夫)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	07/31/2023
中東 (巴林)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	2019/07/29
中東 (阿拉伯聯合大公國)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	2022 年 8 月 30 日
南美洲 (聖保羅)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	2014/06/30
AWS GovCloud (美國東部)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	2018/11/12

區域名稱	區域	控制平面端點	通訊協定	支援日期
AWS GovCloud (美國西部)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	2011/08/16

如需有關使用 CloudTrail 的詳細資訊 AWS GovCloud (US) Regions，請參閱使AWS GovCloud (US) 用指南中的服務端點。

如需有關 CloudTrail 在中國 (北京) 區域使用的詳細資訊，請參閱AWS 中國的端點和 ARN。Amazon Web Services 一般參考

CloudTrail 支援的服務與整合

CloudTrail 支持許多日誌記錄事件 AWS 服務。您可以在每個受支援之服務的指南中找到該服務的詳細資訊。如需服務特定主題的清單，請參閱AWS 的服務主題 CloudTrail。此外，有些 AWS 服務 可用於分析記 CloudTrail 錄中收集的資料並採取行動。

> **Note**
>
> 若要查看各項服務的支援區域清單，請參閱 Amazon Web Services 一般參考 中的服務端點與配額。

主題

- AWS 與 CloudTrail 日誌的服務整合
- CloudTrail 與 Amazon 集成 EventBridge
- CloudTrail 與整合 AWS Organizations
- AWS 的服務主題 CloudTrail
- CloudTrail 不支援服務

AWS 與 CloudTrail 日誌的服務整合

> **Note**
>
> 您也可以使用 CloudTrail Lake 查詢和分析您的事件。 CloudTrail 與事件歷史記錄或運`LookupEvents`行中的簡單鍵和值查詢相比，Lake 查詢提供了更深入且更可自定義的事件視圖。 CloudTrail Lake 使用者可以在 CloudTrail 事件中的多個欄位執行複雜的標準查詢語言 (SQL) 查詢。如需詳細資訊，請參閱 工作, 由于, AWS CloudTrail 湖 及 將路徑活動複製到 CloudTrail湖。
> CloudTrail Lake 事件資料存放區和查詢會產生 CloudTrail 費用。如需 CloudTrail Lake 定價的詳細資訊，請參閱AWS CloudTrail 定價。

您可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列主題。

AWS 服務	主題	描述
Amazon Athena	查詢 AWS CloudTrail 記錄檔	搭配 CloudTrail 日誌使用 Athena 是強化 AWS 服務活動分析的強大方法。例如，您可以使用查詢來識別趨勢，並依屬性 (例如來源 IP 地址或使用者) 進一步隔離活動。 您可以直接從 CloudTrail 主控台自動建立用於查詢記錄的資料表，並使用這些資料表在 Athena 中執行查詢。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的 CloudTrail主控台中的為 CloudTrail 日誌建立表格。 **Note** 在 Amazon Athena 中執行查詢會產生額外

AWS 服務	主題	描述
		的成本。如需詳細資訊，請參閱 Amazon Athena 定價。
Amazon CloudWatch 日誌	使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔	您可以 CloudTrail 使用 CloudWatch 日誌進行配置，以監控跟踪日誌並在特定活動發生時收到通知。例如，您可以定義「 CloudWatch 記錄」指標篩選器，這些篩選器會觸發 CloudWatch 警示，並在觸發警示時傳送通知給您。 **Note** Amazon CloudWatch 和 Amazon CloudWatch 日誌適用標準定價。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

CloudTrail 與 Amazon 集成 EventBridge

Amazon EventBridge 是一項 AWS 服務，可提供描述 AWS 資源變更的近乎即時的系統事件串流。在中 EventBridge，您可以建立規則來回應由記錄的事件 CloudTrail。如需詳細資訊，請參閱在 Amazon 中建立規則 EventBridge。

您可以透 EventBridge 過使用 EventBridge 主控台建立規則，在追蹤上傳送已訂閱的事件。

從 EventBridge 控制台：

- 選擇使用的`AWS API Call via CloudTrail`詳細 CloudTrail 資料類型來傳送資料和管理事件。`eventType` `AwsApiCall`若要記錄詳細資料類型值的事件`AWS API Call via CloudTrail`，您必須擁有目前記錄管理或資料事件的追蹤。

- 選擇AWS Console Sign In via CloudTrail詳細資料類型以傳送AWS Management Console登入事件。若要記錄具有詳細資料類型的事件AWS Console Sign In via CloudTrail，您必須擁有目前正在記錄管理事件的追蹤。
- 選擇AWS Insight via CloudTrail詳細資料類型以提供見解事件。若要記錄詳細資料類型值的事件AWS Insight via CloudTrail，您必須擁有目前正在記錄 Insights 事件的追蹤。如需有關記錄 Insights 事件的詳細資訊，請參閱 記錄 Insights 事件。

如需有關如何建立追蹤的詳細資訊，請參閱 建立追蹤。

CloudTrail 與整合 AWS Organizations

AWS Organizations 組織的管理帳戶可以新增委派管理員來管理組織的 CloudTrail 資源。如有組織會為 AWS Organizations中某組織的所有 AWS 帳戶收集各種事件資料，您可以在該組織的管理帳戶或委派的管理員帳戶中建立組織追蹤或組織事件資料存放區。建立組織追蹤，有助於您為組織定義一個統一的事件記錄策略。

組織追蹤會自動套用至組織中的每個 AWS 帳戶。在成員帳戶中的使用者可以查看這些追蹤，但無法修改它們，而且根據預設，無法查看為組織追蹤建立的日誌檔案。如需詳細資訊，請參閱 建立組織追蹤。

AWS 的服務主題 CloudTrail

您可以深入了解如何將個別 AWS 服務的事件記錄在 CloudTrail 記錄檔中，包括該服務的範例事件在記錄檔中。如需有關特定 AWS 服務如何整合的詳細資訊 CloudTrail，請參閱該服務的個別指南中有關整合的主題。

仍處於預覽狀態，或尚未針對正式上市 (GA) 而發行，或沒有公用 API 的服務均不被視為受支援。CloudTrail 目前不會記錄 Amazon VPC 端點原則特定事件。

> **Note**
>
> 若要查看各項服務的支援區域清單，請參閱 Amazon Web Services 一般參考 中的服務端點與配額。
> 如需有關哪些服務記錄資料事件的資訊，請參閱 資料事件。

AWS 服務	CloudTrail 主題	支援開始時間
Amazon API Gateway	將 API 管理呼叫記錄到 Amazon API Gateway 使用 AWS CloudTrail	2015/07/09
Amazon AppFlow	使用記錄 Amazon AppFlow API 呼叫 AWS CloudTrail	04/22/2020
Amazon AppStream 2.0	使用日誌記錄 Amazon AppStream 2.0 API 調用 AWS CloudTrail	2019/04/25
Amazon Athena	使用記錄 Amazon Athena API 呼叫 AWS CloudTrail	2017/05/19
Amazon Aurora	監控 Amazon Aurora API 呼叫 AWS CloudTrail	2018 年 8 月 31 日
Amazon Bedrock	使用記錄 Amazon 基岩 API 呼叫 AWS CloudTrail	10/23/2023
Amazon Braket	Amazon Braket 日誌記錄與 CloudTrail	08/12/2020
Amazon Chime	使用日誌 Amazon Chime 管理呼叫 AWS CloudTrail	2017/09/27
Amazon 雲端目錄	使用記錄 Cloud Directory API 呼叫 AWS CloudTrail	2017/01/26
Amazon CloudFront	用 AWS CloudTrail 來擷取傳送至 CloudFront API 的要求	2014/05/28
Amazon CloudSearch	使用記錄 Amazon CloudSearch 組態服務呼叫 AWS CloudTrail	2014/10/16

AWS 服務	CloudTrail 主題	支援開始時間
Amazon CloudWatch	記錄 Amazon CloudWatch API 呼叫 AWS CloudTrail	2014/04/30
Amazon CloudWatch 日誌	記錄 Amazon CloudWatch 日誌 API 調用 AWS CloudTrail	2016/03/10
Amazon CodeCatalyst	AWS 帳戶 使用連線記錄 CodeCatalyst API 呼叫 AWS CloudTrail	2022 年 12 月 1 日
Amazon 評論 CodeGuru 家	使用記錄 Amazon CodeGuru 審核者 API 呼叫 AWS CloudTrail	12/02/2019
Amazon CodeWhisperer	AWS CloudTrail 和 CodeWhisperer API	04/13/2023
Amazon Cognito	使用記錄 Amazon Cognito API 呼叫 AWS CloudTrail	2016/02/18
Amazon Comprehend	使用日誌記錄 Amazon Comprehend API 調用 AWS CloudTrail	01/17/2018
Amazon Comprehend Medical	使用 AWS CloudTrail記錄 Amazon Comprehend Medical API 呼叫	11/27/2018
Amazon Connect	使用 AWS CloudTrail記錄 Amazon Connect API 呼叫	12/11/2019
Amazon 數據 Firehose	使用以監控 Amazon 資料 Firehose API 呼叫 AWS CloudTrail	2016/03/17

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Data Lifecycle Manager	使用記錄 Amazon Data Lifecycle Manager API 呼叫 AWS CloudTrail	2018/07/24
Amazon Detective	使用 AWS CloudTrail記錄 Amazon Detective API 呼叫	03/31/2020
Amazon DevOps 大師	使用記錄 Amazon DevOps 大師 API 調用 AWS CloudTrail	2021 年 4 月 5 日
Amazon DocumentDB (with MongoDB compatibility)	使用 AWS CloudTrail記錄 Amazon DocumentDB API 呼叫	2019/01/09
Amazon DynamoDB	使用記錄 DynamoDB 資料庫作業 AWS CloudTrail	2015/05/28
Amazon EC2	使用記錄 Amazon EC2 API 呼叫 AWS CloudTrail	11/13/2013
Amazon EC2 Auto Scaling	使用記錄 Auto Scaling API 呼叫 CloudTrail	2014/07/16
Amazon EC2 容量區塊	記錄容量封鎖 API 呼叫 AWS CloudTrail	10/31/2023
Amazon EC2 Image Builder	使用記錄 EC2 Image Builder API 呼叫 CloudTrail	12/02/2019
Amazon Elastic Block Store (Amazon EBS) EBS 直接 API	使用記錄 API 呼叫 AWS CloudTrail 使用 AWS CloudTrail記錄 EBS 直接 API 的 API 呼叫	Amazon EBS：2013/11/13 EBS 直接 API：2020/06/30
Amazon Elastic Container Registry (Amazon ECR)	使用記錄 Amazon ECR API 呼叫 AWS CloudTrail	2015/12/21

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Elastic Container Service (Amazon ECS)	使用記錄 Amazon ECS API 呼叫 AWS CloudTrail	2015/04/09
Amazon Elastic File System (Amazon EFS)	使用記錄 Amazon EFS API 呼叫 AWS CloudTrail	2016/06/28
Amazon Elastic Kubernetes Service (Amazon EKS)	使用日誌記錄 Amazon EKS API 調用 AWS CloudTrail	2018/06/05
Amazon Elastic Transcoder	使用日誌記錄 Amazon Elastic Transcoder API 調用 AWS CloudTrail	2014/10/27
Amazon ElastiCache	使用記錄 Amazon ElastiCache API 呼叫 AWS CloudTrail	2014/09/15
Amazon EMR	記錄 Amazon EMR API 呼叫 AWS CloudTrail	2014/04/04
EKS 上的 Amazon EMR	使用 AWS CloudTrail在 EKS API 呼叫上記錄 Amazon EMR	12/09/2020
Amazon EventBridge	使用記錄 Amazon EventBridge API 呼叫 AWS CloudTrail	07/11/2019
Amazon FinSpace	查詢 AWS CloudTrail 記錄檔	10/18/2022
Amazon Forecast	使用記錄 Amazon Forecast API 呼叫 AWS CloudTrail	2018/11/28
Amazon Fraud Detector	使用 AWS CloudTrail記錄 Amazon Fraud Detector API 呼叫	01/09/2020
Amazon FSx for Lustre	記錄 Amazon FSx for Lustre API 調用，使用 AWS CloudTrail	01/11/2019

AWS 服務	CloudTrail 主題	支援開始時間
Amazon FSx for Windows File Server	使用監控 AWS CloudTrail	2018/11/28
Amazon GameLift	使用記錄 Amazon GameLift API 呼叫 AWS CloudTrail	2016/01/27
Amazon GuardDuty	使用記錄 Amazon GuardDuty API 呼叫 AWS CloudTrail	2018/02/12
Amazon Inspector	使用記錄 Amazon Inspector API 調用 AWS CloudTrail	11/29/2021
Amazon Inspector Classic	使用記錄 Amazon Inspector 經典 API 調用 AWS CloudTrail	2016/04/20
Amazon Inspector 掃描	Amazon Inspector 掃描信息 CloudTrail	11/27/2023
Amazon Interactive Video Service	使用 AWS CloudTrail記錄 Amazon IVS API 呼叫	07/15/2020
Amazon Kendra	使用日誌記錄 Amazon Kendra API 呼叫，AWS CloudTrail 並記錄 Amazon Kendra 智慧排名 API 呼叫 AWS CloudTrail	05/11/2020
Amazon Keyspaces (適用於 Apache Cassandra)	使用 AWS CloudTrail記錄 Amazon Keyspaces API 呼叫	2020/01/13
Amazon Managed Service for Apache Flink	記錄阿帕奇 Flink API 調用的託管服務 AWS CloudTrail	2019/03/22
Amazon Kinesis Data Streams	使用記錄 Amazon Kinesis Data Streams API 呼叫使用 AWS CloudTrail	2014/04/25

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Kinesis Video Streams	使用記錄 Kinesis Video Streams API 呼叫 AWS CloudTrail	2018/05/24
Amazon Lex	使用記錄 Amazon Lex API 呼叫 CloudTrail	2017/08/15
Amazon Lightsail	使用記錄 Lightsail API 呼叫 AWS CloudTrail	2016/12/23
Amazon Location Service	使用 AWS CloudTrail記錄和監控	12/15/2020
Amazon Lookout for Equipment	監控設備的 Amazon 瞭望	12/01/2020
Amazon Lookout for Metrics	檢視 Amazon Lookout for Metrics API 活動 AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	使用 AWS CloudTrail記錄 Amazon Lookout for Vision 呼叫	12/01/2020
Amazon Machine Learning	使用記錄 Amazon ML API 呼叫 AWS CloudTrail	2015/12/10
Amazon Macie	使用 AWS CloudTrail記錄 Amazon Macie API 呼叫	05/13/2020
Amazon Managed Blockchain	使用 AWS CloudTrail記錄 Amazon Managed Blockchain API 呼叫 使用 AWS CloudTrail記錄 Ethereum 的 Managed Blockchain API 呼叫 (預覽版)	2019 年 1 月 4 日

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Managed Grafana	使用 AWS CloudTrail記錄 Amazon Managed Grafana API 呼叫	12/15/2020
Amazon Managed Service for Prometheus	使用 AWS CloudTrail記錄 Amazon Managed Service for Prometheus API 呼叫	12/15/2020
Amazon Managed Streaming for Apache Kafka	使用記錄 API 呼叫 AWS CloudTrail	2018/12/11
Amazon Managed Workflows for Apache Airflow	檢視稽核記錄 AWS CloudTrail	11/24/2020
Amazon MemoryDB for Redis	記錄 Amazon 內存數據庫與 Redis 的 API 調用 AWS CloudTrail	08/19/2021
Amazon MQ	使用記錄 Amazon MQ API 呼叫 AWS CloudTrail	2018/07/19
Amazon Neptune	使用記錄 Amazon Neptune API 呼叫 AWS CloudTrail	2018/05/30
Amazon Nimble Studio	記錄靈活的工作室通話使用 AWS CloudTrail	06/19/2023
Amazon One Enterprise	使用記錄 Amazon 一個企業 API 呼叫 AWS CloudTrail	11/27/2023
Amazon OpenSearch 服務	使用以監控 Amazon OpenSearch 服務 API 呼叫 AWS CloudTrail	2015/10/01
Amazon Personalize	使用記錄 Amazon Personalize 化 API 調用 AWS CloudTrail	2018/11/28

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Pinpoint	使用記錄 Amazon Pinpoint API 呼叫 AWS CloudTrail	2018/02/06
Amazon Pinpoint SMS 和 Voice API	使用記錄 Amazon Pinpoint API 呼叫 AWS CloudTrail	11/16/2018
Amazon Polly	使用日誌記錄 Amazon Polly API 調用 AWS CloudTrail	11/30/2016
Amazon Q (商用)	使用記錄 Amazon Q API 呼叫 AWS CloudTrail	11/28/2023
Amazon Q (用於 AWS 生成器使用)	使用記錄 Amazon Q API 呼叫 AWS CloudTrail	11/28/2023
Amazon Quantum Ledger Database (Amazon QLDB)	使用 AWS CloudTrail記錄 Amazon QLDB API 呼叫	09/10/2019
Amazon QuickSight	記錄作業 CloudTrail	2017/04/28
Amazon Relational Database Service (Amazon RDS)	使用記錄 Amazon RDS API 呼叫 AWS CloudTrail	11/13/2013
Amazon RDS Performance Insights	使用記錄 Amazon RDS API 呼叫 AWS CloudTrail Amazon RDS 績效詳情 API 是 Amazon RDS API 的子集。	2018/06/21
Amazon Redshift	使用記錄 Amazon Redshift API 呼叫 AWS CloudTrail	2014/06/10
Amazon Rekognition	使用記錄 Amazon Rekognition API 呼叫 AWS CloudTrail	2018/04/06
Amazon Route 53	使用 AWS CloudTrail 來擷取傳送到 Route 53 API 的請求	2015/02/11

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Route 53 應用程式復原控制器	使用日誌記錄 Amazon 路由 53 應用程式恢復控制器 AWS CloudTrail	2021 年 7 月 27 日
Amazon S3	使用記錄 Amazon S3 API 呼叫 AWS CloudTrail	管理事件：2015/09/01 資料事件：2016/11/21
Amazon S3 Glacier	使用記錄 S3 冰川 API 呼叫 AWS CloudTrail	2014/12/11
Amazon SageMaker	使用記錄 Amazon SageMaker API 呼叫 AWS CloudTrail	2018/01/11
Amazon Security Lake	使用記錄 Amazon 安全湖 API 呼叫 CloudTrail	05/30/2023
Amazon Simple Email Service (Amazon SES)	使用記錄 Amazon SES API 呼叫 AWS CloudTrail	2015/05/07
Amazon Simple Notification Service (Amazon SNS)	使用記錄 Amazon SNS API 呼叫 AWS CloudTrail	2014/10/09
Amazon Simple Queue Service (Amazon SQS)	使用記錄 Amazon SQS API 動作 AWS CloudTrail	2014/07/16
Amazon Simple Workflow Service (Amazon SWF)	使用記錄 API 呼叫 AWS CloudTrail	管理事件:2014 年 5 月 13 日 數據事件:2024 年 2 月 14 日
Amazon Textract	使用日誌記錄 Amazon Textract API 調用 AWS CloudTrail	2019/05/29
Amazon Timestream	記錄時間流 API 呼叫 AWS CloudTrail	09/30/2020

AWS 服務	CloudTrail 主題	支援開始時間
Amazon Transcribe	使用日誌記錄 Amazon Transcribe API 調用 AWS CloudTrail	2018/06/28
Amazon Translate	使用 AWS CloudTrail記錄 Amazon Translate API 呼叫	2018/04/04
Amazon Verified Permissions	使用記錄 Amazon 驗證許可 API 調用 AWS CloudTrail	06/13/2023
Amazon Virtual Private Cloud (Amazon VPC)	使用記錄 API 呼叫 AWS CloudTrail Amazon VPC API 是 Amazon EC2 API 的子集。	11/13/2013
Amazon VPC Lattice	CloudTrail 日誌	03/31/2023
Amazon VPC Reachability Analyzer	記錄可達性分析器 API 呼叫使用 AWS CloudTrail	11/27/2023
Amazon WorkDocs	使用記錄 Amazon WorkDocs API 呼叫 AWS CloudTrail	2014/08/27
Amazon WorkMail	使用記錄 Amazon WorkMail API 呼叫 AWS CloudTrail	2017/12/12
Amazon WorkSpaces	使用記錄 Amazon WorkSpaces API 呼叫 CloudTrail	2015/04/09
Amazon WorkSpaces 瘦客戶端	使用記錄 Amazon WorkSpaces 精簡型用戶端 API 呼叫 AWS CloudTrail	11/26/2023
Amazon WorkSpaces 網站	使用記錄 Amazon WorkSpaces 網頁 API 呼叫 AWS CloudTrail	11/30/2021

AWS 服務	CloudTrail 主題	支援開始時間
Application Auto Scaling	記錄 Application Auto Scaling API 呼叫 AWS CloudTrail	2016/10/31
AWS Amplify	使用 AWS CloudTrail記錄 Amplify API 呼叫	11/30/2020
AWS App Mesh	使用 AWS CloudTrail記錄 App Mesh API 呼叫	AWS App Mesh 10/30/2019 App Mesh Envoy 管理服務 03/18/2022
AWS App Runner	記錄應用程序運行器 API 調用 AWS CloudTrail	05/18/2021
AWS AppConfig	使用記錄 AWS AppConfig API 呼叫 AWS CloudTrail	管理層事件:7 月 31 日 數據事件:2024 年 1 月 4 日
AWS AppFabric	使用記錄 AWS AppFabric API 呼叫 AWS CloudTrail	06/27/2023
AWS 應用程式成本分析工具	AWS 應用程式成本分析工具 API 參考	2021 年 5 月 13 日
AWS Application Discovery Service	使用 AWS CloudTrail記錄 Application Discovery Service API 呼叫	2016/05/12
AWS 應用轉型服務	（ AWS 工具使用的後端服務，例如 .NET 的 AWS 微服務提取器）	08/26/2023
AWS AppSync	使用記錄 AWS AppSync API 呼叫 AWS CloudTrail	2018/02/13
AWS Artifact	使用記錄 AWS Artifact API 呼叫 AWS CloudTrail	01/27/2023

AWS 服務	CloudTrail 主題	支援開始時間
AWS Audit Manager	使用記錄 AWS Audit Manager API 呼叫 AWS CloudTrail	12/07/2020
AWS Auto Scaling	使用記錄 AWS Auto Scaling API 呼叫 CloudTrail	08/15/2018
AWS 數據交換	使用記錄 AWS B2B 資料交換 API 呼叫 AWS CloudTrail	12/01/2023
AWS Backup	使用記錄 AWS Backup API 呼叫 AWS CloudTrail	2019/02/04
AWS Batch	使用記錄 AWS Batch API 呼叫 AWS CloudTrail	2018/1/10
AWS Billing and Cost Management	使用記錄 AWS Billing and Cost Management API 呼叫 AWS CloudTrail	2018/06/07
AWS Billing Conductor	使用記錄 AWS Billing Conductor API 呼叫 AWS CloudTrail	03/12/2024
AWS BugBust	使用記錄 BugBust API 呼叫 CloudTrail	06/24/2021
AWS Certificate Manager	使用 AWS CloudTrail	2016/03/25
AWS Clean Rooms	使用記錄 AWS Clean Rooms API 呼叫 AWS CloudTrail	03/21/2023
AWS Cloud Map	使用記錄 AWS Cloud Map API 呼叫 AWS CloudTrail	2018/11/28
AWS Cloud9	使用記錄 AWS Cloud9 API 呼叫 AWS CloudTrail	01/21/2019

AWS 服務	CloudTrail 主題	支援開始時間
AWS CloudFormation	記錄 AWS CloudFormation API 呼叫 AWS CloudTrail	2014/04/02
AWS CloudHSM	使用記錄 AWS CloudHSM API 呼叫 AWS CloudTrail	2015/01/08
AWS CloudShell	登錄和監控 AWS CloudShell	12/15/2020
AWS CloudTrail	AWS CloudTrail API 參考資料 (所有 CloudTrail API 呼叫皆由記錄 CloudTrail。)	11/13/2013
AWS CodeArtifact	使用記錄 CodeArtifact API 呼叫 AWS CloudTrail	06/10/2020
AWS CodeBuild	使用記錄 AWS CodeBuild API 呼叫 AWS CloudTrail	2016/12/01
AWS CodeCommit	使用記錄 AWS CodeCommit API 呼叫 AWS CloudTrail	2017/01/11
AWS CodeDeploy	監視部署 AWS CloudTrail	2014/12/16
AWS CodePipeline	使用記錄 CodePipeline API 呼叫 AWS CloudTrail	2015/07/09
AWS CodeStar	使用記錄 AWS CodeStar API 呼叫 AWS CloudTrail	2017/06/14
AWS CodeStar 通知	記錄 AWS CodeStar 通知 API 呼叫 AWS CloudTrail	11/05/2019
AWS Config	使用記錄 AWS Config API 呼叫的方式 AWS CloudTrail	2015/02/10
AWS 控制目錄	記錄 AWS 控制目錄 API 呼叫使用 AWS CloudTrail	04/08/2024

AWS 服務	CloudTrail 主題	支援開始時間
AWS Control Tower	記錄 AWS Control Tower 動作 AWS CloudTrail	08/12/2019
AWS Data Pipeline	使用記錄 AWS Data Pipeline API 呼叫 AWS CloudTrail	2014/12/02
AWS Database Migration Service (AWS DMS)	使用記錄 AWS Database Migration Service API 呼叫 AWS CloudTrail	2016/02/04
AWS DataSync	使用記錄 AWS DataSync API 呼叫 AWS CloudTrail	11/26/2018
AWS 截止日期雲	記錄呼叫 CloudTrail	04/02/2024
AWS Device Farm	使用記錄 AWS Device Farm API 呼叫 AWS CloudTrail	2015/07/13
AWS Direct Connect	記錄 AWS Direct Connect API 呼叫 AWS CloudTrail	2014/03/08
AWS Directory Service	使用記錄 AWS Directory Service API 呼叫 CloudTrail	2015/05/14
AWS Elastic Beanstalk (Elastic Beanstalk)	使用 Elastic Beanstalk API 呼叫搭配使用 AWS CloudTrail	2014/03/31
AWS Elastic Disaster Recovery	使用記錄 AWS Elastic Disaster Recovery API 呼叫 AWS CloudTrail	11/17/2021
AWS Elemental MediaConnect	使用記錄 AWS Elemental MediaConnect API 呼叫 AWS CloudTrail	11/27/2018

AWS 服務	CloudTrail 主題	支援開始時間
AWS Elemental MediaConvert	使用記錄 AWS Elemental MediaConvert API 呼叫 CloudTrail	2017/11/27
AWS Elemental MediaLive	使用記錄 MediaLive API 呼叫 AWS CloudTrail	01/19/2019
AWS Elemental MediaPackage	使用記錄 AWS Elemental MediaPackage API 呼叫 AWS CloudTrail	12/21/2018
AWS Elemental MediaStore	使用記錄 AWS Elemental MediaStore API 呼叫 CloudTrail	2017/11/27
AWS Elemental MediaTailor	使用記錄 AWS Elemental MediaTailor API 呼叫 AWS CloudTrail	2019/02/11
AWS 實體解析度	使用 A 記錄 AWS 實體解析 API 呼叫AWS CloudTrail	07/26/2023
AWS Fault Injection Service	使用記錄 API 呼叫 AWS CloudTrail	03/15/2021
AWS Firewall Manager	使用記錄 AWS Firewall Manager API 呼叫 AWS CloudTrail	2018/04/05
AWS Global Accelerator	記錄 AWS 全域加速器 API 呼叫 AWS CloudTrail	11/26/2018
AWS Glue	記錄 AWS Glue 作業使用 AWS CloudTrail	2017/11/07
AWS Ground Station	使用記錄 AWS Ground Station API 呼叫 AWS CloudTrail	05/31/2019

AWS 服務	CloudTrail 主題	支援開始時間
AWS Health	使用記錄 AWS Health API 呼叫 AWS CloudTrail	2016/11/21
AWS Health Dashboard	使用記錄 AWS Health API 呼叫 AWS CloudTrail	2016/12/01
AWS HealthImaging	使用記錄 AWS HealthImaging API 呼叫 AWS CloudTrail	07/26/2023
AWS HealthLake	使用記錄 AWS HealthLake API 呼叫 AWS CloudTrail	12/07/2020
AWS HealthOmics	使用記錄 AWS HealthOmics API 呼叫 AWS CloudTrail	11/29/2022
AWS IAM Identity Center	使用記錄 IAM 身分識別中心 API 呼叫 AWS CloudTrail	2017/12/07
AWS Identity and Access Management (IAM)	使用記錄 IAM 事件 AWS CloudTrail	11/13/2013
AWS IoT	使用記錄 AWS IoT API 呼叫 AWS CloudTrail	2016/04/11
AWS IoT 1-Click	使用記錄 AWS IoT 1-Click API 呼叫 AWS CloudTrail	2018/05/14
AWS IoT 分析	記錄 AWS IoT 分析 API 呼叫 AWS CloudTrail	2018/04/23
AWS IoT 活動	記錄 AWS IoT 事件 API 呼叫 AWS CloudTrail	2019/06/11
AWS IoT Greengrass	使用記錄 AWS IoT Greengrass API 呼叫 AWS CloudTrail	10/29/2018
AWS IoT Greengrass V2	使用記錄 AWS IoT Greengrass V2 API 呼叫 AWS CloudTrail	12/14/2020

AWS 服務	CloudTrail 主題	支援開始時間
AWS IoT SiteWise	使用記錄 AWS IoT SiteWise API 呼叫 AWS CloudTrail	2020/04/29
AWS Key Management Service (AWS KMS)	使用記錄 AWS KMS API 呼叫 AWS CloudTrail	2014/11/12
AWS Lake Formation	使用記錄 AWS Lake Formation API 呼叫 AWS CloudTrail	08/09/2019
AWS Lambda	使用記錄 AWS Lambda API 呼叫 AWS CloudTrail	管理事件：2015/04/09 資料事件：2017/11/30
AWS Launch Wizard	使用記錄 AWS Launch Wizard API 呼叫 AWS CloudTrail	11/08/2023
AWS License Manager	使用記錄 L AWS icense Manager API 呼叫 AWS CloudTrail	2019/03/01
AWS Mainframe Modernization	使用記錄 AWS Mainframe Modernization API 呼叫 AWS CloudTrail	2022 年 8 月 6 日
AWS Managed Services	AMS Accelerate 中的日誌管理	2016/12/21
AWS Marketplace 協議	記錄協議 API 呼叫使用 AWS CloudTrail	09/01/2023
AWS Marketplace 部署服務	記錄 AWS Marketplace 部署服務呼叫 CloudTrail	11/29/2023
AWS Marketplace 發現	使用記錄 AWS Marketplace 探索 API 呼叫 AWS CloudTrail	12/15/2022
AWS Marketplace 計量服務	使用記錄 AWS Marketplace API 呼叫 AWS CloudTrail	2018/08/22

AWS 服務	CloudTrail 主題	支援開始時間
AWS Migration Hub	使用記錄 AWS Migration Hub API 呼叫 AWS CloudTrail	2017/08/14
AWS Network Firewall	使用以下方式記錄對 AWS Network Firewall API 的呼叫 AWS CloudTrail	11/17/2020
AWS OpsWorks for Chef Automate	使用記錄 AWS OpsWorks for Chef Automate API 呼叫 AWS CloudTrail	2018/07/16
AWS OpsWorks for Puppet Enterprise	記錄 OpsWorks 木偶企業 API 呼叫時使用 AWS CloudTrail	2018/07/16
AWS OpsWorks Stacks	使用記錄 AWS OpsWorks Stacks API 呼叫 AWS CloudTrail	2014/06/04
AWS Organizations	使用記錄 AWS Organizations API 呼叫 AWS CloudTrail	2017/02/27
AWS Outposts	使用記錄 AWS Outposts API 呼叫 AWS CloudTrail	02/04/2020
AWS Panorama	AWS Panorama API 參考	10/20/2021
AWS Payment Cryptography	使用記錄 AWS Payment Cryptography API 呼叫 AWS CloudTrail	06/08/2023
AWS 私人 5G	使用記錄 AWS 私有 5G API 呼叫 AWS CloudTrail	2022 年 11 月 8 日
AWS Private Certificate Authority (AWS Private CA)	使用 CloudTrail	2018/04/04
AWS Proton	登錄和監控 AWS Proton	2021 年 6 月 9 日

AWS 服務	CloudTrail 主題	支援開始時間
AWS re:Post 私人	使用記錄 AWS re:Post 私人 API 呼叫 AWS CloudTrail	11/26/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	使用記錄 AWS RAM API 呼叫 AWS CloudTrail	11/20/2018
AWS 資源總管	使用記錄 AWS 資源總管 API 呼叫 AWS CloudTrail	11/07/2022
AWS Resource Groups	Resource Groups 中的記錄和監控	2018/06/29
AWS RoboMaker	使用記錄 AWS RoboMaker API 呼叫 AWS CloudTrail	2019/01/16
AWS Secrets Manager	監控 AWS Secrets Manager 秘密的使用	2018/04/05
AWS Security Hub	使用記錄 AWS Security Hub API 呼叫 AWS CloudTrail	11/27/2018
AWS Security Token Service (AWS STS)	使用記錄 IAM 事件 AWS CloudTrail IAM 主題包含的資訊 AWS STS。	11/13/2013
AWS Serverless Application Repository	使用記錄 AWS Serverless Application Repository API 呼叫 AWS CloudTrail	2018/02/20
AWS Service Catalog	使用記錄 Service Catalog API 呼叫 AWS CloudTrail	2016/07/06
AWS Shield	使用記錄 Shield 進階 API 呼叫 AWS CloudTrail	2018/02/08

AWS 服務	CloudTrail 主題	支援開始時間
AWS Snowball 邊緣	使用記錄 AWS Snowball 邊緣 API 呼叫 AWS CloudTrail	2019/01/25
AWS Step Functions	使用記錄 AWS Step Functions API 呼叫 AWS CloudTrail	2016/12/01
AWS Storage Gateway	使用記錄 Storage Gateway API 呼叫 AWS CloudTrail	2014/12/16
AWS Support	使用記錄 AWS Support API 呼叫 AWS CloudTrail	2016/04/21
AWS Support 建議 (預覽)	記錄 AWS Support 建議 API 呼叫 AWS CloudTrail	05/22/2024
AWS Systems Manager	使用記錄 AWS Systems Manager API 呼叫 AWS CloudTrail	2017/11/29
AWS Systems Manager Incident Manager	使用記錄 AWS Systems Manager 事件管理員 API 呼叫 AWS CloudTrail	2021 年 5 月 10 日
AWS 電信網絡生成器（AWS TNB）	使用記錄 AWS 電信網絡生成器 API 調用 AWS CloudTrail	02/21/2023
AWS Transfer for SFTP	使用記錄 AWS Transfer for SFTP API 呼叫 AWS CloudTrail	2019/01/08
AWS Transit Gateway	使用 AWS CloudTrail記錄 Transit Gateway 的 API 呼叫	11/26/2018
AWS Trusted Advisor	記錄 AWS Trusted Advisor 主控台動作 AWS CloudTrail	10/22/2020

AWS 服務	CloudTrail 主題	支援開始時間
AWS Verified Access	使用記錄 AWS Verified Access API 呼叫 AWS CloudTrail	04/27/2023
AWS WAF	使用記錄 AWS WAF API 呼叫 AWS CloudTrail	2016/04/28
AWS Well-Architected Tool	使用記錄 AWS Well-Architected Tool API 呼叫 AWS CloudTrail	12/15/2020
AWS X-Ray	使用記錄 AWS X-Ray API 呼叫 CloudTrail	2018/04/25
Elastic Load Balancing	AWS CloudTrail C@@lassic Load Balancer 的AWS CloudTrail記錄和 Application Load Balancer 的記錄	2014/04/04
FreeRTOS 無線更新 (OTA)	使用記錄 AWS IoT OTA API 調用 AWS CloudTrail	2019/05/22
Service Quotas	記錄 Service Quotas API 呼叫使用 AWS CloudTrail	06/24/2019

CloudTrail 不支援服務

服務尚在預覽階段，或還未正式發佈供普通用戶使用 (GA)，或者因沒有公有 API 而不在考慮支援之列。

此外，不支援下列 AWS 服務和事件：

- AWS Import/Export
- Amazon VPC 端點的政策特定事件

如需支援 AWS 服務的清單，請參閱AWS 的服務主題 CloudTrail。

配額 AWS CloudTrail

下表說明範圍內的配額 (先前稱為限制) CloudTrail。 CloudTrail 沒有可調整的配額。如需中其他配額的相關資訊 AWS，請參閱AWS 服務配額。

資源	預設配額	說明
每個區域的追蹤數目	5	此配額無法增加。
取得、說明和列出 API	每秒 10 次交易 (TPS)	您每秒可以提出而不受限制的操作請求數量上限。`CancelQuery` 、`LookupEvents` `ListInsightsMetricData` `PutAuditEvents` 、和 `StartQuery` API 不包含在此類別中。
CancelQuery、 StartQuery API	每秒 3 次交易 (TPS)	您每秒可以提出而不受限制的操作請求數量上限。 此配額無法增加。
LookupEvents API	每秒 2 次交易 (TPS)。	您每秒可以提出而不受限制的操作請求數量上限。 此配額無法增加。
ListInsightsMetricData API	一秒 1 個交易 (TPS)	您每秒可以提出而不受限制的操作請求數量上限。 此配額無法增加。
PutAuditEvents API	每秒 100 次交易 (TPS)	您每秒可以提出而不受限制的操作請求數量上限。 此配額無法增加。

資源	預設配額	說明
所有其他 API	一秒 1 個交易 (TPS)	您每秒可以提出而不受限制的操作請求數量上限。 此配額無法增加。
事件資料存放區	10	在任何一個 AWS 區域中，您可以擁有的事件資料存放區的數目上限。這包括針對某個區域的單一區域事件資料存放區，以及針對全部 AWS 區域的任何多區域事件資料存放區。它還包括處於任何生命週期階段的事件資料存放區。 此配額無法增加。
頻道	25	此配額適用於 CloudTrail Lake 與外部事件來源整合的頻道 AWS，且不適用於服務連結通道。 此配額無法增加。
並行查詢	10	您可以在 CloudTrail Lake 中同時執行的佇列或執行中查詢數目上限。 此配額無法增加。
每個 PutAuditEvents 請求的事件	100	每個 `PutAuditEvents` 請求最多可供新增 100 個活動事件 (或最多 1 MB 大小)。 此配額無法增加。
事件選取器	一個追蹤 5 個	此配額無法增加。

資源	預設配額	說明
進階事件選取器	涵蓋所有進階事件選取器的 500 個條件	如果追蹤或事件資料存放區使用進階事件選取器，則允許用於有進階事件選取器的所有條件值最大總數為 500。除非追蹤或事件資料存放區記錄所有資源 (例如所有 S3 儲存貯體或所有 Lambda 函數) 上的資料事件，否則限制為 250 個資料資源。資料資源可以分散在事件選取器，但整體總數不可以超過 250 個。 此配額無法增加。

資源	預設配額	說明
事件選取器中的資料資源	追蹤中跨所有事件選取器共 250 個	如果選擇使用事件選擇器或進階事件選擇器限制資料事件，追蹤中所有事件選取器的資料資源總數不得超過 250 個。個別事件選取器的資源數目限制最多可設定為 250。只有資料資源總數在所有事件選取器當中未超過 250 時，才允許此上限。 範例： • 允許具有 5 個事件選取器的追蹤，而且每個都設定 50 個資料資源。(5*50=250) • 也允許具有 5 個事件選取器的追蹤，而其中 3 個設定 50 個資料資源、其中 1 個設定 99 個資料資源，而其中 1 個設定 1 個資料資源。((3*50)+1+99=250) • 不允許設定 5 個事件選取器的追蹤，而所有這些事件選取器都設定 100 個資料資源。(5*100=500) 事件選取器僅適用於追蹤。對於事件資料存放區，您必須使用進階事件選取器。 此配額無法增加。 如果您選擇在所有資源 (例如所有 S3 儲存貯體或所有 Lambda

資源	預設配額	說明
		函數) 上記錄資料事件，則此配額不適用。
事件大小	所有事件版本：超過 256 KB 的事件無法傳送至 CloudWatch 記錄 事件版本 1.05 及更新版本：總事件大小限制為 256 KB	Amazon CloudWatch 日誌和 Amazon EventBridge 每個允許 256 KB 的最大事件大小。CloudTrail 不會將超過 256 KB 的事件傳送至 CloudWatch 記錄檔或 EventBridge。 從事件版本 1.05 開始，事件的大小上限為 256 KB。這是為了防止惡意行為者利用，並允許其他 AWS 服務（例如 CloudWatch Logs 和 EventBridge.
CloudTrail 傳送至 Amazon S3 的檔案大小	50 MB 的 ZIP 檔案 (壓縮後)	對於管理和資料事件，請以最大 50 MB (壓縮) ZIP 檔案 CloudTrail 傳送事件至 S3。 如果在追蹤上啟用，Amazon SNS 會在 CloudTrail 將 ZIP 檔案傳送到 S3 之後傳送日誌交付通知。

開始使用 AWS CloudTrail 教學課程

如果您不熟悉 AWS CloudTrail，這些教學課程可協助您學習如何使用其功能。

主題

- 授予使用權限 CloudTrail
- 檢視事件記錄
- 建立記錄管理事件的追蹤
- 為 S3 資料事件建立事件資料存放區
- 將追蹤事件複製到 CloudTrail Lake 事件資料存放區
- 檢視 CloudTrail 湖泊儀表板
- 檢視和執行 CloudTrail 湖泊範例查詢
- 將 CloudTrail 湖泊查詢結果儲存至 S3 儲存貯體

授予使用權限 CloudTrail

若要建立、更新和管理追蹤、事件 CloudTrail 資料存放區和通道等資源，您需要授予使用權限 CloudTrail。本節提供可用的受管理原則的相關資訊 CloudTrail。

> **Note**
>
> 您授予使用者執行 CloudTrail 管理任務的許可與將日誌檔傳送到 Amazon S3 儲存貯體或傳送通知至 Amazon SNS 主題所 CloudTrail 需的許可不同。如需這些許可的詳細資訊，請參閱 Amazon S3 存儲桶政策 CloudTrail。
>
> 如果您設定與 Amazon CloudWatch 日誌的整合， CloudTrail 還需要一個角色，該角色可將事件傳遞到 Amazon CloudWatch 日誌日誌群組。您必須建立使 CloudTrail 用的角色。如需詳細資訊，請參閱 授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限及 將事件傳送至 CloudWatch 記錄檔。

下列 AWS 受管理的策略適用於 CloudTrail：

- AWSCloudTrail_FullAccess— 此原則提供對 CloudTrail 資源 CloudTrail 動作 (例如追蹤、事件資料存放區和通道) 的完整存取權。此原則提供建立、更新和刪除 CloudTrail追蹤、事件資料存放區和通道所需的權限。

此政策還提供管理 Amazon S3 儲存貯體、 CloudWatch 日誌的日誌群組和追蹤的 Amazon SNS 主題的許可。不過，受AWSCloudTrail_FullAccess管政策並未提供刪除 Amazon S3 儲存貯體、CloudWatch 日誌的日誌群組或 Amazon SNS 主題的許可。如需其他 AWS 服務之受管理策略的相關資訊，請參閱受AWS 管理策略參考指南。

> **Note**
>
> 該AWSCloudTrail_FullAccess政策不打算在您 AWS 帳戶的. 使用此角色的使用者可以在自己的 AWS 帳戶中關閉或重新設定最敏感和重要的稽核功能。因此，您必須僅向帳戶管理員套用此政策。您必須嚴密控制並監視此政策的使用狀況。

- AWSCloudTrail_ReadOnlyAccess— 此原則授與檢視 CloudTrail 主控台的權限，包括最近的事件和事件歷程記錄。此政策還允許您檢視現有的追蹤、事件資料存放區和通道。使用此政策的角色和使用者可以下載事件歷史記錄，但無法建立或更新追蹤、事件資料存放區或通道。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

  建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。

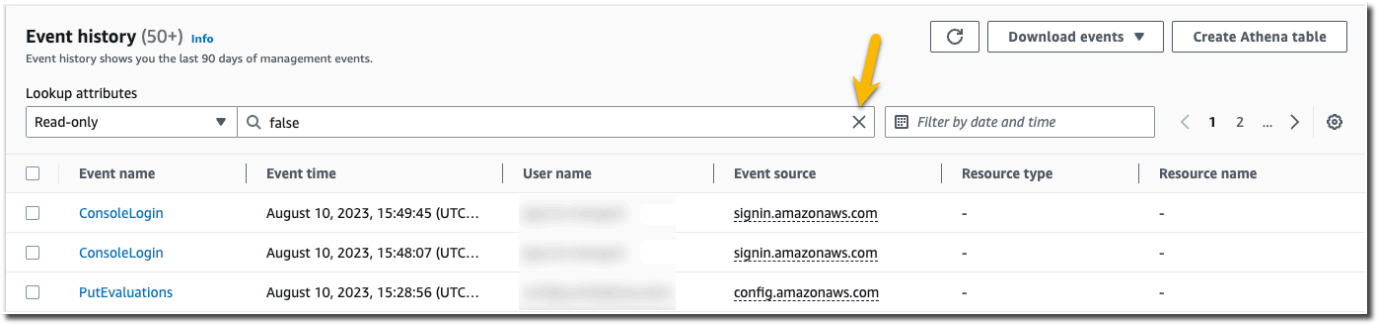
- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

檢視事件記錄

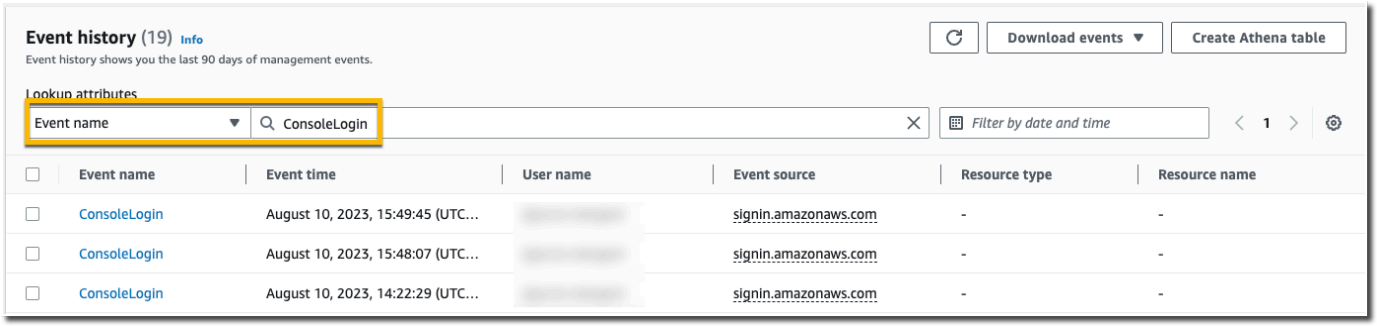
本節說明如何使用 CloudTrail 主控台上的 [CloudTrail 事件歷史記錄] 頁面來檢視目前的過去 90 天的管理事件 AWS 區域。 AWS 帳戶

若要檢視事件歷史記錄

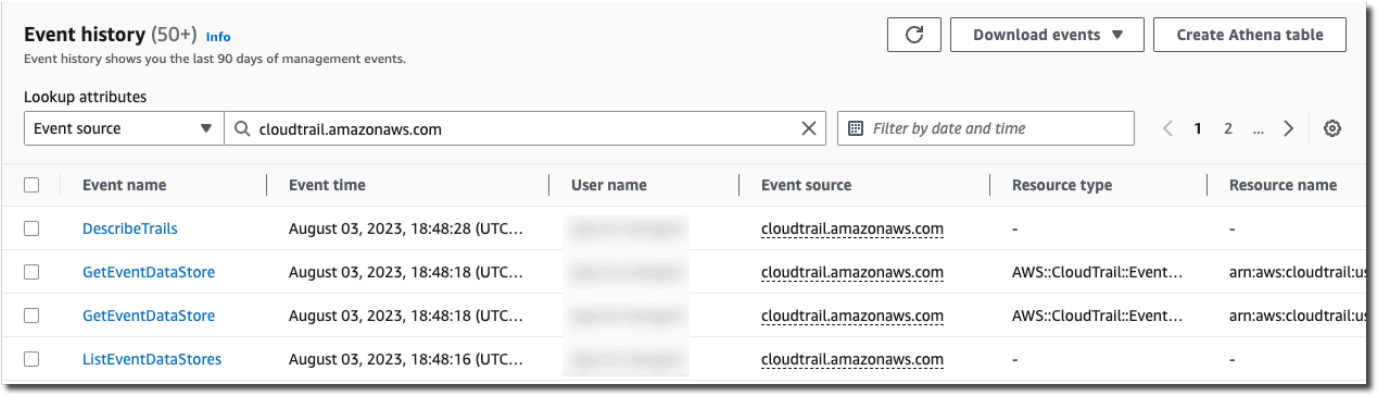
1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Event history (事件歷史記錄)。您可以看到已篩選的事件清單，並最先顯示最近的事件。事件的預設篩選條件為唯讀，並設為 false。您可以選擇過濾器右側的 X 來清除該篩選條件。您可以篩選單一屬性上的事件，以搜尋事件歷史記錄中的事件



3. 選擇要篩選的屬性，然後輸入屬性的完整值。 CloudTrail 無法篩選部分值。例如，若要檢視所有主控台登入事件，請選擇 [事件名稱] 篩選器，然後指定ConsoleLogin屬性值。



或者，若要檢視最近的 CloudTrail 管理事件，請選擇 [事件來源]，然後指定`cloudtrail.amazonaws.com`。



4. 若要檢視特定管理事件，請選擇事件名稱。在事件詳細資訊頁面上，您可以了解事件的相關詳細資訊，查看任何參考資源以及檢視事件記錄。
5. 若要比較事件，請透過填寫事件歷史記錄資料表左邊距中的核取方塊，最多可選取五個事件。您可以 side-by-side 在「比較」事件詳細資訊表格中檢視所選事件的詳細資訊。
6. 您可以將事件歷史記錄下載為 CSV 或 JSON 格式的檔案。下載事件歷史記錄可能需要幾分鐘的時間。

如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。

建立記錄管理事件的追蹤

對於您的第一個追蹤，我們建議您建立記錄所有 AWS 區域中的所有管理事件的追蹤，而不會記錄任何資料事件。管理事件的範例包括安全事件 (例如 IAM `CreateUser` 和 `AttachRolePolicy` 事件)、資源事件 (例如 `RunInstances` 和 `CreateBucket`) 等等。您將建立 Amazon S3 儲存貯體，在其中存放追蹤的日誌檔，做為在 CloudTrail 主控台中建立追蹤的一部分。

> **Note**
>
> 此教學課程將假設您正在建立第一個追蹤。視您 AWS 帳戶中的追蹤數量以及這些追蹤的設定方式而定，下列程序可能會產生也可能不會產生費用。 CloudTrail 將日誌檔存放在 Amazon S3 儲存貯體中，這會產生成本。如需定價的詳細資訊，請參閱 AWS CloudTrail 定價和 Amazon S3 定價。

若要建立追蹤記錄

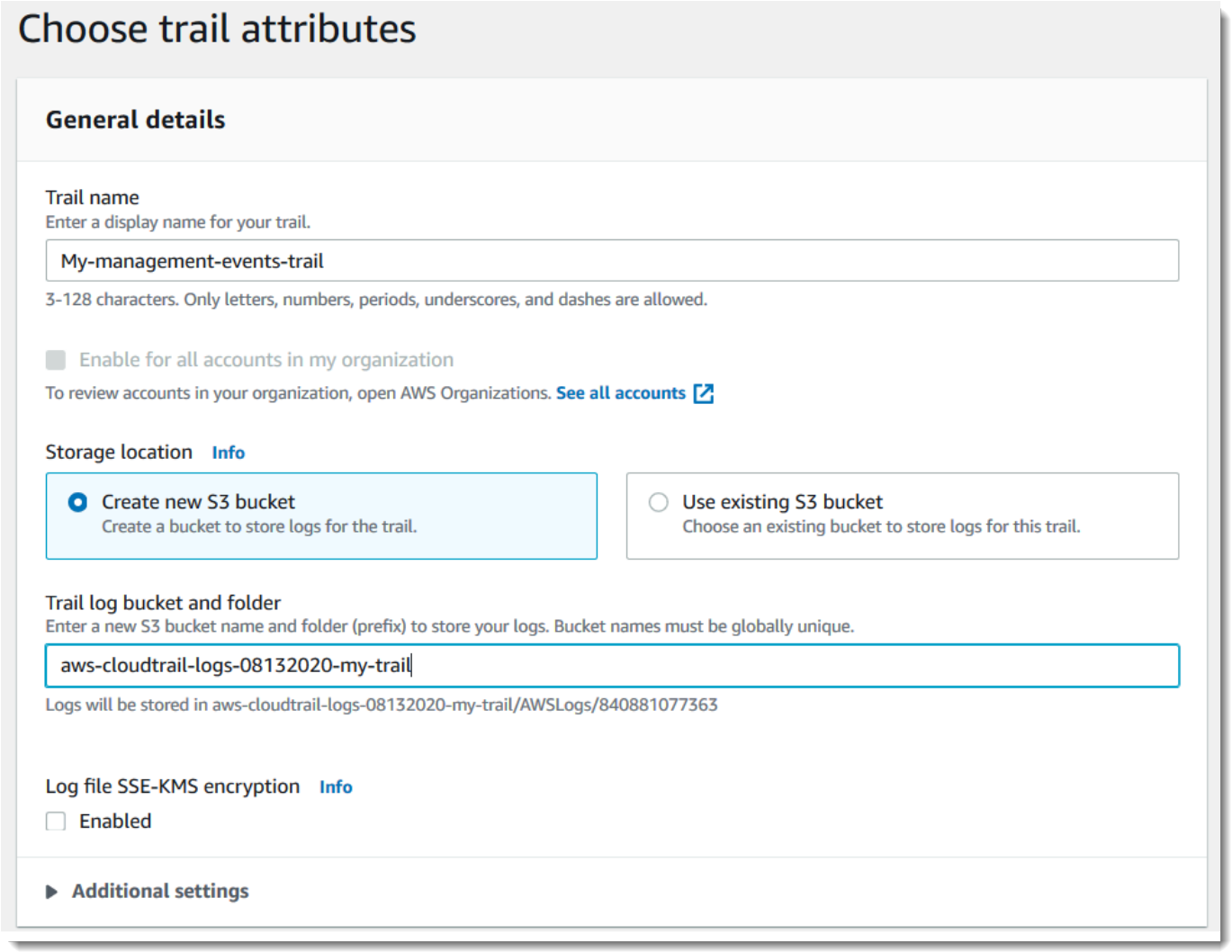
1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在「地區」選取器中，選擇您要建立路徑的「 AWS 區域」。這是該追蹤的主要區域。

> **Note**
>
> 「主區域」是唯一可讓您在建立追蹤後檢視和更新追蹤的 AWS 區域，即使追蹤記錄了所有區 AWS 域中的事件也一樣。

3. 在 CloudTrail 服務首頁、「追蹤」頁面或「儀表板」頁面的「追蹤」區段中，選擇「建立軌跡」。
4. 在 Trail name (追蹤名稱) 中為追蹤命名，例如 *My-Management-Events-Trail*。根據最佳實務，請使用可快速識別追蹤目的的名稱。在此案例中，您正在建立記錄管理事件的追蹤。
5. 保留針對組織中的所有帳戶啟用的預設設定。除非您已在 [Organizations] 中設定帳戶，否則此選項將無法變更。
6. 針對 Storage location (儲存位置)，選擇 Create a new S3 bucket (建立新 S3 儲存貯體)，以建立儲存貯體。建立值區時， CloudTrail 會建立並套用所需的值區政策。如果您選擇建立新的 S3 儲存貯體，您的 IAM 政策需要包含`s3:PutEncryptionConfiguration`動作的權限，因為預設情況下會為儲存貯體啟用伺服器端加密。為您的儲存貯體指定一個易於識別的名稱。

   為了更輕鬆地找到您的日誌，請在現有存儲桶中創建一個新文件夾（也稱為前綴）以存儲 CloudTrail 日誌。

   > **Note**
   >
   > 您 Amazon S3 儲存貯體的名稱在全域中都必須是唯一的。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體命名規則。

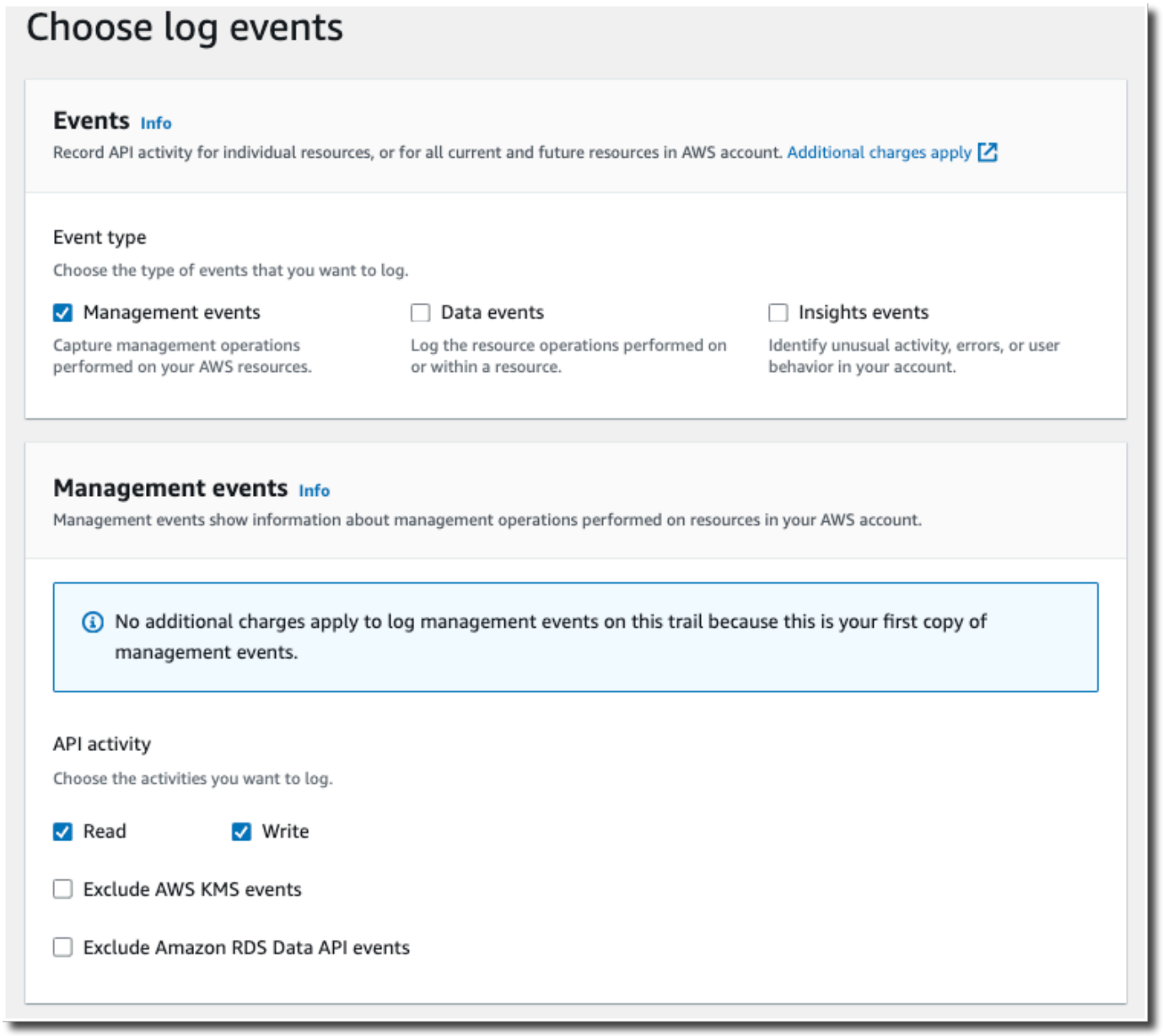


7. 清除核取方塊以停用記錄檔 SSE-KMS 加密。根據預設，您的日誌檔案使用 SSE-S3 加密進行加密。如需有關此設定的詳細資訊，請參閱將伺服器端加密與 Amazon S3 受管金鑰搭配使用 (SSE-S3)。
8. 保留其他設定的預設設定。
9. 保留記CloudWatch 錄檔的預設設定。目前，不要將日誌發送到 Amazon CloudWatch 日誌。
10. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的追蹤。標籤可協助您識別 CloudTrail 追蹤和其他資源，例如包含 CloudTrail 日誌檔的 Amazon S3 儲存貯體。例如，您可以附加名稱為 **`Compliance`**，值為 **`Auditing`** 的標籤。

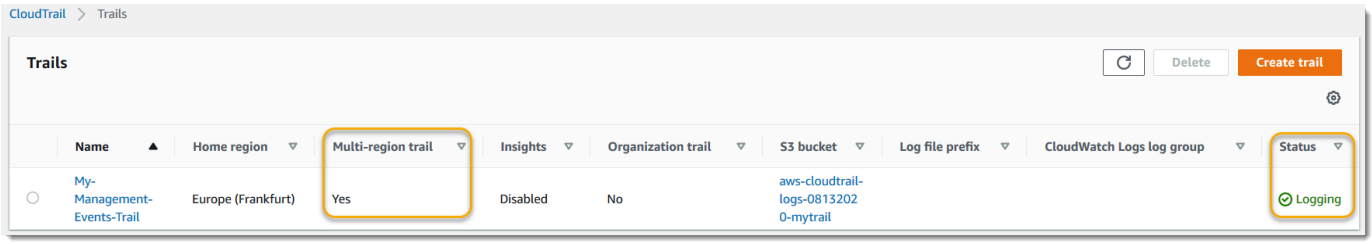
> **Note**
>
> 雖然您可以在 CloudTrail 主控台中建立追蹤時為追蹤新增標籤，並且可以建立 Amazon S3 儲存貯體將日誌檔存放在 CloudTrail 主控台中，但您無法從主控 CloudTrail 台將標籤新增至 Amazon S3 儲存貯體。如需檢視和變更 Amazon S3 儲存貯體屬性 (包括將標籤新增至儲存貯體) 的詳細資訊，請參閱《Amazon S3 使用者指南》。

完成時，選擇 Next (下一步)。

11. 在 Choose log events (選擇記錄事件) 頁面上，選取要記錄的事件類型。對於此追蹤，請保留預設值管理事件。在 Management events 管理事件區域中，選擇同時記錄閱讀和寫入事件 (如果尚未選取)。將排除 AWS KMS 事件和排除 Amazon RDS 資料 API 事件的核取方塊保留空白，以記錄所有管理事件。



12. 保留資料事件和 Insights 事件的預設設定。此追蹤不會記錄任何資料或 CloudTrail 見解事件。選擇 Next (下一步)。
13. 在 Review and create (檢閱和建立) 頁面上，檢閱您為追蹤選擇的設定。針對某個區段選擇 Edit (編輯)，以返回並進行變更。當您準備好建立追蹤時，請選擇 Create trail (建立追蹤)。
14. 此 Trails (追蹤) 頁面會在資料表中顯示您的新追蹤。請注意，追蹤預設設定為多區域追蹤，並且預設會開啟追蹤的記錄功能。



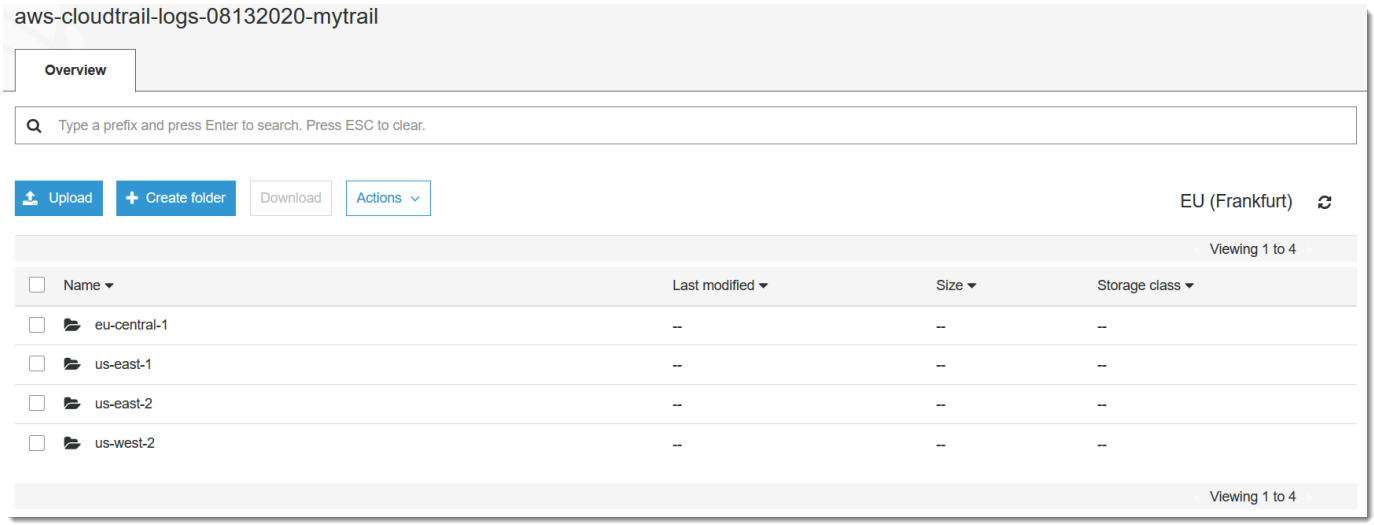
檢視您的日誌檔案

在建立第一個追蹤的平均約 5 分鐘內，將第一組日誌檔 CloudTrail 交付到 Amazon S3 儲存貯體以供追蹤使用。您可以查看這些檔案，並了解其包含的資訊。

> **Note**
>
> CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內提供記錄檔。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
> 如果您錯誤設定追蹤 (例如，無法連線 S3 儲存貯體)， CloudTrail 將嘗試將日誌檔重新傳送到 S3 儲存貯體 30 天，而且這些 attempted-to-deliver 事件將收取標準費用。 CloudTrail 若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

若要檢視您的日誌檔案

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Trails (追蹤記錄)。在追蹤頁面上，尋找您剛才建立的追蹤名稱 (本範例為 *My-Management-Events-Trail*)。
3. 在追蹤的資料列中，選擇 S3 儲存貯體的值 (在範例中，*aws-cloudtrail-logs-08132020-*我追蹤)。
4. Amazon S3 主控台會開啟，並在日誌檔案的最上層顯示該儲存貯體。由於您建立了記錄所有區 AWS 域中事件的追蹤，因此會在顯示每個區域資料夾的層級開啟顯示畫面。*#### Amazon S3 ############/AWS###/## ID/#* CloudTrail選擇您要檢閱記錄檔的「 AWS 地區」資料夾。例如，如果您想要檢閱美國東部 (俄亥俄) 區域的日誌檔案，請選擇 us-east-2。



5. 您可依在該區域中想檢閱的日誌來瀏覽年、月和日的儲存貯體資料夾結構。在該日中，有多個檔案。檔案名稱以您的 AWS 帳戶 ID 開頭，並以副檔名結尾.gz。*###############123456789012##############CloudTrail*

   若要檢視這些檔案，您可以將它們下載、解壓縮，然後在純文字編輯器或 JSON 檔案檢視器進行檢視。有些瀏覽器也支援直接檢視 .gz 和 JSON 檔案。我們建議使用 JSON 檢視器，因為它可以更輕鬆地剖析 CloudTrail 記錄檔中的資訊。

計劃後續步驟

現在您已經有了追蹤，您可以存取 AWS 帳戶中持續的事件和活動記錄。此持續記錄可協助您滿足 AWS 帳戶的會計和稽核需求。但是，您還可以使用 CloudTrail 和 CloudTrail 數據執行更多操作。

- 為追蹤資料增加額外的安全性。 CloudTrail當您建立追蹤時，會自動套用特定等級的安全性。不過，您還可以採取其他的步驟來協助保持資料的安全性。
  - 根據預設，您在建立追蹤時建立的 Amazon S3 儲存貯體會套用政策，允許 CloudTrail 將日誌檔寫入該儲存貯體。該值區無法公開存取，但如果您帳戶中的其他使用者具有讀取和寫入您 AWS 帳戶中儲存貯體的權限，就可以存 AWS 取該值區。檢閱您的儲存貯體政策，若有需要，請透過變更限制存取。如需詳細資訊，請參閱 Amazon S3 安全文件和逐步解說保護儲存貯體的範例。
  - 傳送 CloudTrail 到儲存貯體的日誌檔會使用 Amazon 伺服器端加密，使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。若要提供可直接管理的安全性層級，您可以改為使用伺服器端加密與 AWS KMS—managed 金鑰 (SSE-KMS) 作為記錄檔 CloudTrail 。若要搭配使用 SSE-KMS CloudTrail，您可以建立和管理 KMS 金鑰，也稱為. AWS KMS key 如需詳細資訊，請參閱 使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)。
  - 如需其他安全性規劃，請檢閱的安全性最佳做法 CloudTrail。

- 建立追蹤以記錄資料事件。如果您有興趣在一或多個 Amazon S3 儲存貯體中新增、擷取和刪除物件、在 DynamoDB 表中新增、變更或刪除項目時，或者叫用一個或多個 AWS Lambda 函數時記錄，這些都是資料事件。您先前在此教學課程中建立的管理事件追蹤並不會記錄這些類型的事件。您可以專門為部分或所有支援的資源類型記錄資料事件建立個別追蹤。如需詳細資訊，請參閱 資料事件。

  > **Note**
  >
  > 記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

- 記錄您追蹤上的 CloudTrail 見解事件。 AWS CloudTrail 透過持續分析 CloudTrail 管理事件，深入解析可協助 AWS 使用者識別並回應與 API 呼叫和 API 錯誤率相關的異常活動。 CloudTrail 深入解析會使用數學模型來判斷帳戶的正常 API 和服務事件活動等級。它會識別超出正常模式的行為、產生 Insights 事件，並將這些事件傳送至所選目的地 S3 儲存貯體中 `/CloudTrail-Insight` 資料夾供您進行追蹤。如需 CloudTrail 深入解析的詳細資訊，請參閱記錄 Insights 事件。

  > **Note**
  >
  > 記錄 Insights 事件需支付額外費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

- 設置 CloudWatch 日誌警報以在發生某些事件時提醒您。 CloudWatch 記錄可讓您監視和接收由擷取的特定事件的警示 CloudTrail。例如，您可以監控金鑰的安全性和網路相關的管理事件，例如安全群組變更、失敗 AWS Management Console 登入事件,或 IAM 政策的變更。如需詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。
- 使用分析工具來識別 CloudTrail 日誌中的趨勢。雖然在事件歷史記錄中的篩選條件可協助您在最近的活動中尋找特定事件或事件類型，但它不提供在較長時間區間內搜尋活動的能力。如需更深入且更複雜的分析，您可以使用 Amazon Athena。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的查詢 AWS CloudTrail 記錄。

為 S3 資料事件建立事件資料存放區

您可以建立事件資料存放區來記錄 CloudTrail 事件 (管理事件、資料事件)、CloudTrail Insights 事件、AWS Audit Manager 證據、AWS Config 設定項目或非AWS 事件。

當您為資料事件建立事件資料存放區時，您可以選擇要記錄其資料事件的資源類型 AWS 服務 和資源類型。如需有關記錄 AWS 服務 資料事件的資訊，請參閱資料事件。

本逐步解說說明如何為 Amazon S3 資料事件建立事件資料存放區。在本教學中，我們會選擇一個自訂日誌選取器範本，以便僅在刪除特定 S3 儲存貯體中的物件時記錄事件，而不是記錄所有 Amazon S3 資料事件。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

若要為 S3 資料事件建立事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在 [設定事件資料存放區] 頁面的 [一般詳細資料] 中，為您的事件資料存放區命名，例如 *s3-data-events-eds*。根據最佳實務，請使用可快速識別事件資料存放區目的的名稱。如需 CloudTrail 命名需求的資訊，請參閱命名要求。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

7. (選用) 在加密中，選擇您是否想要使用自己的 KMS 金鑰加密事件資料存放區。依預設，事件資料存放區中的所有事件都會 CloudTrail 使用為您 AWS 擁有和管理的 KMS 金鑰加密。

   若要啟用使用您自己的 KMS 金鑰加密，請選擇使用我自己的 AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail 記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

   > **Note**
   >
   > 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

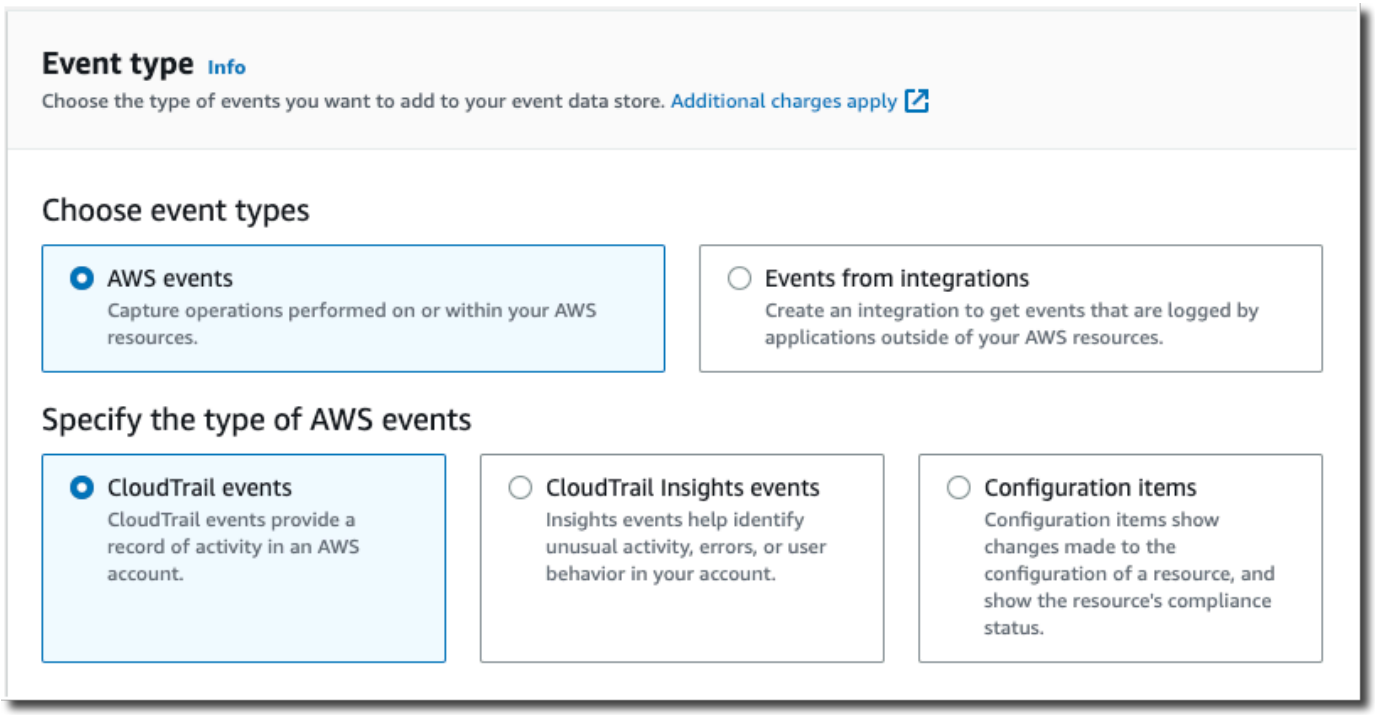
   b. 如果您要建立新角色，請輸入名稱以識別角色。

   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

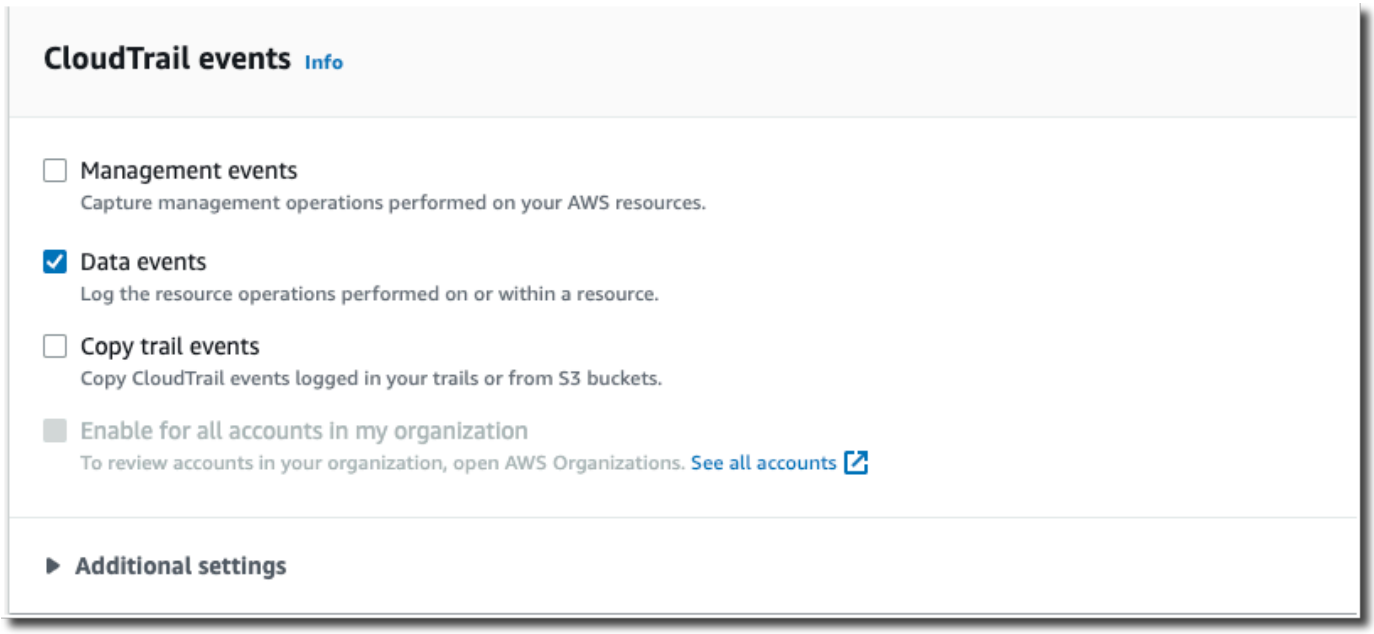
9. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的事件資料存放區。標籤可協助您識別 CloudTrail 事件資料存放區。例如，您可以附加名稱為 **`stage`**，值為 **`prod`** 的標籤。您可以使用標籤來限制對事件資料存放區的存取。您還可以使用標籤來追蹤事件資料存放區的查詢和擷取成本。

如需有關如何使用標籤追蹤成本的資訊，請參閱 為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置。如需有關如何使用 IAM 政策，對以標籤為基礎的事件資料存放區授予存取權的資訊，請參閱 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱《標記資 AWS 源使用指南》中的〈標記 AWS 資源〉。

10. 選擇 Next (下一步) 以設定事件資料存放區。
11. 在選擇事件頁面上，保留事件類型的預設選項。



12. 對於CloudTrail 事件，請選擇資料事件並取消選取管理事件。如需有關資料事件的詳細資訊，請參閱 記錄資料事件。

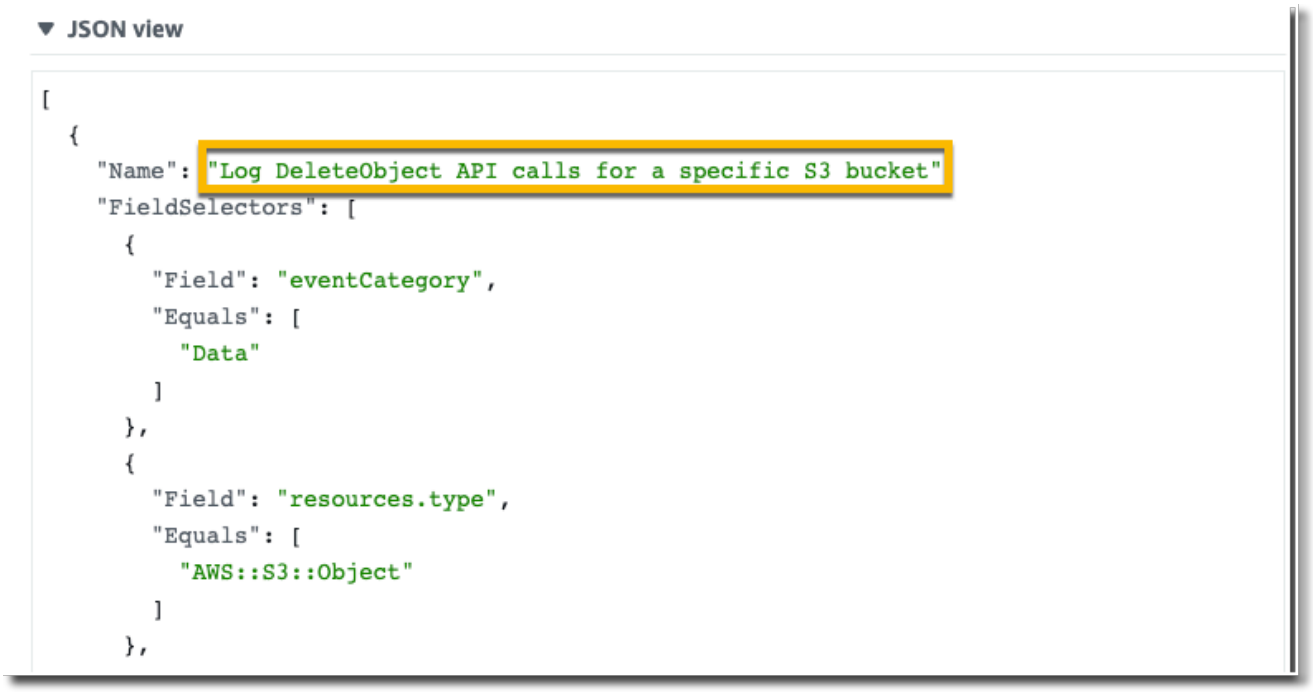


13. 保留複製追蹤事件的預設設定。您可以使用此選項，將現有追蹤事件複製到您的事件資料存放區。如需詳細資訊，請參閱 將追蹤事件複製到事件資料存放區。
14. 如果這是組織事件資料存放區，選擇針對組織中的所有帳戶啟用。除非您已在 AWS Organizations 中設定帳戶，否則此選項將無法變更。
15. 對於其他設定，保留預設選項。依預設，事件資料存放區會為所有人收集事件， AWS 區域 並在建立事件時開始擷取事件。
16. 對於資料事件，請執行下列選擇：

    a. 在資料事件類型中，選擇 S3。資料事件類型可識別記錄資料事件的 AWS 服務 和資源。

    b. 在日誌選取器範本中，選擇自訂。選擇自訂讓您可以定義用於篩選 `eventName`、`resources.ARN` 和 `readOnly` 欄位的自訂事件選取器。如需這些欄位的詳細資訊，請AdvancedFieldSelector參閱 AWS CloudTrail API 參考中的。

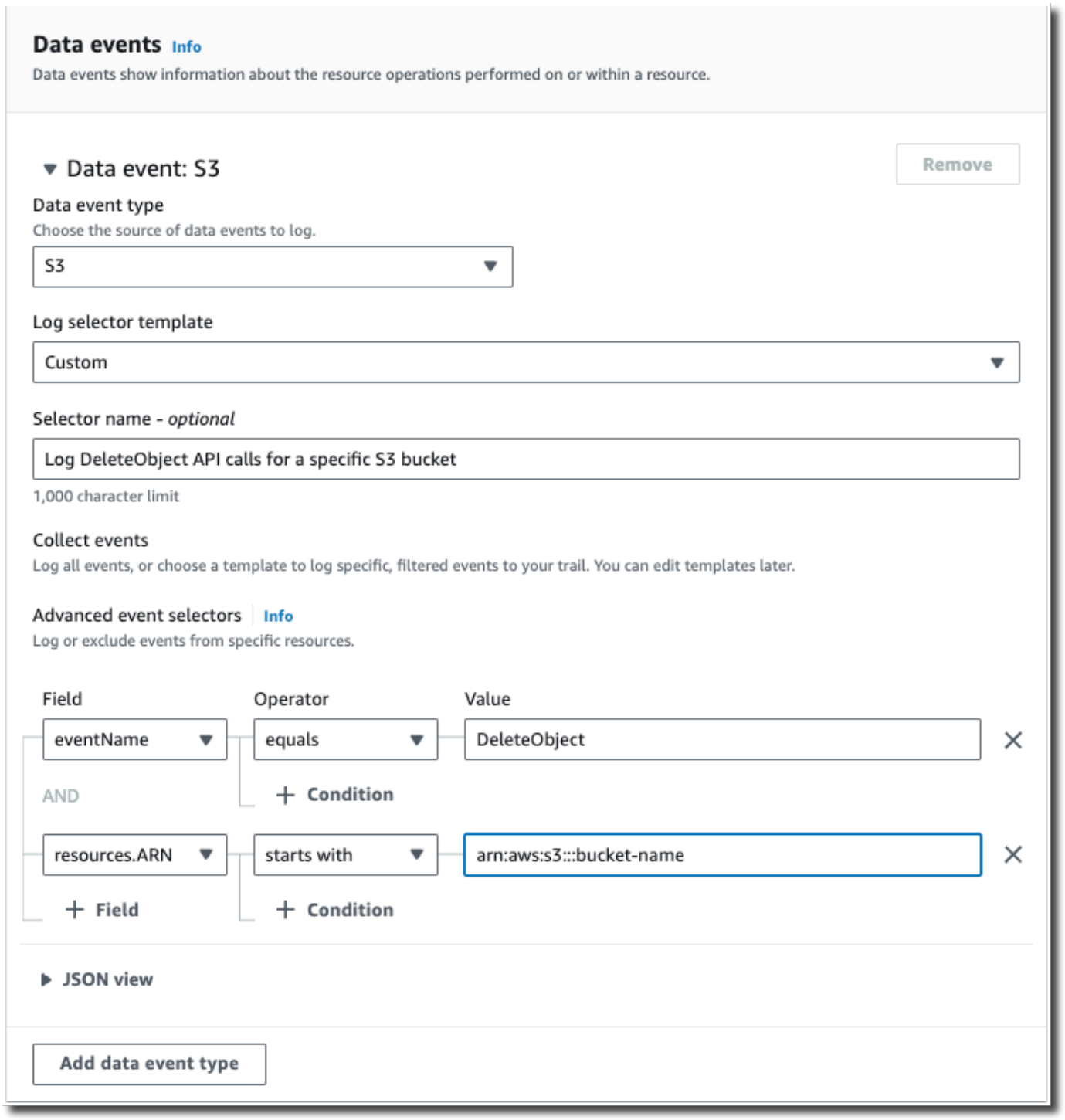
    c. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選取器的描述性名稱，例如「特定 S3 儲存貯體的記錄 DeleteObject API 呼叫」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。



d. 在高級事件選擇器中，我們將構建自定義事件選擇器以對`eventName`和`resources.ARN`字段進行過濾。事件資料存放區的進階事件選取器與套用於追蹤的進階事件選取器所運作的方式相同。如需建立進階事件選取器的詳細資訊，請參閱使用進階事件選取器記錄資料事件。

   i. 對於欄位，選擇 eventName。對於運算子，選擇 equals。針對數值，輸入 **`DeleteObject`**。選擇 [+ 欄位] 以篩選另一個欄位。

   ii. 對於欄位，選擇 resources.ARN。對於「運算子」，選擇StartsWith。對於值，輸入您的儲存貯體的 ARN (例如 *`arn:aws:s3:::bucket-name`*)。如需有關如何取得 ARN 的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 資源。



17. 選擇 Next (下一步) 以檢閱您的選項。
18. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
19. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

從此開始，事件資料存放區將擷取與其進階事件選取器相符的事件。建立事件資料存放區之前發生的事件，不會儲存在事件資料存放區中，除非您選擇複製現有追蹤事件。

您現在可以對您的事件資料存放區執行查詢。如需有關如何檢視和執行範例查詢的資訊，請參閱 檢視和執行 CloudTrail 湖泊範例查詢。

將追蹤事件複製到 CloudTrail Lake 事件資料存放區

本逐步解說說明如何將追蹤事件複製到新的 CloudTrail Lake 事件資料倉庫以進行歷史分析。如需有關複製追蹤事件的詳細資訊，請參閱 將追蹤事件複製到事件資料存放區。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

將追蹤事件複製到 CloudTrail Lake 事件資料存放區時，會根據事件資料存放區擷取的未壓縮資料量產生費用。

將追蹤事件複製到 CloudTrail Lake 時，會 CloudTrail 解壓縮以 gzip (壓縮) 格式儲存的記錄檔，然後將記錄中包含的事件複製到事件資料存放區。未壓縮資料的大小可能大於實際的 S3 儲存大小。若要取得未壓縮資料大小的一般估計值，您可以將 S3 儲存貯體中的日誌大小乘以 10。

您可以縮小指定的複製事件的時間範圍，來降低該費用。如果您計劃只使用事件資料存放區來查詢複製的事件，可以關閉事件擷取以避免因未來事件而產生費用。如需有關成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

若要將追蹤事件複製到新的事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在「設定事件資料存放區」頁面的「一般」詳細資料中，為您的事件資料存放區命名，例如*my-management-events-eds*。根據最佳實務，請使用可快速識別事件資料存放區目的的名稱。如需 CloudTrail 命名需求的資訊，請參閱命名要求。

5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

   > **Note**
   >
   > 如果您要 CloudTrail 將追蹤事件複製到此事件資料存放區，如果事件早於指定的保留期間，`eventTime`則不會複製該事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*)。例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。

7. (選用) 在加密中，選擇您是否想要使用自己的 KMS 金鑰加密事件資料存放區。依預設，事件資料存放區中的所有事件都會 CloudTrail 使用為您 AWS 擁有和管理的 KMS 金鑰加密。

   若要啟用使用您自己的 KMS 金鑰加密，請選擇使用我自己的 AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail 記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail

還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

> **Note**
>
> 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的事件資料存放區。標籤可協助您識別 CloudTrail 事件資料存放區。例如，您可以附加名稱為 **`stage`**，值為 **`prod`** 的標籤。您可以使用標籤來限制對事件資料存放區的存取。您還可以使用標籤來追蹤事件資料存放區的查詢和擷取成本。

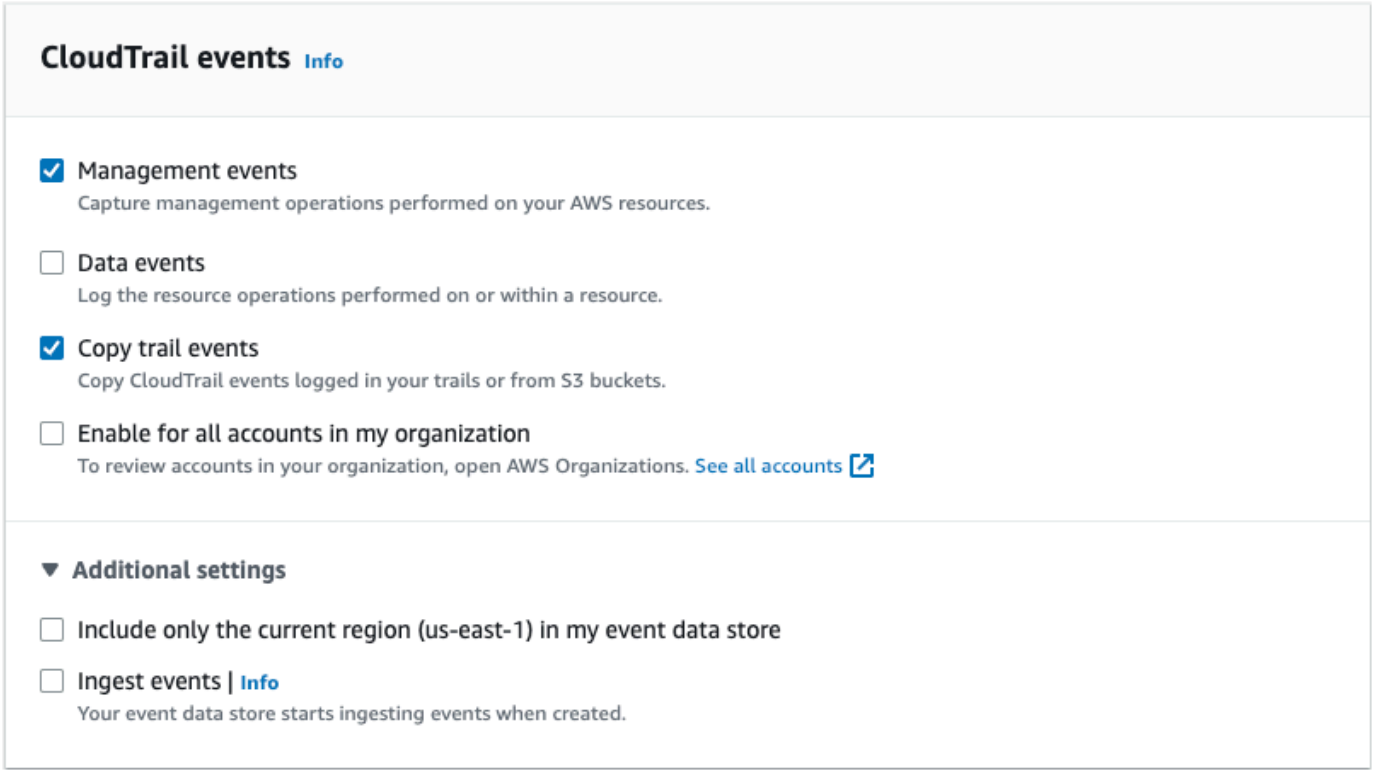
   如需有關如何使用標籤追蹤成本的資訊，請參閱 為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置。如需有關如何使用 IAM 政策，對以標籤為基礎的事件資料存放區授予存取權的資訊，請參閱 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱《標記資 AWS 源使用指南》中的〈標記 AWS 資源〉。

10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在選擇事件頁面上，保留事件類型的預設選項。

12. 對於CloudTrail 活動，我們將保留選取管理事件，然後選擇「複製追蹤事件」。在此範例中，我們不關心事件類型，因為我們只使用事件資料存放區來分析過往事件，而不會擷取未來事件。

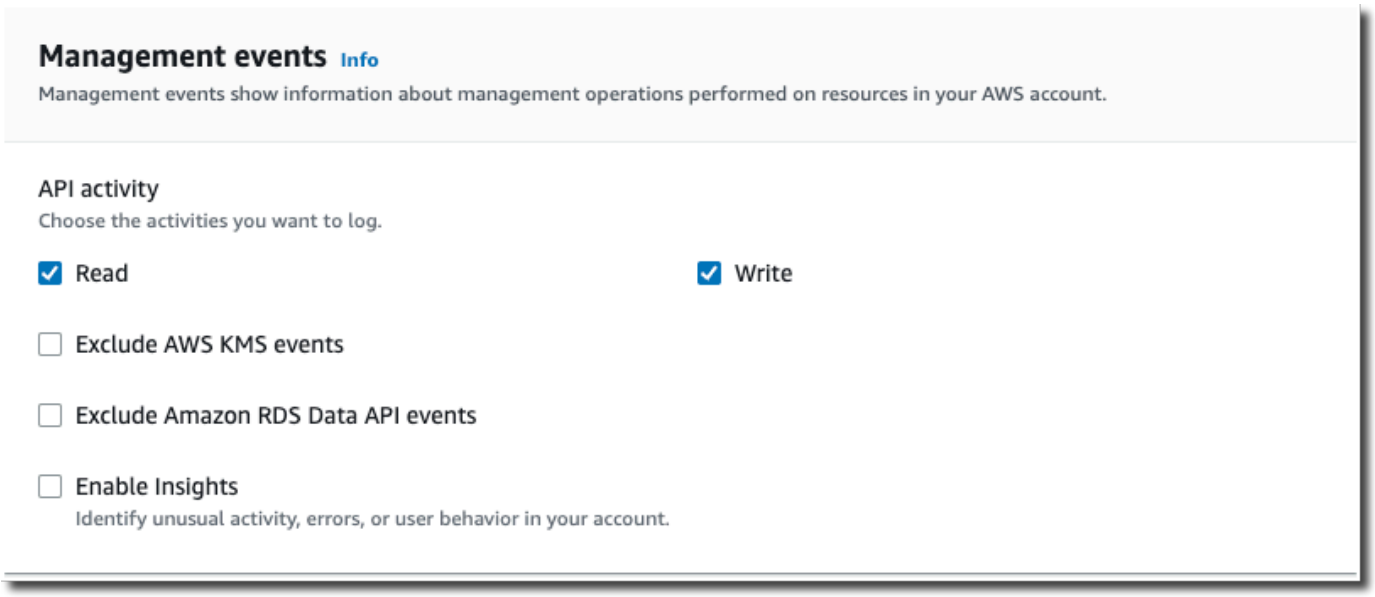
如果您要建立事件資料存放區來取代現有的追蹤，選擇與追蹤相同的事件選取器，以確保事件資料存放區有相同的事件涵蓋範圍。



13. 如果這是組織事件資料存放區，選擇針對組織中的所有帳戶啟用。除非您已在 AWS Organizations 中設定帳戶，否則此選項將無法變更。

> **Note**
>
> 如果要建立組織事件資料存放區，您必須使用組織的管理帳戶登入，因為只有管理帳戶可以將追蹤事件複製到組織事件資料存放區。

14. 對於其他設定，我們將取消選取擷取事件，因為在此範例中，我們不希望事件資料存放區擷取任何未來事件，而且我們只對查詢複製的事件感興趣。依預設，事件資料存放區會為所有人收集事件，AWS 區域 並在建立事件時開始擷取事件。
15. 對於管理事件，我們將保留預設設定。



16. 在複製追蹤事件區域中，完成下列步驟。

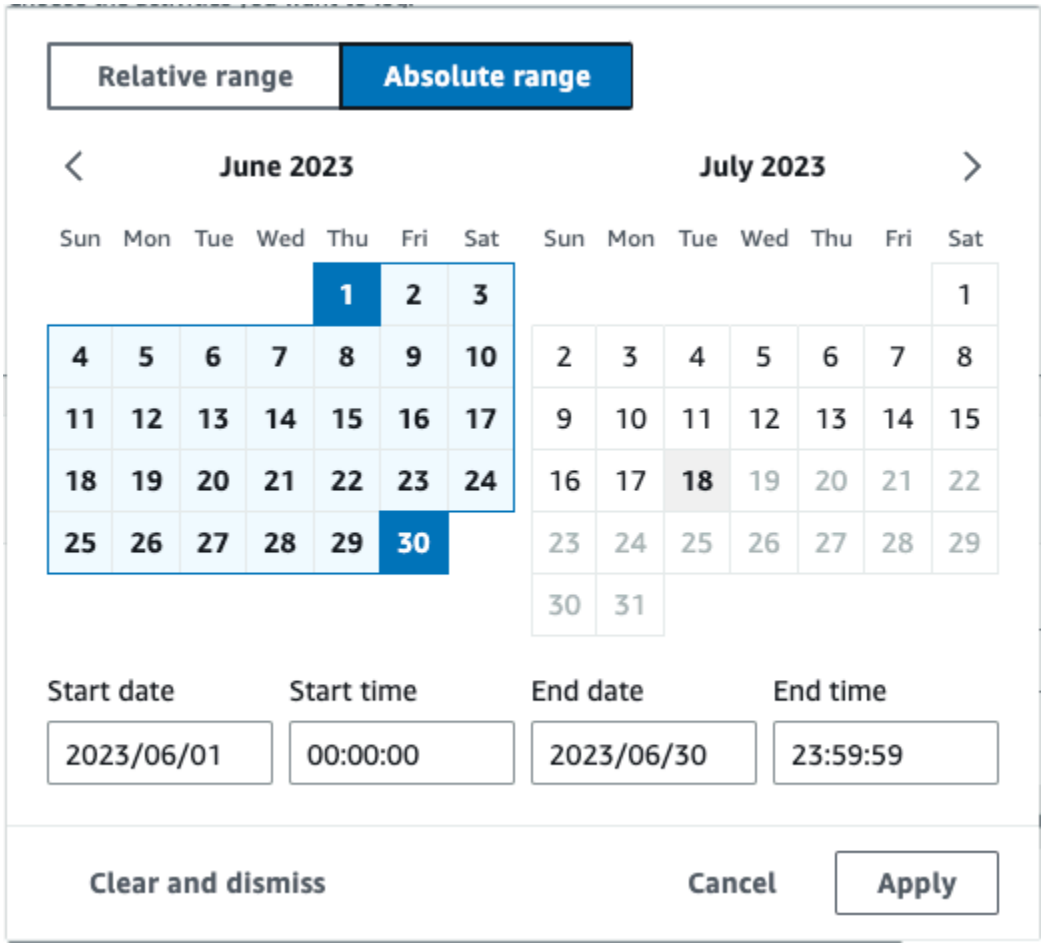
    a. 選擇您要複製的追蹤。在此範例中，我們將選擇名為 *management-events* 的追蹤。

    根據預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前綴。如果您要複製其他前置詞中包含的 CloudTrail 事件，請選擇 [輸入 S3 URI]，然後選擇 [瀏覽 S3] 以瀏覽至首碼。如果追蹤的來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策 CloudTrail 允許解密資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策， CloudTrail 以允許解密儲存貯體中的資料。如需更新 KMS 金鑰政策的詳細資訊，請參閱 用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策。

    b. 選擇複製事件的時間範圍。 CloudTrail 在嘗試複製追蹤事件之前，先檢查字首和記錄檔名稱，以確認名稱包含在所選開始日期與結束日期之間的日期。您可以選擇 Relative range (相對範圍) 或 Absolute range (絕對範圍)。若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請選擇早於事件資料存放區建立日期的時間範圍。

    - 如果您選擇「相對範圍」，則可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。 CloudTrail 複製所選期間內記錄的事件。
    - 如果選擇「絕對範圍」，則可以選擇特定的開始和結束日期。 CloudTrail 複製所選開始日期和結束日期之間發生的事件。

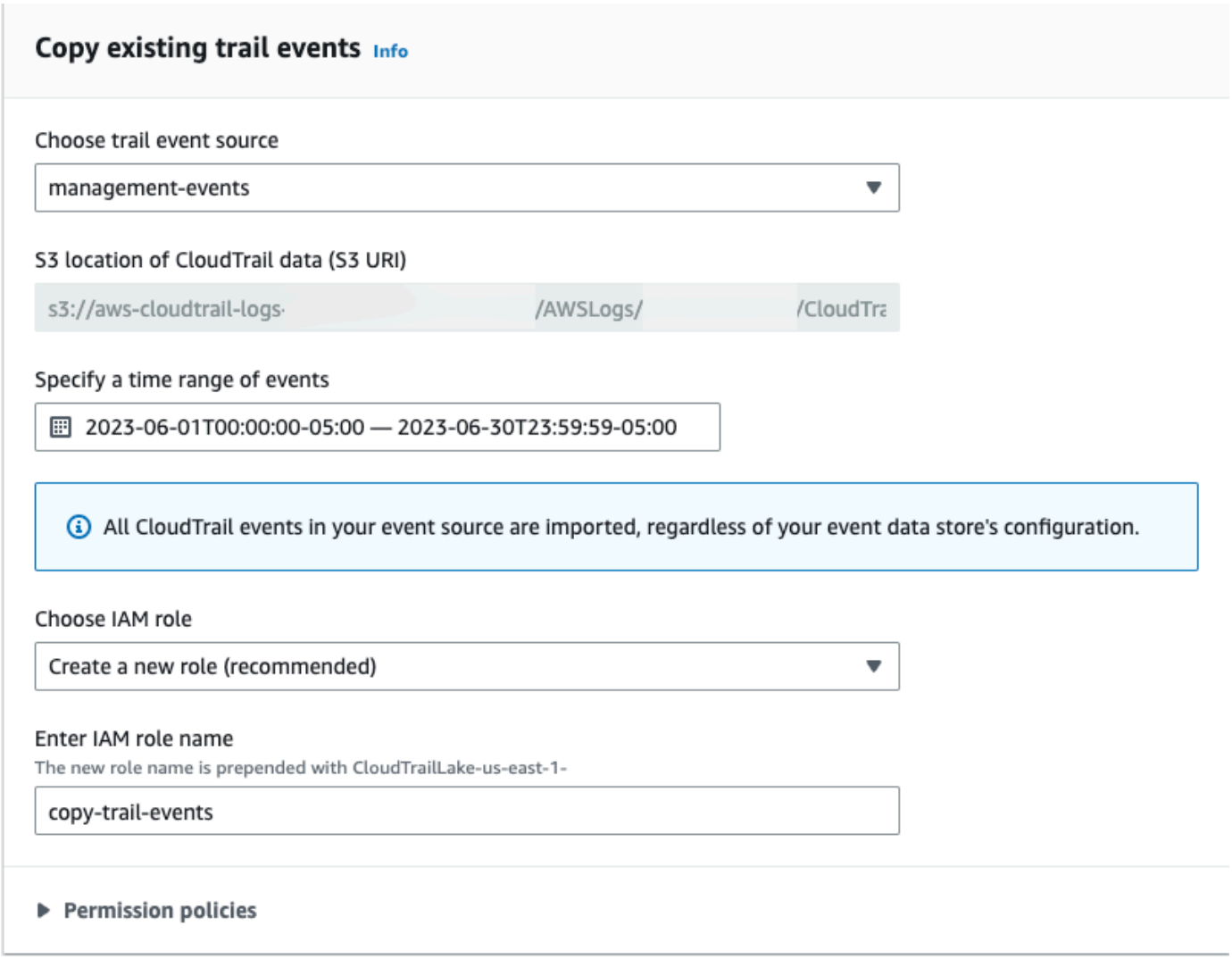
    在此範例中，我們將選擇絕對範圍，然後選取整個六月份。



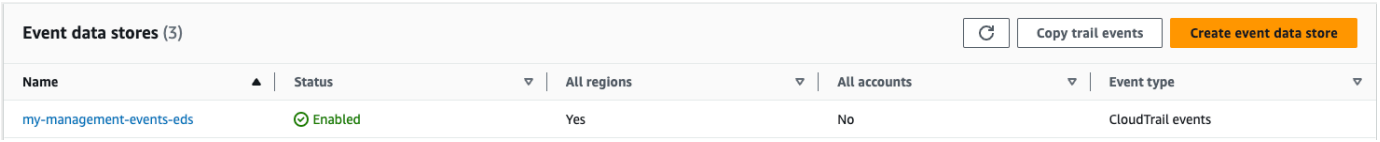
c. 對於 Permissions (許可)，從下列 IAM 角色選項中選擇。如果您選擇現有的 IAM 角色，請確認 IAM 角色政策提供必要的許可。如需更新 IAM 角色許可的詳細資訊，請參閱[複製追蹤事件的 IAM 許可]。

- 選擇 Create a new role (recommended) (建立新角色 (建議使用)) 以建立新的 IAM 角色。在「輸入 IAM 角色名稱」中，輸入角色的名稱。 CloudTrail會自動為此新角色建立必要的權限。
- 選擇「使用自訂 IAM 角色 ARN」以使用未列出的自訂 IAM 角色。對於 Enter IAM role ARN (輸入 IAM 角色 ARN)，輸入 IAM ARN。
- 從下拉式清單中選擇現有的 IAM 角色。

在此範例中，我們將選擇建立新角色 (建議)，並命名為 **`copy-trail-events`**。

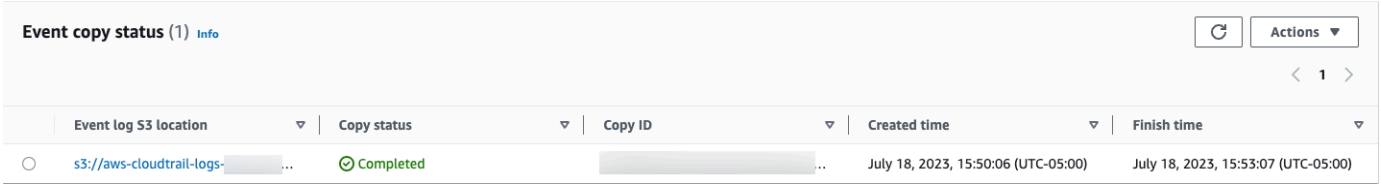


17. 選擇 Next (下一步) 以檢閱您的選項。
18. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
19. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

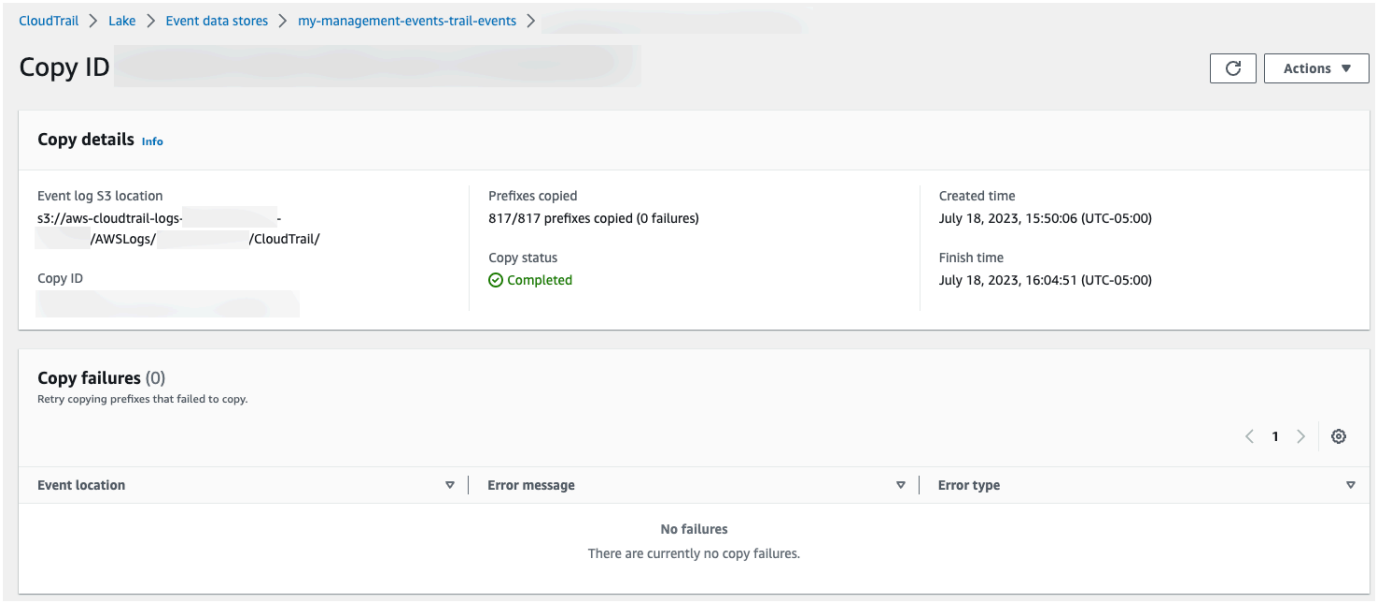


20. 選擇事件資料存放區名稱，以檢視其詳細資訊頁面。詳細資訊頁面顯示您的事件資料存放區的詳細資訊以及複製狀態。事件複製狀態顯示在事件複製狀態區域中。

    追蹤事件複製完成時，如果沒有錯誤，則其 Copy status (複製狀態) 設定為 Completed (完成)；如果發生錯誤，則設定為 Failed (失敗)。



21. 若要檢視有關複製的詳細資訊，請在事件日誌 S3 位置欄中選擇複製名稱，或者選擇動作選單中檢視詳細資訊選項。如需檢視追蹤事件複製之詳細資訊，請參閱 事件複製詳細資訊。



22. 複製失敗區域會顯示複製追蹤事件時發生的任何錯誤。如果 Copy status (複製狀態) 是 Failed (失敗)，修正 Copy failures (複製失敗) 中顯示的任何錯誤，接著選擇 Retry copy (重試複製)。當您重試副本時，會在發生失敗的位置 CloudTrail 繼續複製。

檢視 CloudTrail 湖泊儀表板

本逐步解說說明如何檢視 CloudTrail Lake 儀表板。CloudTrailLake 儀表板可讓您以視覺化方式呈現事件資料存放區中的事件，並查看趨勢，例如熱門使用者和最常見的錯誤。

每個儀表板均包含多個小工具，每個小工具代表一個 SQL 查詢。若要填入儀表板，請 CloudTrail 執行系統產生的查詢。查詢會依據掃描的資料量而產生費用。

> **Note**
>
> 目前，儀表板僅適用於收集 CloudTrail管理事件、Amazon S3 資料事件和見解事件的事件資料存放區。

若要檢視 Lake 儀表板

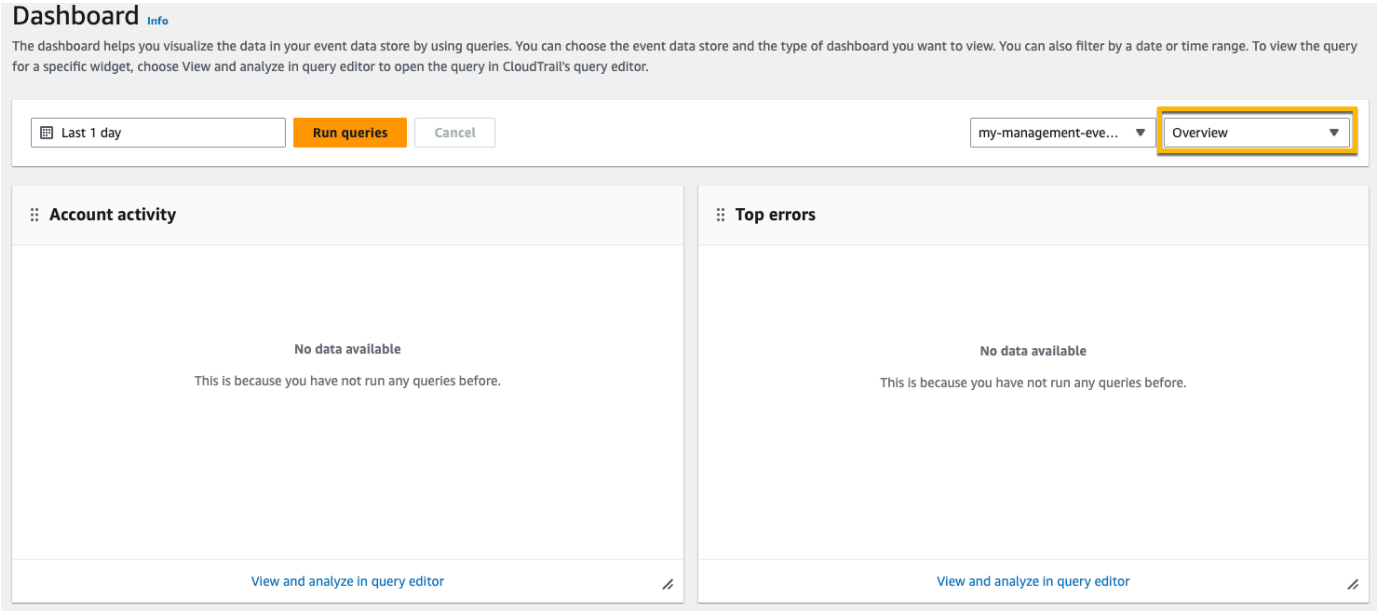
1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的儀表板。
3. 第一次檢視「儀表板」頁面時， CloudTrail 會要求您確認與執行查詢相關的成本。選擇我同意以確認執行查詢的相關費用。您只需確認一次。如需有關 CloudTrail 定價的詳細資訊，請參閱CloudTrail定價。
4. 在清單中選擇您的事件資料存放區，然後選擇您想要檢視的儀表板類型。

   下列是可能的儀表板類型。

   - 概觀控制面板-顯示最活躍的使用者 AWS 區域，以及 AWS 服務 按事件計數。您還可以檢視有關 `read` 和 `write` 管理事件活動、最常調節事件和常見錯誤的資訊。此儀表板適用於收集管理事件的事件資料存放區。
   - 管理事件儀表板 - 依使用者顯示主控台登入事件、存取遭拒事件、破壞性動作和常見錯誤。您還可以檢視有關 TLS 版本以及使用者的過期 TLS 呼叫的資訊。此儀表板適用於收集管理事件的事件資料存放區。
   - S3 資料事件儀表板 - 顯示 S3 帳戶活動、最常存取的 S3 物件、最常用的 S3 使用者和最常執行的 S3 動作。此儀表板適用於收集 Amazon S3 資料事件的事件資料存放區。
   - Insights 事件儀表板 - 依 Insights 類型顯示 Insights 事件的總體比例，依最常使用的使用者和服務的 Insights 類型顯示 Insights 事件的比例，以及顯示每天的 Insights 事件數量。此儀表板還包含一個小工具，可列出最多 30 天的 Insights 事件。它僅適用於收集 Insights 事件的事件資料存放區。

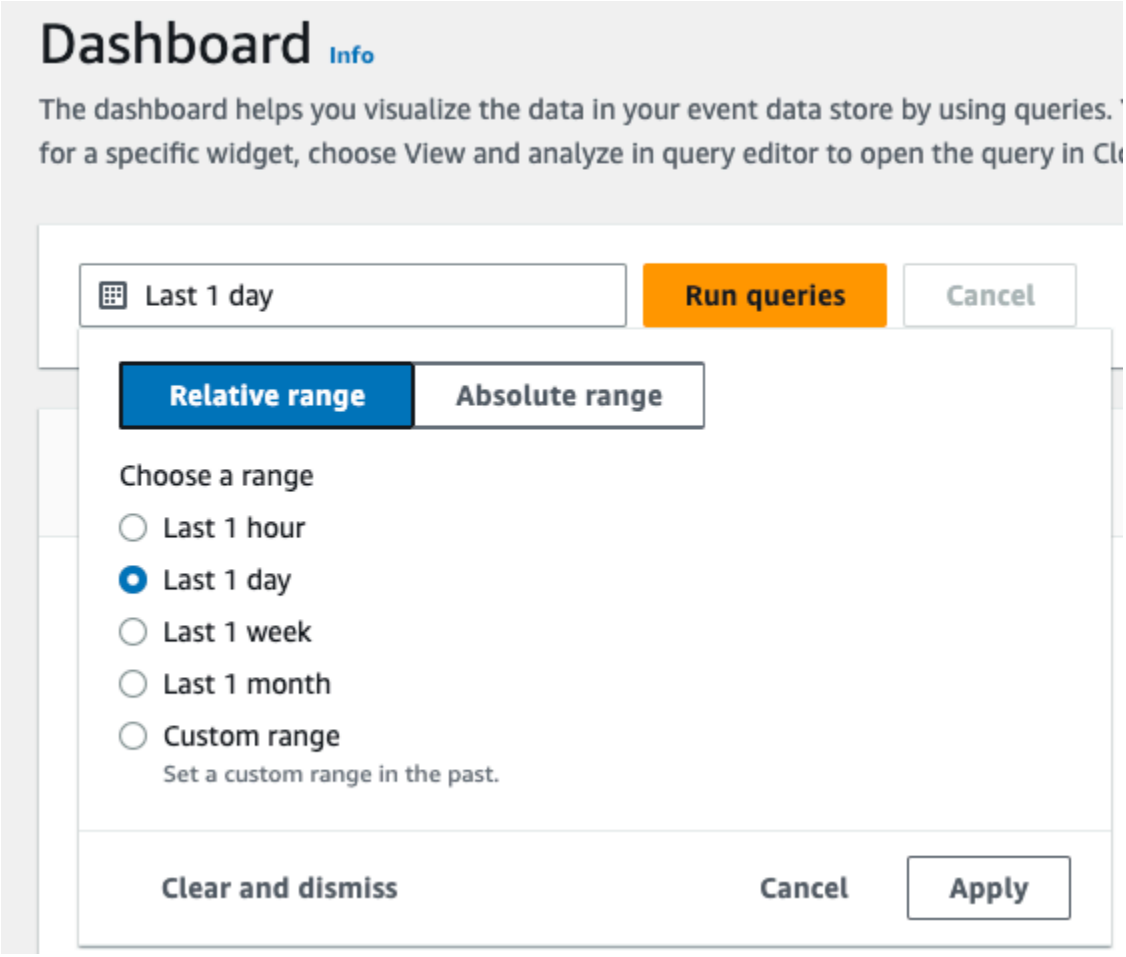
   > **Note**
   >
   > - 在來源事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天才能傳遞第一個 Insights 事件。如需詳細資訊，請參閱 了解 Insights 事件傳遞。
   > - Insights 事件儀表板僅顯示由所選事件資料存放區收集的 Insights 事件的相關資訊，這取決於來源事件資料存放區的組態。例如，如果您設定來源事件資料存放區啟用 `ApiCallRateInsight` 的 Insights 事件，而不啟用 `ApiErrorRateInsight` 的 Insights 事件，您將不會看到有關 `ApiErrorRateInsight` 的 Insights 事件的資訊。

在此範例中，我們會選擇概觀儀表板。



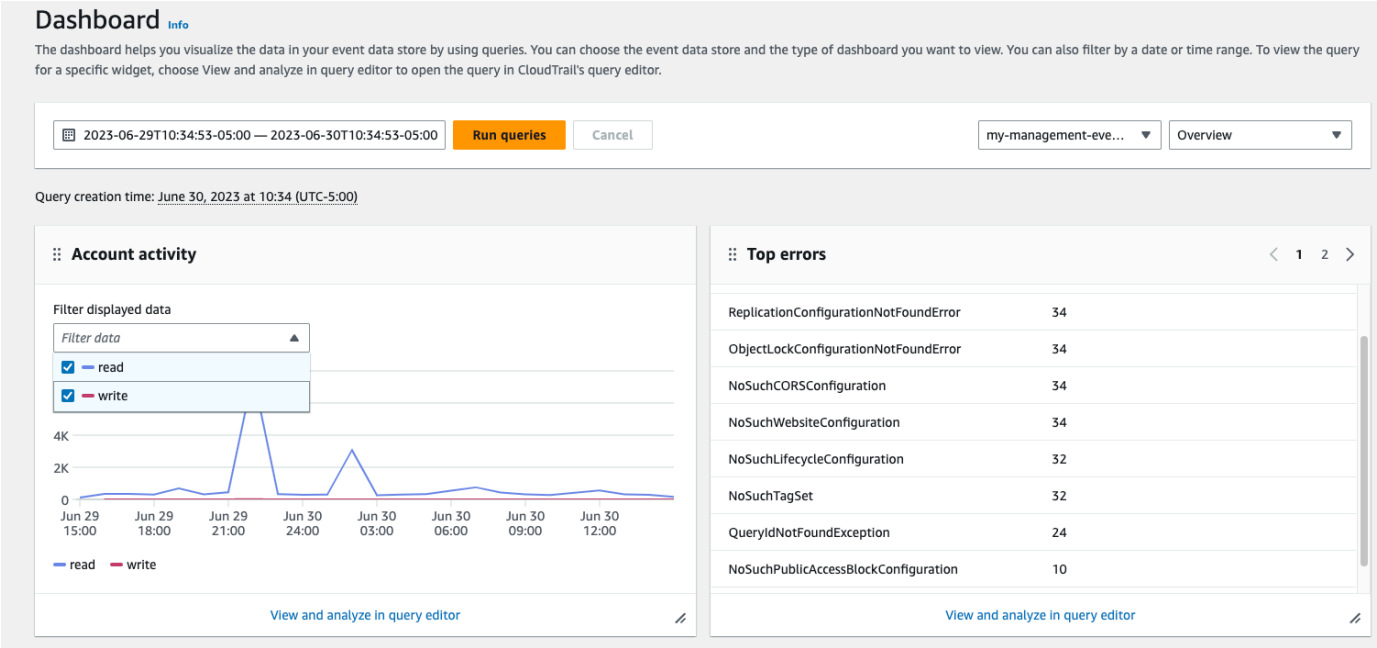
5. 選擇日期欄位以篩選時間範圍，然後選擇套用。選擇絕對範圍以選取特定的日期和時間範圍。選擇相對範圍以選取預先定義的時間範圍或自訂範圍。依預設，儀表板會顯示過去 24 小時的事件資料。

> **Note**
>
> 由於 CloudTrail 查詢是根據掃描的資料量計費，因此您可以透過篩選較窄的時間範圍來降低成本。

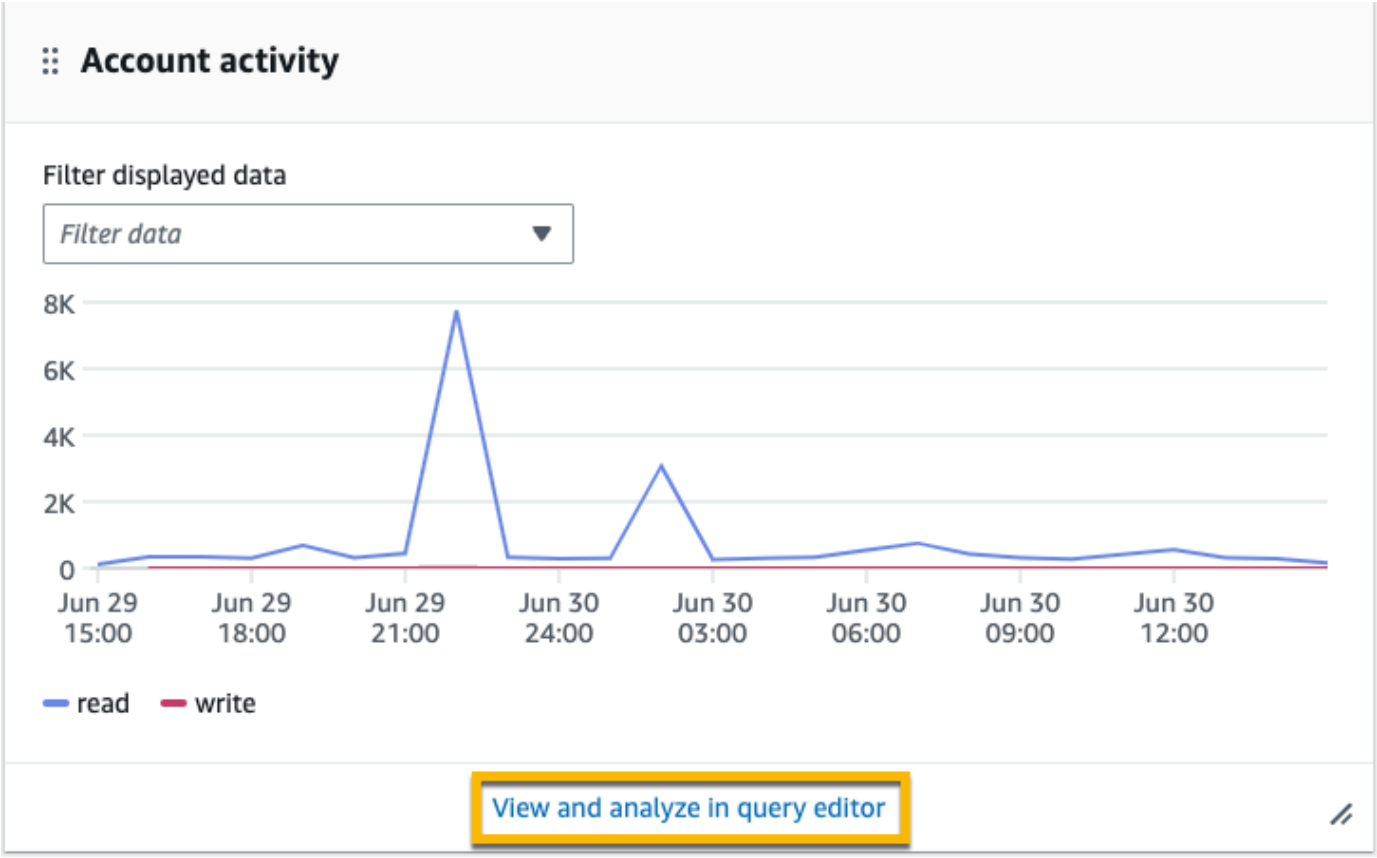


6. 選擇執行查詢以填入儀表板。每個小工具都會單獨顯示其關聯查詢的狀態，並在查詢完成時顯示資料。

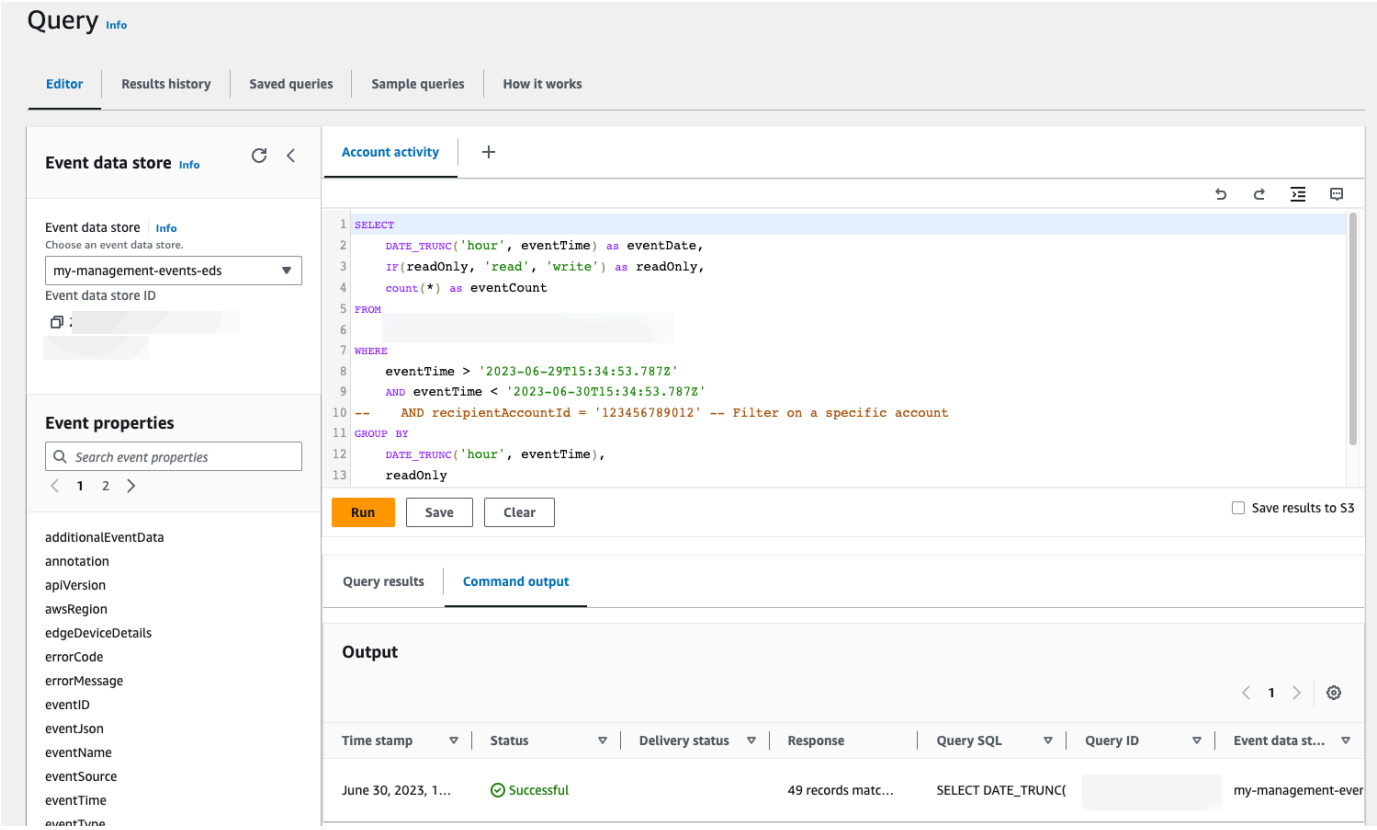
   您可以在一些小工具上執行更多篩選，例如帳戶活動，它讓您可以篩選 `read` 和 `write` 事件活動。



7. 若要檢視某個小工具的查詢，請選擇在查詢編輯器中檢視並分析。



在查詢編輯器中選擇 [檢視和分析] 會在 CloudTrail Lake 的查詢編輯器中開啟查詢，讓您進一步分析儀表板外部的查詢結果。如需有關編輯查詢的詳細資訊，請參閱 建立或編輯查詢。如需有關執行查詢和儲存查詢結果的詳細資訊，請參閱 執行查詢並儲存查詢結果。



如需有關儀表板的詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

檢視和執行 CloudTrail 湖泊範例查詢

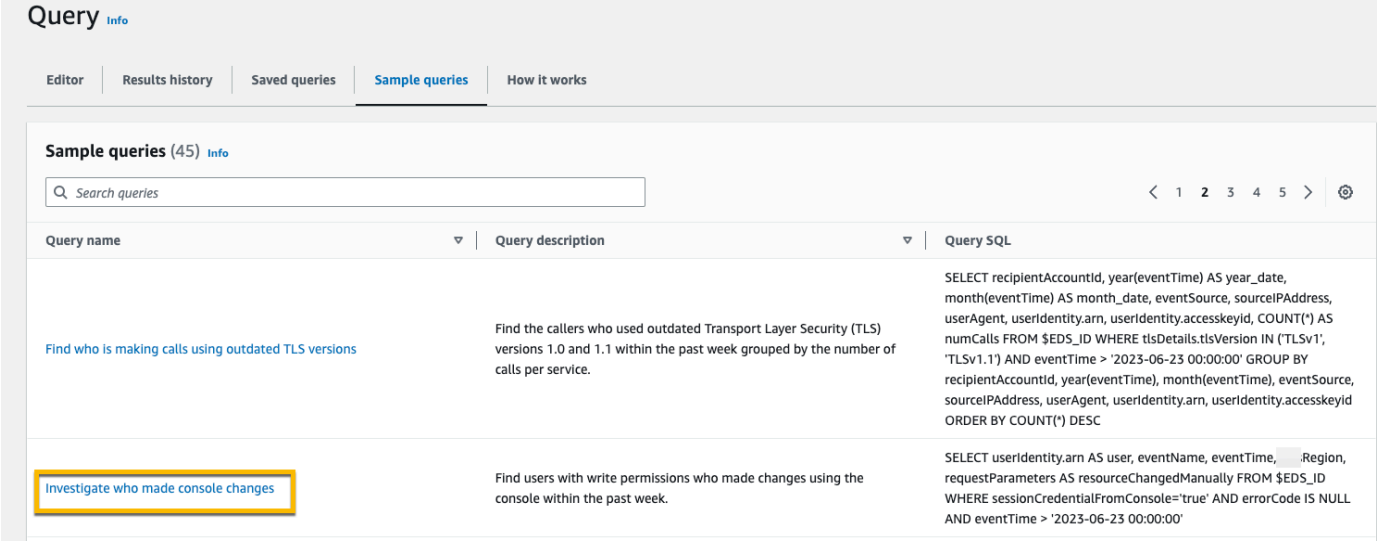
CloudTrail Lake 提供了許多範例查詢，可協助您開始撰寫自己的查詢。本逐步解說說明如何選取和執行範例查詢。

CloudTrail 查詢會根據掃描的資料量產生費用。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

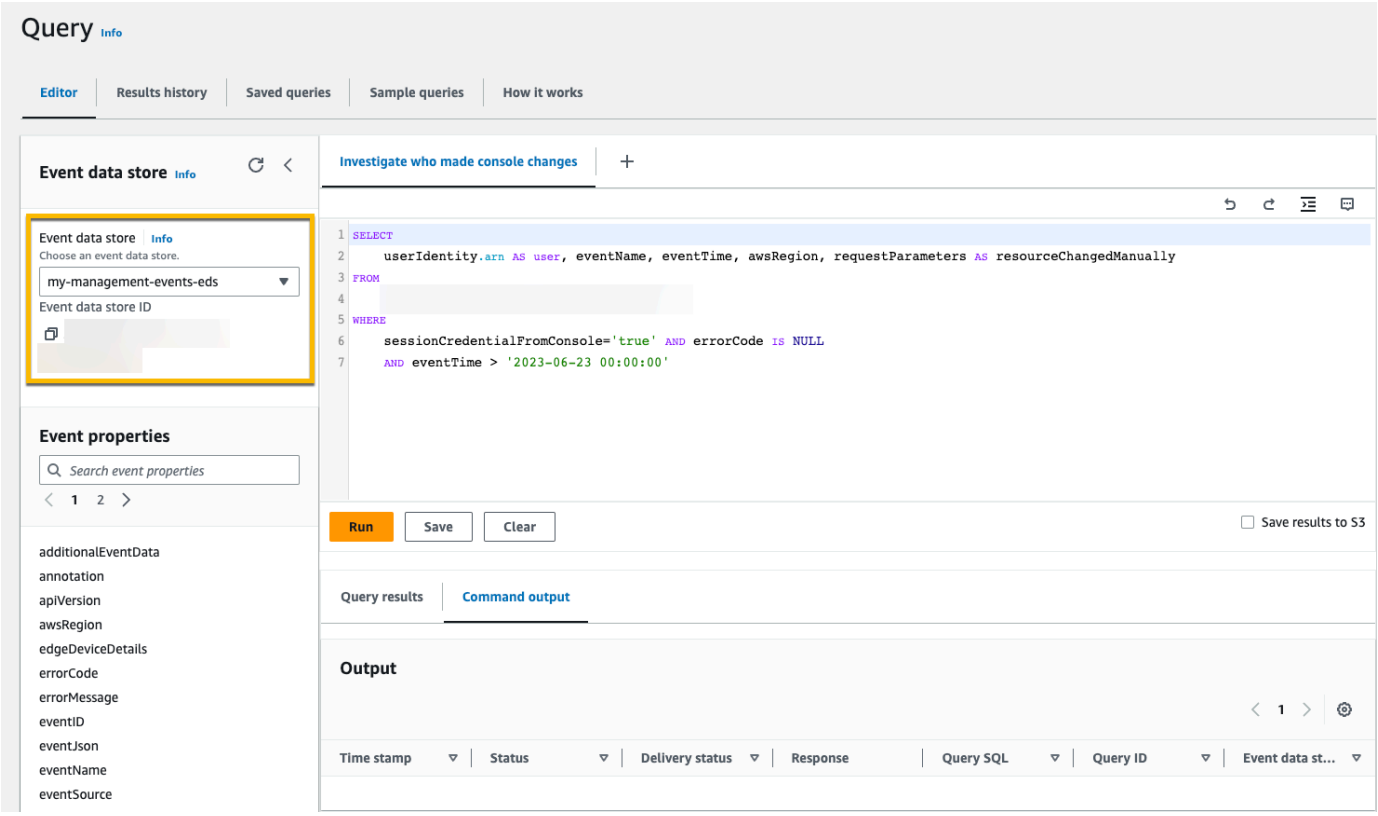
若要檢視與執行範例查詢

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。

2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在 Query (查詢) 頁面上，選擇 Sample queries (範例查詢) 索引標籤。
4. 在清單中選擇一個範例查詢，或者搜尋查詢以篩選清單。在此範例中，我們將透過選擇查詢名稱打開查詢調查誰變更了主控台。這會在 Editor (編輯器) 索引標籤中開啟查詢。

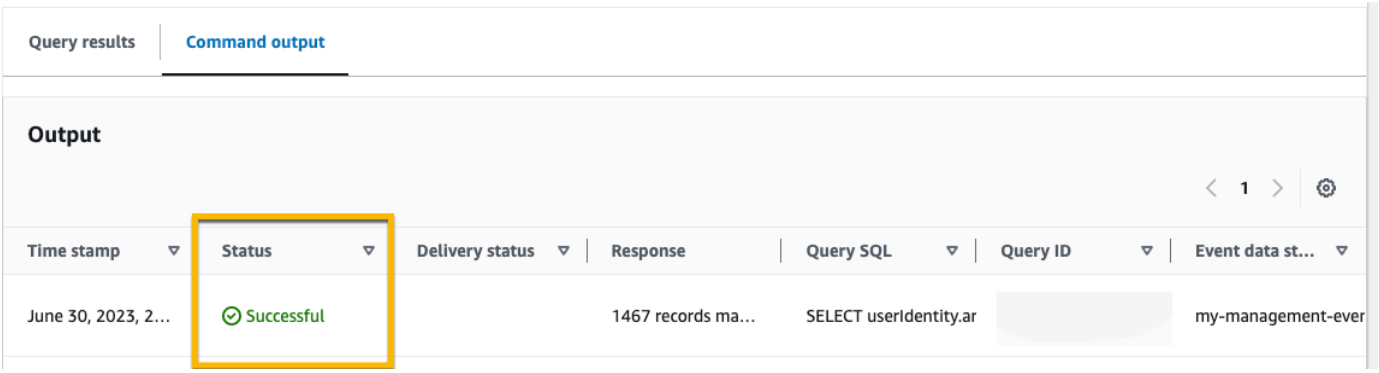


5. 在編輯器索引標籤上，選擇您想要為哪個事件資料存放區執行查詢。當您從清單中選擇事件資料倉庫時， CloudTrail 會自動將事件資料存放區 ID 填入查詢編輯器的FROM行中。

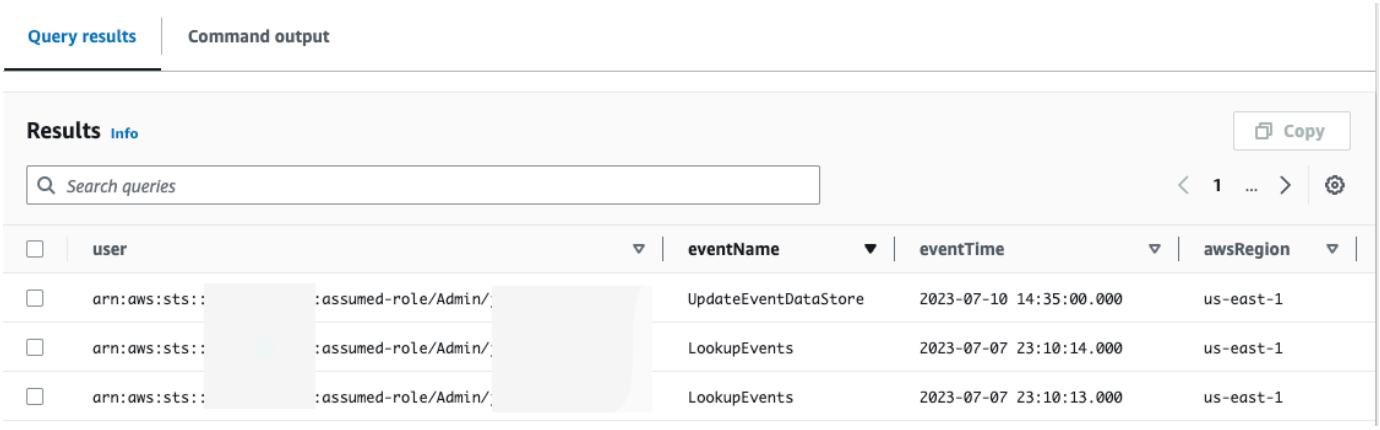


6. 選擇執行以執行查詢。

命令輸出索引標籤顯示您的查詢的相關中繼資料，例如查詢是否成功，相符的記錄數目，以及查詢的執行事件。



查詢結果索引標籤顯示所選事件資料存放區中與您的查詢相符的事件資料。



如需有關編輯查詢的詳細資訊，請參閱 建立或編輯查詢。如需有關執行查詢和儲存查詢結果的詳細資訊，請參閱 執行查詢並儲存查詢結果。

將 CloudTrail 湖泊查詢結果儲存至 S3 儲存貯體

本逐步解說說明如何將 CloudTrail Lake 查詢結果儲存至 S3 儲存貯體，然後下載這些查詢結果。

在 CloudTrail Lake 中執行查詢時，會根據查詢掃描的資料量產生費用。將查詢結果儲存到 S3 儲存貯體不會產生額外的 CloudTrail Lake 費用，不過需支付 S3 儲存費用。如需 S3 定價的詳細資訊，請參閱 Amazon S3 定價。

儲存查詢結果時，查詢結果可能會在 S3 儲存貯體中檢視之前顯示在 CloudTrail 主控台中，因為查詢掃描完成後會 CloudTrail 傳送查詢結果。雖然大多數查詢會在幾分鐘內完成，但視事件資料存放區的大小而定，將查詢結果傳遞 CloudTrail 到 S3 儲存貯體可能需要相當長的時間。 CloudTrail 以壓縮的

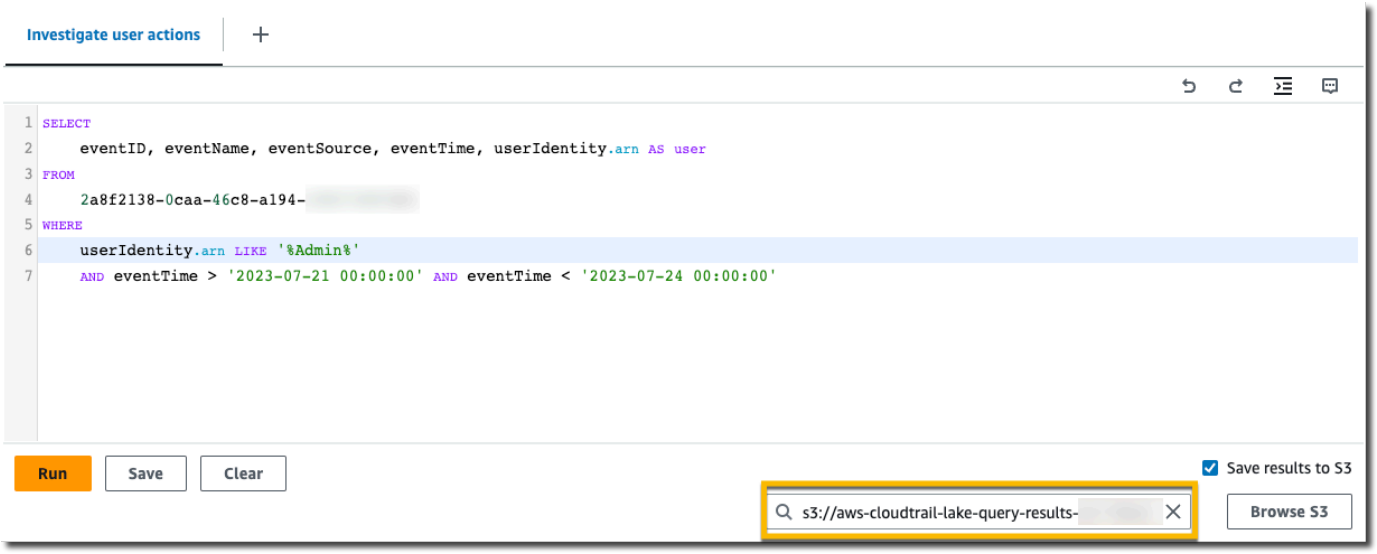
gzip 格式將查詢結果傳送至 S3 儲存貯體。平均而言，查詢掃描完成後，每傳遞 1 GB 的資料到 S3 儲存貯體，可能會有 60 到 90 秒的延遲。

若要將查詢結果儲存至 Amazon S3 儲存貯體

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在範例查詢或已儲存的查詢索引標籤上，選擇查詢名稱以選擇要執行的查詢。在此範例中，我們將選擇名為調查使用者動作的範例查詢。
4. 在 Editor (編輯器) 索引標籤，針對 Event data store (事件資料存放區)，從下拉式清單中選擇事件資料存放區。當您從清單中選擇事件資料倉庫時， CloudTrail 會自動在該`From`行中填入事件資料倉庫 ID。
5. 在此範例查詢中，我們將編輯 `userIdentity.ARN` 值以指定名為 Admin 的使用者，然後我們將保留 `eventTime` 的預設值。執行查詢時，您將為掃描的資料量支付費用。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。

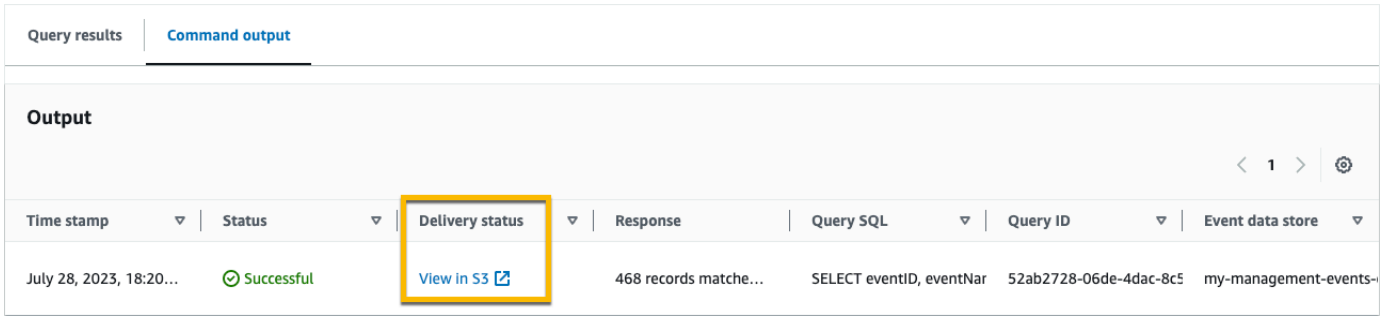
6. 選擇將結果儲存至 S3，以便將查詢結果儲存至 S3 儲存貯體。選擇預設 S3 儲存貯體時， CloudTrail 會建立並套用所需的儲存貯體政策。如果您選擇預設 S3 儲存貯體，您的 IAM 政策需要包含`s3:PutEncryptionConfiguration`動作的權限，因為預設情況下會為儲存貯體啟用伺服器端加密。如需有關儲存查詢結果的詳細資訊，請參閱已儲存查詢結果的其他相關資訊。在此範例中，我們使用預設的 S3 儲存貯體。

> **Note**
>
> 若要使用不同的儲存貯體，請指定儲存貯體名稱，或選擇 Browse S3 (瀏覽 S3) 以選擇儲存貯體。值區政策必須授 CloudTrail 予將查詢結果傳遞給值區的權限。如需手動編輯儲存貯體政策的資訊，請參閱「CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策」。

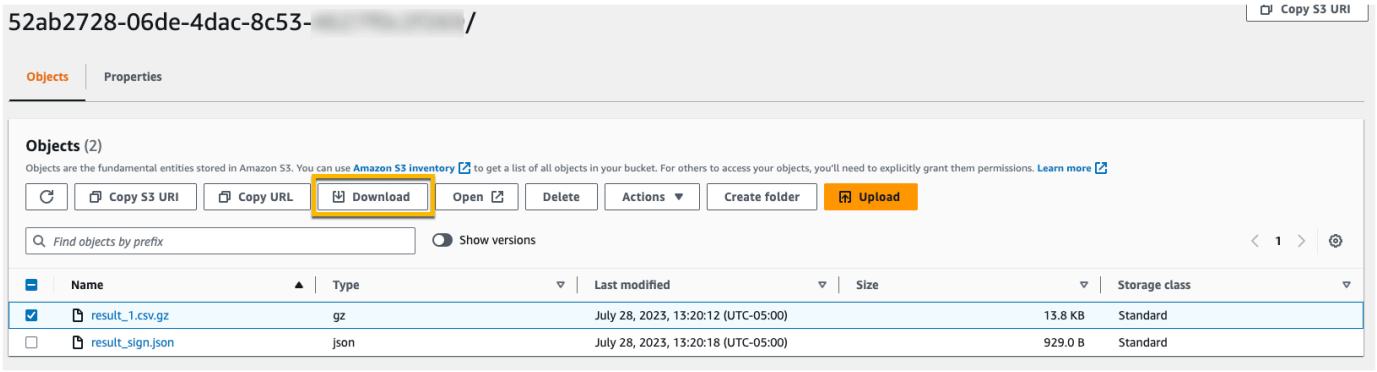


7. 選擇執行。根據事件資料存放區的大小及其中包含的資料天數，查詢可能需要幾分鐘才能執行。所以 Command output (命令輸出) 索引標籤會顯示查詢的狀態，以及查詢是否已完成執行。查詢完成執行後，開啟 Query results (查詢結果) 索引標籤查看作用中查詢 (目前編輯器中顯示的查詢) 的結果表格。
8. CloudTrail 完成將儲存的查詢結果交付到 S3 儲存貯體時，[交付狀態] 欄會提供 S3 儲存貯體的連結，該儲存貯體包含已儲存的查詢結果檔案，以及可用來驗證已儲存查詢結果的簽署檔案。選擇在 S3 中檢視，在 S3 儲存貯體中檢視查詢結果檔案和簽署檔案。

> **Note**
>
> 當您儲存查詢結果時，查詢結果可能會在 S3 儲存貯體中檢視之前顯示在 CloudTrail 主控台中，因 CloudTrail 為查詢掃描完成後會傳送查詢結果。雖然大多數查詢會在幾分鐘內完成，但視事件資料存放區的大小而定，將查詢結果傳遞 CloudTrail 到 S3 儲存貯體可能需要相當長的時間。 CloudTrail 以壓縮的 gzip 格式將查詢結果傳送至 S3 儲存貯體。平均而言，查詢掃描完成後，每傳遞 1 GB 的資料到 S3 儲存貯體，可能會有 60 到 90 秒的延遲。



9. 若要下載您的查詢結果，選擇查詢結果檔案 (在此範例中為 `result_1.csv.gz`)，然後選擇下載。



如需有關驗證已儲存查詢結果的資訊，請參閱 [驗證已儲存查詢結果]。

以下列方式檢視 CloudTrail 成本和用量 AWS Cost Explorer

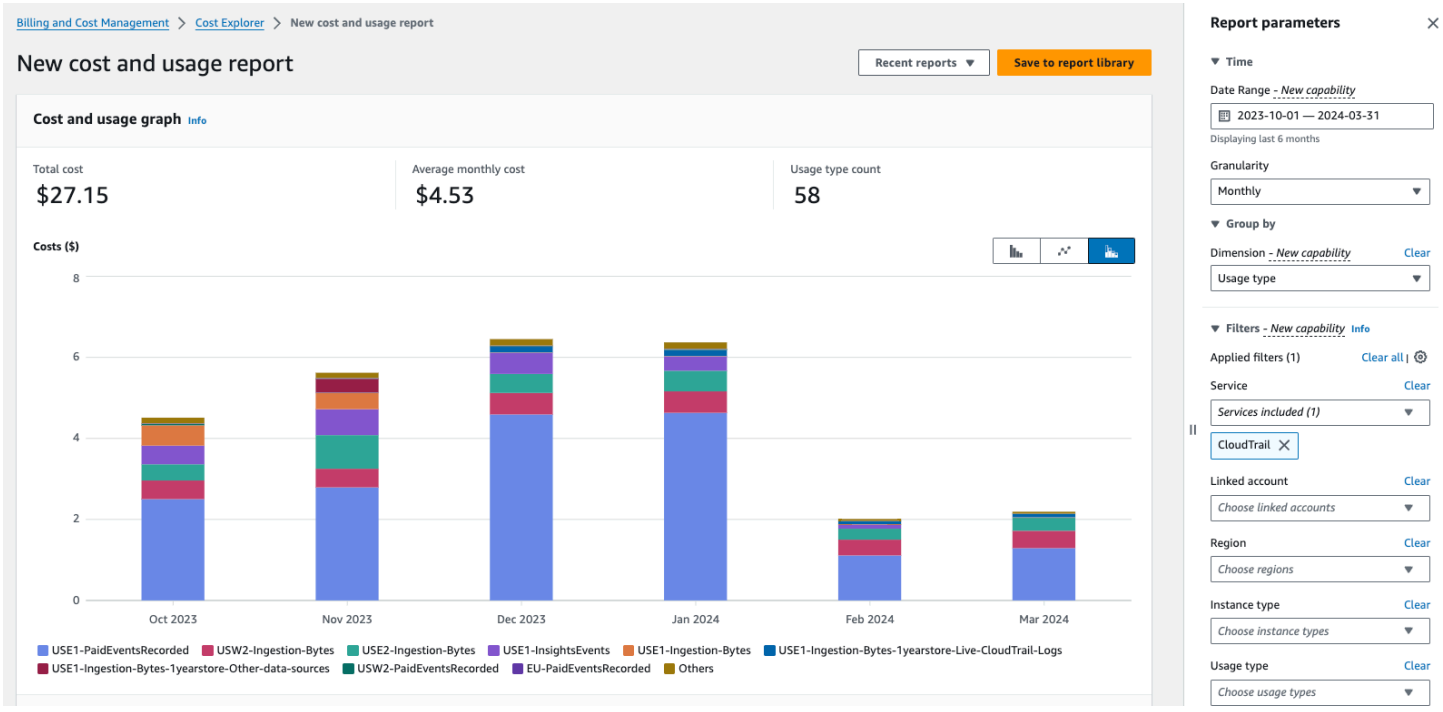
本節說明如何使用檢視 CloudTrail 成本和用量AWS Cost Explorer。Cost Explorer 讓您能夠視覺化、瞭解並管理一段時間內的 AWS 成本和用量。

如需 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

若要使用 CloudTrail Cost Explorer 檢視成本和使用量

1. 登入 AWS Management Console 並開啟 Cost Explorer 主控台，網址為 https://console.aws.amazon.com/cost-management/home#/custom。
2. 在 [時間] 底下，選擇您要分析的日期範圍。
3. 在「分組依據」下，對於維度，選擇「用法類型」。
4. 在「篩選器」下，針對「服務」選擇CloudTrail。

下圖顯示依「使用情況」類型篩選 CloudTrail 並分組的成本報告範例。



檢閱「用法」類型，以查看哪些 CloudTrail 圖徵產生的成本最高。每種使用類型都以產生費用 AWS 區域 的代碼開頭。

下表說明每個 CloudTrail 功能的 CloudTrail 用法類型。

CloudTrail 特徵	用量類型	描述
CloudTrail 小徑	*region*-FreeEventsRecorded	管理事件的第一個副本免費傳送給 AWS 區域.
	region-PaidEventsRecorded	傳送至 AWS 區域.
	region-DataEventsRecorded	將資料事件傳送至 AWS 區域. 資料事件一律會產生費用。
CloudTrail 湖	*region*-Ingestion-Bytes	使用七年保留定價選項將事件導入 CloudTrail Lake 事件資料存放區的費用。擷取定價是根據擷取的資料量而定，所有事件類型都相同。
	region-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	使用一年可延長保留定價選項，將 CloudTrail 資料事件和管理事件導入 CloudTrail Lake 事件資料存放區的費用。
	region-Ingestion-Bytes-1yearstore-Other-data-sources	使用一年可延長保留定價選項將其他事件來源導入 CloudTrail Lake 事件資料存放區的費用。這包括 CloudTrail

CloudTrail 特徵	用量類型	描述
		見解事件、來自的組態項目 AWS Config、來自 S3 的證據 AWS Audit Manager、從 S3 匯入的 (未壓縮) 歷史 CloudTrail 記錄，以及外部的 AWS事件。
	region-QueryScanned-Bytes	執行 CloudTrail Lake 查詢的費用。在 CloudTrail Lake 中執行查詢時，會根據掃描的最佳化和壓縮資料量產生費用。
CloudTrail 洞察力	*region*-InsightsEvents	CloudTrail 深入解析事件的費用。對於 Insights 事件，您會根據每個 Insight 類型分析的管理事件數量產生費用。

其他資源

- AWS CloudTrail 定價
- 管理 CloudTrail 追蹤成本
- 管理 CloudTrail 湖泊成本

使用 CloudTrail 事件歷史記錄

CloudTrail 默認情況下，您的 AWS 帳戶已啟用，並且您可以自動訪問 CloudTrail 活動歷史記錄。事件歷史記錄提供過去 90 天發生的 AWS 區域管理事件的可檢視、可搜尋、可下載而且不可變的記錄。這些事件會擷取透過 AWS Management Console AWS Command Line Interface、和 AWS SDK 和 API 所做的活動。事件歷史記錄在事件發生的 AWS 區域 地方記錄事件。查看活動歷史記錄不 CloudTrail 收取任何費用。

您可以檢視事件歷史記錄頁面，在 CloudTrail 主控台中依區域查詢與建立、修改或刪除資源 (例如 IAM 使用者或 Amazon EC2 執行個體) 相關的事件。 AWS 帳戶 您也可以執行 aws cloudtrail lookup-events 命令或使用 `LookupEvents` API 以查詢這些事件。

您可以使用 CloudTrail 主控台中的 [事件歷史記錄] 頁面來檢視、搜尋、下載、封存、分析和回應 AWS 基礎結構中的帳戶活動。您可以透過選取在每個頁面上顯示多少事件以及顯示或隱藏哪些欄，對主控台中事件歷史記錄的檢視畫面進行自訂。您還可以在事件歷史記錄中比較事件的詳細信息 side-by-side。您可以使用 AWS SDK 或 AWS Command Line Interface以程式設計方式查詢事件。

> **Note**
>
> 隨著時間的推移， AWS 服務 可能會增加其他事件 CloudTrail 將這些事件記錄在事件歷史記錄中，但是在新增事件後 90 天之後，將無法使用包含新增事件的完整 90 天活動記錄。
> 事件歷史記錄與您為帳戶建立的任何追蹤或事件資料存放區是分開的。您對事件資料存放區或追蹤所做的變更不會影響事件歷史記錄。

以下各節說明如何使用 CloudTrail 主控台查詢最近的管理事件 AWS CLI，並說明如何下載事件檔案。如需使用 `LookupEvents` API 擷取 CloudTrail 事件資訊的相關資訊，請參閱 AWS CloudTrail API 參考LookupEvents中的。

主題

- 事件歷史記錄的限制
- 使用主控台檢視最近的管理事件
- 檢視最近的管理事件 AWS CLI

事件歷史記錄的限制

下列限制適用於事件歷史記錄。

- CloudTrail 主控台上的 [事件歷程記錄] 頁面只會顯示管理事件。它不會顯示資料事件或 Insights 事件。
- 事件歷史記錄僅限於過去 90 天的事件。若要在您的中持續記錄事件 AWS 帳戶，請建立事件資料存放區或追蹤。
- 當您從 CloudTrail 主控台的 [事件歷程記錄] 頁面下載事件時，最多可以在單一檔案中下載 200,000 個事件。如果您達到 200,000 個事件限制，主 CloudTrail 控台將提供下載其他檔案的選項。
- 事件歷史記錄不提供組織層級事件彙總。若要記錄整個組織的事件，則建立組織事件資料存放區或追蹤。
- 事件歷史記錄搜索僅限於單個 AWS 帳戶，僅返回單個事件 AWS 區域，並且無法查詢多個屬性。您只能套用一個屬性篩選條件和一個時間範圍篩選條件。

  您可以建立 CloudTrail Lake 事件資料倉庫，以跨多個屬性和進行查詢 AWS 區域。您也可以在 AWS Organizations 組織 AWS 帳戶 中跨多個查詢。在 CloudTrail Lake 中，您可以查詢多個事件類型，包括管理事件、資料事件、見解事件、 AWS Config 設定項目、Audit Manager 證據和非AWS 事件。 CloudTrail 與事件歷史記錄或運`LookupEvents`行中的簡單鍵和值查詢相比，Lake 查詢提供了更深入且更可自定義的事件視圖。如需詳細資訊，請參閱 工作, 由于, AWS CloudTrail 湖 及 使用主控台為 CloudTrail事件建立事件資料存放區。
- 您無法從事件歷史記錄中排除 AWS KMS 或從事件歷史記錄中排除 Amazon RDS Data API 事件；套用至追蹤或事件資料存放區的設定不適用於事件歷史記錄。

使用主控台檢視最近的管理事件

您可以使用 CloudTrail 主控台中的 [事件歷史記錄] 頁面來檢視 AWS 區域. 您也可以根據選擇的篩選條件和時間範圍，下載具有該資訊的檔案或具有一部分資訊的檔案。您可以透過選擇在每個頁面上顯示多少事件以及在主控台中顯示哪些欄，自訂事件歷史記錄的檢視畫面。您也可以依適用於特定服務的資源類型來查詢和篩選事件。您可以在事件歷史記錄中選擇最多五個事件並比較其詳細信息 side-by-side。

Event history (事件歷史記錄) 不會顯示資料事件。若要檢視資料事件，請建立事件資料存放區或追蹤。

90 天後，事件不會再顯示在 Event history (事件歷史記錄) 中。您無法手動刪除 Event history (事件歷史記錄) 中的事件。

您可以參閱該服務的文件，進一步瞭解特定服務 CloudTrail 記錄事件的詳細資訊。如需詳細資訊，請參閱 AWS 的服務主題 CloudTrail。

> **Note**
>
> 如需過去 90 天的持續活動和事件記錄，請建立事件資料存放區或追蹤。

若要檢視事件歷史記錄

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Event history (事件歷史記錄)。您可以看到已篩選的事件清單，並最先顯示最近的事件。事件的預設篩選條件為唯讀，並設為 false。您可以選擇過濾器右側的 X 來清除該篩選條件。
3. 您可以篩選單一屬性上的事件，您可以從下拉式清單中選擇該屬性。若要篩選屬性，請從下拉式清單中選擇屬性，然後輸入屬性的完整值。例如，若要檢視所有主控台登入事件，請選擇 [事件名稱] 篩選器，然後指定ConsoleLogin。或者，若要檢視最近的 S3 管理事件，請選擇事件來源篩選器，然後指定`s3.amazonaws.com`。
4. 若要檢視特定管理事件，請選擇事件名稱。在事件詳細資訊頁面上，您可以了解事件的相關詳細資訊，查看任何參考資源以及檢視事件記錄。
5. 若要比較事件，請透過填寫事件歷史記錄資料表左邊距中的核取方塊，最多可選取五個事件。您可以在「比較」事件詳細資訊表格 side-by-side 中檢視所選事件的詳細資訊。
6. 您可以將事件歷史記錄下載為 CSV 或 JSON 格式的檔案。下載事件歷史記錄可能需要幾分鐘的時間。

內容

導覽頁面

您可以選擇要檢視的頁面，在事件歷史記錄中導覽不同頁面。您還可以在事件歷史記錄中查看下一頁和上一頁。

選擇 < 可檢視事件歷史記錄的上一頁。

選擇 > 可檢視事件歷史記錄的下一頁。

自訂顯示

您可以從下列偏好設定中選取，在 CloudTrail 主控台中自訂事件歷程記錄的檢視。

- 頁面大小 - 選擇您想在每個頁面上顯示 10 個、25 個還是 50 個事件。
- 換行 - 文字換行，以便您查看每個事件的全部文字。
- 條紋效果 - 表格中相鄰兩列的顏色深淺相間。
- 事件時間顯示 - 選擇以 UTC 或當地時區顯示事件時間。
- 選取可見欄 - 選取要顯示的欄。預設會顯示下列欄位：
  - 事件名稱
  - Event time (事件時間)
  - 使用者名稱
  - 事件來源
  - Resource Type (資源類型)
  - 資源名稱

> **Note**
>
> 您無法變更欄位順序，或從 Event history (事件歷史記錄) 手動刪除事件。

若要自訂顯示

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Event history (事件歷史記錄)。
3. 選擇齒輪圖示。
4. 在頁面大小中，選擇要在單個頁面上顯示的總事件數。

5. 選擇換行，以查看每個事件的全部文字。
6. 選擇條紋效果，使表格中相鄰兩列的顏色深淺相間。
7. 對於事件時間顯示，選擇以 UTC 或當地時區顯示事件時間。預設值為選取 UTC。
8. 在 Select visible columns (選取可見欄位) 中，選取您要顯示的欄位。關閉您不要顯示的欄位。
9. 完成變更後，選擇確認。

篩選 CloudTrail 事件

Event history (事件歷史記錄) 的事件預設顯示使用屬性篩選條件，排除顯示事件清單裡的唯讀事件。此屬性篩選條件名稱為 Read only (唯讀)，且設定為 false。可以刪除此篩選條件，顯示讀取事件和寫入事件。若要僅檢視 Read (讀取) 事件，可以把篩選條件改成 true 您也可以依其他屬性篩選事件。您還可以依時間範圍篩選。

> **Note**
>
> 您只能套用一個屬性篩選條件和一個時間範圍篩選條件。您無法套用多個屬性篩選條件。

AWS 存取金鑰

用來簽署要求的 AWS 存取金鑰 ID。如果使用暫時性安全登入資料提出請求，則此為暫時性登入資料的存取金鑰 ID。

事件 ID

事件的 CloudTrail 識別碼。每個事件都會有唯一的 ID。

事件名稱

事件的名稱。例如，您可以根據 IAM 事件 (例如 `CreatePolicy`) 或 Amazon EC2 事件 (例如 `RunInstances`) 進行篩選。

事件來源

提出要求的 AWS 服務，例如`iam.amazonaws.com`或`s3.amazonaws.com`。在您選擇 Event source (事件來源) 篩選條件之後，即可捲動事件來源清單。

唯讀

事件的讀取類型。事件可分類為讀取事件或寫入事件。如果設定為 false，顯示事件清單就不會包含閱讀事件。預設套用此屬性篩選條件，此值預設設定為 false。

資源名稱

事件所參考之資源的名稱或 ID。例如，對於 Auto Scaling 組，資源名稱可能是「auto-scaling-test-group」，對於 EC2 執行個體，資源名稱可能是「i-12345678910」。

資源類型

事件所參考之資源的類型。例如，資源類型可以是 `Instance` (用於 EC2) 或 `DBInstance` (用於 RDS)。每個 AWS 服務的資源類型都有所不同。

時間範圍

您想要篩選事件的時間範圍。您可以選擇相對範圍或絕對範圍。您可以篩選過去 90 天的事件。

使用者名稱

事件所參考的身分。舉例來說，它可以是使用者、角色名稱，或服務角色。

如果在您所選擇的屬性或時間下沒有記錄的事件，則結果清單會是空的。除了時間範圍之外，您只能套用一個屬性篩選條件。如果您選擇不同的屬性篩選條件，則會保留您指定的時間範圍。

下列步驟說明如何依屬性進行篩選。

依屬性篩選

1. 若要依屬性篩選結果，請從 Lookup attributes (查閱屬性) 下拉式清單選擇屬性，然後在文字方塊中輸入或選擇屬性的值。
2. 若要移除屬性篩選條件，請選擇屬性篩選條件方塊右側的 X。

下列步驟說明如何依開始與結束日期及時間進行篩選。

依開始與結束日期及時間進行篩選

1. 若要縮小您要查看之事件的時間範圍，請選擇時間範圍列中的時間範圍。您可以選擇相對範圍或絕對範圍。

   選擇相對範圍以選取預設值，或者選擇自訂範圍。預設值有 30 分鐘、1 小時、12 小時或 1 天。若要指定自訂時間範圍，請選擇 Custom (自訂)。

   選擇絕對範圍以指定特定的開始和結束時間。您還可以選擇當地時區或 UTC。
2. 若要移除時間範圍篩選條件，請選擇時間範圍列中的清除並關閉。

檢視事件的詳細資訊

1. 在結果清單中選擇事件，以顯示其詳細資訊。
2. 事件中參照的資源會顯示在 Resources referenced (所參考的資源) 事件詳細資訊頁面上的資料表。
3. 有些參考的資源可能會有連結。請選擇可開啟該資源之主控台的連結。
4. 捲動至詳細資訊頁面上的 Event record (事件記錄) 以查看 JSON 事件記錄，也稱為事件酬載。
5. 選擇頁面導覽路徑中的 Event history (事件歷史記錄)，以關閉事件詳細資料頁面並返回 Event history (事件歷史記錄)。

下載事件

您可以將已記錄之事件歷史記錄以 CSV 或 JSON 檔案格式下載。您可以在一個文件中下載多達 200,000 個事件。如果您達到 200,000 個事件限制，主 CloudTrail 控台將提供下載其他檔案的選項。善用篩選條件和時間範圍，減少下載的檔案大小。

> **Note**
>
> CloudTrail 事件歷程記錄檔案是包含可由個別使用者設定的資訊 (例如資源名稱) 的資料檔案。有些資料在用來讀取與分析資料 (CSV injection) 的程式中很可能會被解譯為命令。例如，當 CloudTrail 事件匯出為 CSV 並匯入試算表程式時，該程式可能會警告您安全性考量。您應該選擇停用此內容，以保持系統的安全。請一律停用連結或巨集下載事件歷史記錄檔案。

1. 在事件歷史記錄中針對您想要下載的事件新增篩選條件和時間範圍。例如，您可以指定事件名稱 `StartInstances`，並指定活動的時間範圍為最後三天。
2. 選擇 Download events (下載事件)，然後選擇 Download as CSV (下載為 CSV) 或 Download as JSON (下載為 JSON)。下載會即刻開始。

> **Note**
>
> 您的下載可能需要一些時間才能完成。如需更快速的結果，請在您開始下載程序之前，使用更特定的篩選條件或較短的時間範圍來縮小結果範圍。您可以取消下載。如果您取消下載，本機電腦上可能會包含部分事件資料的部分下載。若要下載完整的事件歷史記錄，請重新啟動下載。

3. 下載完成後，請開啟檔案，以檢視您指定的事件。
4. 若要取消下載，請選擇 Cancel (取消)，然後選擇 Cancel download (取消下載)。如果您需要重新啟動下載，請等到先前的下載完成取消。

使用 AWS Config檢視所參考的資源

AWS Config 記錄組態詳細資訊、關係和 AWS 資源的變更。

在 [資源參照] 窗格中，選擇 [AWS Config 資源時間表] 欄中的，以檢視 AWS Config 主控台中的資源。

如果  圖示為灰色、 AWS Config 未開啟或未記錄資源類型。選擇圖示以移至 AWS Config 主控台以開啟服務或開始記錄該資源類型。如需詳細資訊，請參閱AWS Config 開發人員指南中的AWS Config 使用主控台進行設定。

如果 Link not available (連結無法使用) 出現在欄位中，則因下列其中一個原因而無法檢視資源：

- AWS Config 不支援資源類型。如需詳細資訊，請參閱中的 AWS Config 開發人員指南 中的支援的資源、組態項目和關係。
- AWS Config 最近增加了對資源類型的支持，但尚未從 CloudTrail 控制台提供。您可以在 AWS Config 控制台中查看資源以查看資源的時間表。
- 該資源由另一個擁有 AWS 帳戶。
- 資源由另一個資源所擁有 AWS 服務，例如受管 IAM 政策。
- 資源在建立後就立即刪除。
- 最近建立或更新資源。

若要授與使用者在 AWS Config 主控台中檢視資源的唯讀權限，請參閱授與檢視 CloudTrail 主控台 AWS Config 資訊的權限。

如需詳細資訊 AWS Config，請參閱AWS Config 開發人員指南。

檢視最近的管理事件 AWS CLI

您可以 AWS 區域 使用aws cloudtrail lookup-events命令查詢目前 90 天的 CloudTrail 管理事件。該aws cloudtrail lookup-events命令顯示事件發生的 AWS 區域 地方。

查詢支援管理事件的下列屬性：

- AWS 存取金鑰
- 事件 ID
- 事件名稱
- 事件來源
- 唯讀
- 資源名稱
- 資源類型
- 使用者名稱

所有屬性均為選用。

`lookup-events` 命令包含下列選項：

- `--max-items` *`<integer>`* – 要在命令輸出中傳回的總項目數。如果可用的總項目數超過指定的值，會在命令的輸出中提供 `NextToken`。若要繼續分頁，請在後續命令的 starting-token 引數中提供 `NextToken` 值。請勿在 AWS CLI外部直接使用 `NextToken` 回應元素。
- `--start-time` *`<timestamp>`* – 指定只會傳回在所指定時間或之後發生的事件。如果指定的開始時間晚於指定的結束時間，則會傳回錯誤。
- `--lookup-attributes` *`<integer>`* – 包含查詢屬性清單。目前，該清單只可包含一個項目。
- `--generate-cli-skeleton` *`<string>`* – 將 JSON 骨架列印至標準輸出，而不傳送 API 請求。如果未提供值或值輸入，則列印可用作 `--cli-input-json` 引數的範例輸入 JSON。同樣，若提供 yaml-input，它將列印可與 `--cli-input-yaml` 搭配使用的範例輸入 YAML。如果提供值輸出，它將驗證命令輸入，並為該命令傳回範例返回 JSON。生成的 JSON 骨架在版本之間不穩定，AWS CLI 並且在生成的 JSON 骨架中沒有向後兼容性保證。
- `--cli-input-json` *`<string>`* – 從提供的 JSON 字串讀取引數。JSON 字串遵循 `--generate-cli-skeleton` 參數所提供的格式。若命令列上提供了其他引數，這些值將覆寫 JSON 提供的值。任意二進位值不可透過使用 JSON 提供的值傳遞，因為字串將依照字面意思處理。這可能不會與 `--cli-input-yaml` 參數一同指定。

若要取得有關使用指 AWS 令行介面的一般資訊，請參閱《使AWS Command Line Interface 用指南》。

內容

必要條件

- 若要執行 AWS CLI 命令，您必須安裝 AWS CLI. 如需詳細資訊，請參閱開始使用 AWS CLI.
- 確保您的 AWS CLI 版本大於 1.6.6。若要驗證 CLI 版本，請在命令列上執行 aws --version。
- 若要設定 AWS CLI 工作階段的帳戶 AWS 區域、和預設輸出格式，請使用aws configure指令。若要取得更多資訊，請參閱〈規劃 AWS 指令行介面〉。

> **Note**
>
> 這些命 CloudTrail AWS CLI 令是區分大小寫的。

取得命令列說明

若要查看 `lookup-events` 的命令列說明，請輸入下列命令：

```
aws cloudtrail lookup-events help
```

查詢事件

> **Important**
>
> 查詢請求的速率上限為每秒、每個帳戶、每個區域兩個。若超出此上限，則將發生限流錯誤。

若要查看十個最新的事件，請輸入下列命令：

```
aws cloudtrail lookup-events --max-items 10
```

所傳回的事件類似下列虛構範例，其已針對可讀性進行格式化：

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
                  \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                  \"eventType\":\"AwsApiCall\",
```

```
                \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```

如需輸出中查詢相關欄位的說明，請參閱本文件後面的「查詢輸出欄位」一節。如需 CloudTrail 事件中欄位的說明，請參閱CloudTrail 記錄內容。

指定要傳回的事件數目

若要指定要傳回的事件數目，請輸入下列命令：

```
aws cloudtrail lookup-events --max-items <integer>
```

可能值為 1 到 50。以下範例會傳回一個事件。

```
aws cloudtrail lookup-events --max-items 1
```

依時間範圍查詢事件

過去 90 天的事件可用於查詢。若要指定時間範圍，請輸入下列命令：

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *`<timestamp>`* 指定 (UTC) 只會傳回在所指定時間或之後發生的事件。如果指定的開始時間晚於指定的結束時間，則會傳回錯誤。

`--end-time` *`<timestamp>`* 指定 (UTC) 只會傳回在所指定時間或之前發生的事件。如果指定的結束時間早於指定的開始時間，則會傳回錯誤。

預設的開始時間是過去 90 天內可使用資料的最早日期。預設的結束時間是在最接近目前時間所發生之事件的時間。

所有時間戳記均會以 UTC 顯示。

依屬性查詢事件

若要依屬性進行篩選，請輸入下列命令：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

您只能為每個 lookup-events 命令指定一個屬性鍵/值對。以下是 AttributeKey 的有效值。值名稱區分大小寫。

- AccessKeyId
- EventId
- EventName
- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

的最大長度AttributeValue為 2000 個字元。以下字符（'_'，"， "，,'\\n'）算作兩個字符，朝著 2000 個字符限制。

屬性查詢範例

下列範例命令會傳回 AccessKeyId 值為 AKIAIOSFODNN7EXAMPLE 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

下列範例命令會傳回指定的事件 CloudTrailEventId。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

下列範例命令會傳回 EventName 值為 RunInstances 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

下列範例命令會傳回 EventSource 值為 iam.amazonaws.com 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

下列範例命令會傳回寫入事件。不包括寫入事件，例如 GetBucketLocation跟 DescribeStream。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

下列範例命令會傳回 ResourceName 值為 CloudTrail_CloudWatchLogs_Role 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

下列範例命令會傳回 ResourceType 值為 AWS::S3::Bucket 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

下列範例命令會傳回 Username 值為 root 的事件。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

指定下一頁的結果

若要從 lookup-events 命令取得下一頁的結果，請輸入下列命令：

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

其中 *<token>* 的值取自先前命令輸出的第一個欄位。

當您在命令中使用 --next-token 時，必須使用與先前命令相同的參數。例如，假設您執行下列命令：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

若要取得下一頁的結果，您的下一個命令會如下所示：

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

從檔案取得 JSON 輸入

對 AWS CLI 於某些 AWS 服務有兩個參數，`--generate-cli-skeleton`並且`--cli-input-json`，您可以使用它來生成 JSON 模板，您可以修改該模板並將其用作`--cli-input-json`參數的輸入。本節說明如何搭配使用這些參數與 `aws cloudtrail lookup-events`。如需詳細資訊，請參閱AWS CLI 骨架和輸入檔案。

從檔案取得 JSON 輸入來查詢 CloudTrail 事件

1. 將 `lookup-events` 輸出重新導向至檔案，以建立與 `--generate-cli-skeleton` 搭配使用的輸入範本，如下列範例所示。

   ```
   aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
   ```

   生成的模板文件（在本例中為 LookupEvents .txt）如下所示：

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
           }
       ],
       "StartTime": null,
       "EndTime": null,
       "MaxResults": 0,
       "NextToken": ""
   }
   ```

2. 視需要使用文字編輯器來修改 JSON。JSON 輸入只能包含所指定的值。

   > **Important**
   >
   > 必須先從範本移除所有空白值或 null 值，才能使用它。

下列範例指定時間範圍以及要傳回的結果數目上限。

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. 若要使用編輯過的檔案做為輸入，請使用語法 `--cli-input-json file://<filename>`，如下列範例所示：

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> 您可以在與 `--cli-input-json` 相同的命令列上使用其他引數。

查詢輸出欄位

事件

根據所指定查詢屬性和時間範圍的查詢事件清單。事件清單是依時間排序，而且會先列出最新的事件。每個項目都包含查詢要求的相關資訊，並包含擷取之 CloudTrail 事件的字串表示法。

下列項目說明每個查詢事件中的欄位。

CloudTrailEvent

包含以物件呈現所傳回事件的 JSON 字串。如需所有傳回之元素的資訊，請參閱記錄內文內容。

EventId

字串，包含所傳回事件的 GUID。

EventName

字串，包含所傳回事件的名稱。

EventSource

提出要求的 AWS 服務。

EventTime

事件的日期和時間 (UNIX 時間格式)。

資源

所傳回之事件所參考的資源清單。每個資源項目都會指定資源類型和資源名稱。

ResourceName

字串，包含事件所參考資源的名稱。

ResourceType

字串，包含事件所參考資源的類型。無法判定資源類型時，會傳回 null。

使用者名稱

字串，包含所傳回事件之帳戶的使用者名稱。

NextToken

字串，可從先前的 `lookup-events` 命令取得下一頁的結果。若要使用字符，參數必須與原始命令中的參數相同。如果 `NextToken` 項目未出現在輸出中，則沒有可傳回的其他結果。

工作, 由于, AWS CloudTrail 湖

AWS CloudTrail Lake 可讓您針對事件執行 SQL 型查詢。 CloudTrail 湖將基於行的 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。如果您選擇一年可延長保留定價選項，則可將事件資料保留在事件資料存放區中最多 3,653 天 (約 10 年)；如果您選擇七年保留定價選項，則最多可保留 2,557 天 (約 7 年)。您套用至事件資料存放區的選取器會控制哪些事件持續存在，而且可供您查詢。 CloudTrail Lake 是一種稽核解決方案，可以補充您的合規性堆疊，並協助您進行近乎即時的疑難排解。

CloudTrail 湖泊事件資料存放區

建立事件資料存放區時，您可以選擇要包含在事件資料存放區中的事件類型。您可以建立事件資料存放區，以包含CloudTrail 事件、CloudTrail 見解事件、AWS Config 組態項目、AWS Audit Manager 證據或來自外部的事件 AWS。每個事件資料倉庫只能包含特定的事件類別 (例如， AWS Config 組態項目)，因為事件結構描述對事件類別來說是唯一的。您可以將組織的事件儲存 AWS Organizations 在組織事件資料存放區中，包括來自多個區域和帳戶的事件。您也可以使用支援的 SQL JOIN 關鍵字，在多個事件資料存放區中執行 SQL 查詢。如需跨多個事件資料存放區執行查詢的詳細資訊，請參閱 進階的多重資料表查詢支援。

您可以將追蹤事件複製到新的或現有的事件資料存放區，以建立記錄至追蹤的事件 point-in-time 快照。如需詳細資訊，請參閱 將追蹤事件複製到事件資料存放區。

您可以聯合事件資料存放區，藉此在 AWS Glue Data Catalog 中查看與事件資料存放區相關聯的中繼資料，並使用 Amazon Athena 對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

依預設，事件資料存放區中的所有事件均由加密 CloudTrail。設定事件資料存放區時，您可以選擇使用自己的 AWS Key Management Service 金鑰。使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

您可以使用以標籤為基礎的授權，來控制對事件資料存放區動作的存取。如需詳細資訊，請參閱本指南中的 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。

您可以使用 CloudTrail Lake 儀表板來視覺化事件資料存放區中的資料。每個儀表板均包含多個小工具，每個小工具代表一個 SQL 查詢。如需有關 Lake 儀表板的詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

CloudTrail Lake 支援 Amazon CloudWatch 指標，提供有關擷取資料和儲存位元組的資訊。如需有關支援 CloudWatch 量度的詳細資訊，請參閱支援的 CloudWatch 指標。

> **Note**
>
> CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內傳遞事件。此時間無法保證。

CloudTrail 湖泊整合

您可以使用 CloudTrail Lake 整合功能，從混合式環境中的 AWS任何來源記錄和儲存使用者活動資料，例如內部部署或雲端中託管的 SaaS 應用程式、虛擬機器或容器。在 CloudTrail Lake 中建立事件資料存放區並建立用於記錄活動事件的通道後，您可以呼叫 `PutAuditEvents` API 來擷取應用程式活動 CloudTrail。然後，您可以使用 CloudTrail Lake 搜尋、查詢和分析應用程式記錄的資料。

整合還可以將來自十幾個合 CloudTrail作夥伴的事件記錄到您的事件資料存放區。在合作夥伴整合中，您可以建立目的地事件資料存放區、通道和資源政策。建立整合之後，您將通道 ARN 提供給合作夥伴。整合有兩種類型：直接和解決方案。透過直接整合，合作夥伴會呼叫 `PutAuditEvents` API，將事件傳送至您 AWS 帳戶的事件資料存放區。透過解決方案整合，應用程式會在您的 AWS 帳戶中執行，而應用程式會呼叫 `PutAuditEvents` API，將事件傳送至您 AWS 帳戶的事件資料存放區。

如需有關整合的詳細資訊，請參閱以外的事件來源建立整合 AWS。

CloudTrail 湖泊查詢

CloudTrail 與事件歷史記錄或運`LookupEvents`行中的簡單鍵和值查詢相比，Lake 查詢提供了更深入且更可自定義的事件視圖。事件歷史記錄搜索僅限於單個 AWS 帳戶，僅返回單個事件 AWS 區域，並且無法查詢多個屬性。相反地， CloudTrailLake 使用者可以跨多個事件欄位執行複雜的 SQL 查詢。CloudTrail 湖支持所有有效的普雷斯托`SELECT`語句和功能。如需支援之 SQL 函數和運算子的詳細資訊，請參閱 Presto 文件網站上的函數和運算子。

您可以儲存 CloudTrail Lake 查詢以備 future 使用，並檢視最多七天的查詢結果。執行查詢時，您可以將查詢結果儲存至 Amazon S3 儲存貯體。

主 CloudTrail 控台提供許多範例查詢，可協助您開始撰寫自己的查詢。如需詳細資訊，請參閱 在 CloudTrail 主控台中檢視範例查詢。

CloudTrail 湖泊查詢會產生費用。在 Lake 中執行查詢時，您需要依據掃描的資料量付費。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

其他資源

以下資源可以幫助您更好地了解什麼是 CloudTrail 湖泊以及如何使用它。

- 使用 CloudTrail Lake 將稽核記錄管理現代化 (YouTube 影片)
- 記錄來自 AWS CloudTrail 湖泊中非AWS 來源的活動事件 (YouTube 視頻)
- 使用 AWS CloudTrail 湖泊和 Amazon Athena 分析活動日誌 (YouTube 影片)
- 瞭解員工和客戶身分的活動日誌 (AWS 部落格)
- 使用 AWS CloudTrail Lake 識別舊版 TLS 連線至 AWS 服務端點 (AWS 部落格)
- 北極狼如何利用 AWS CloudTrail 湖泊簡化安全性和營運 (AWS 部落格)
- CloudTrail 湖常見問題
- AWS CloudTrail API 參考
- AWS CloudTrail 資料 API 參考資料
- AWS CloudTrail 合作夥伴上線指南

CloudTrail 湖泊支持的地區

目前，以下支援 CloudTrail 湖泊 AWS 區域：

區域名稱	區域
美國東部 (維吉尼亞北部)	us-east-1
美國東部 (俄亥俄)	us-east-2
美國西部 (加州北部)	us-west-1
美國西部 (奧勒岡)	us-west-2

區域名稱	區域
非洲 (開普敦)	af-south-1
亞太區域 (香港)	ap-east-1
亞太區域 (海德拉巴)	ap-south-2
亞太區域 (雅加達)	ap-southeast-3
亞太區域 (孟買)	ap-south-1
亞太區域 (大阪)	ap-northeast-3
亞太區域 (首爾)	ap-northeast-2
亞太區域 (新加坡)	ap-southeast-1
亞太區域 (雪梨)	ap-southeast-2
亞太區域 (東京)	ap-northeast-1
加拿大 (中部)	ca-central-1
歐洲 (法蘭克福)	eu-central-1
歐洲 (愛爾蘭)	eu-west-1
歐洲 (倫敦)	eu-west-2
歐洲 (米蘭)	eu-south-1
歐洲 (巴黎)	eu-west-3
歐洲 (西班牙)	eu-south-2
歐洲 (斯德哥爾摩)	eu-north-1
歐洲 (蘇黎世)	eu-central-2
以色列 (特拉維夫)	il-central-1

區域名稱	區域
中東 (巴林)	me-south-1
中東 (阿拉伯聯合大公國)	me-central-1
南美洲 (聖保羅)	sa-east-1
AWS GovCloud (美國東部)	us-gov-east-1
AWS GovCloud (美國西部)	us-gov-west-1

如需 CloudTrail 服務端點的相關資訊，請參閱AWS CloudTrail 端點和配額。

如需有關使用 CloudTrail 的詳細資訊 AWS GovCloud (US) Regions，請參閱使AWS GovCloud (US) 用指南中的服務端點。

CloudTrail 湖泊概念和術語

本節說明可協助您使用 AWS CloudTrail Lake 的關鍵概念和術語。

概念和術語

- 事件資料存放區
- 整合
- 查詢
- 儀表板

事件資料存放區

系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。

您可以建立事件資料存放區來記錄CloudTrail 管理事件和資料事件、CloudTrail Insights 事件、AWS Audit Manager 證據、AWS Config 組態項目或外部的事件 AWS。

進階事件選取器

進階事件選取器可決定要包含在事件資料存放區中的事件。這些事件選取器可以僅記錄對您而言重要的事件，從而協助您控制成本。

您可以使用進階事件選取器，針對管理事件和資料事件來篩選事件。例如，如果您要建立事件資料存放區來收集管理事件，則可以篩選掉 AWS Key Management Service (AWS KMS) 或 Amazon Relational Database Service (Amazon RDS) 資料 API 事件。通常情況下`Encrypt`， AWS KMS 動作如`Decrypt`、和`GenerateDataKey`產生超過 99% 的事件。

對於 AWS Config 組態項目、Audit Manager 證據或以外的事件 AWS，進階事件選取器僅用於在事件資料存放區中包含該類型的事件。

聯合

聯合可讓您在 AWS Glue Data Catalog 中查看與事件資料存放區相關聯的中繼資料，並使用 Amazon Athena 對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。

當您啟用 Lake 查詢同盟時，會代表您 CloudTrail 建立聯合資源，並使AWS Lake Formation用註冊這些資源。啟用 Lake 聯合後，您可以直接在 Athena 中查詢您的事件資料，無須執行任何其他步驟。如需詳細資訊，請參閱 聯合事件資料存放區。

定價選項

建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需定價的詳細資訊，請參閱 AWS CloudTrail 定價和管理 CloudTrail 湖泊成本。

保留期間

事件資料存放區的保留期決定了事件資料在事件資料存放區中保留的時間長度。 CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

預設保留期

事件資料存放區的預設保留期是事件資料保留在事件資料存放區中的預設天數。在事件資料存放區的預設保留期內，儲存已包含在擷取定價中，無須額外付費。在預設保留期之後，儲存空間的定價為 pay-as-you-go。

最長保留期

事件資料存放區的最長保留期代表您可以將資料保留在事件資料存放區中的天數上限。

終止保護

依預設，事件資料存放區會啟用終止保護，以防止意外刪除事件資料存放區。若要刪除啟用終止保護的事件資料存放區，請前往事件資料存放區的詳細資訊頁面，從動作功能表中選擇變更終止保護。然後，您可以繼續刪除事件資料存放區。如需詳細資訊，請參閱 使用主控台變更終止保護。

整合

您可以使用 CloudTrail Lake 整合來記錄和儲存下列來源的使用者活動資料：

- 外面 AWS
- 混合環境中任何來源，例如在內部部署或雲端、虛擬機器或容器中託管的內部或軟體即服務 (SaaS) 應用程式

整合需要通道來傳遞事件，並需要事件資料存放區來接收事件。設定整合之後，請呼叫 PutAuditEventsAPI 作業以擷取應用程式活動 CloudTrail。然後，您可以使用 CloudTrail Lake 搜尋、查詢和分析應用程式記錄的資料。如需詳細資訊，請參閱 建立與事件來源以外的整合 AWS。

整合類型

整合有兩種類型：直接和解決方案。透過直接整合，合作夥伴可呼叫 PutAuditEvents API 操作，將事件傳遞至您 AWS 帳戶的事件資料存放區。透過解決方案整合，應用程式會在您的中執行， AWS 帳戶 而應用程式會呼叫 PutAuditEvents API 作業，將事件傳送至您的事件資料存放區 AWS 帳戶。

頻道

來自 AWS 工作以外來源的活動事件 CloudTrail，透過使用管道將活動從與其合作的外部合作夥伴或從您自己的來源引入 CloudTrail Lake。建立通道時，您可以選擇一或多個事件資料存放區，以儲存從通道來源到達的事件。只要目的地事件資料存放區設定為記錄 eventCategory="ActivityAuditLog" 事件，您就可以視需要變更通道的目的地事件資料存放區。當您為來自外部合作夥伴的事件建立通道時，您會將通道 Amazon Resource Name (ARN) 提供給合作夥伴或來源應用程式。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。連接至通道的資源型政策允許來源透過通道傳輸事件。如果通道沒有資源政策，則只有通道擁有者可以在通道上呼叫 PutAuditEvents API 操作。如需詳細資訊，請參閱 AWS CloudTrail 資源型政策範例。

查詢

CloudTrail 湖泊中的查詢是使用 SQL 編寫的。您可以從頭開始以 SQL 撰寫查詢，或開啟已儲存或範例查詢並進行編輯，在 CloudTrail Lake Editor 索引標籤上建立查詢。您不能透過變更覆寫包含的範例查詢，但可以將其另存為新查詢。如需詳細資訊，請參閱 建立或編輯查詢。

CloudTrail 湖支持所有有效的PrestoSELECT語句和功能。如需支援之 SQL 函數和運算子的詳細資訊，請參閱 Presto 文件網站上的函數和運算子。

儀表板

透過使用 CloudTrail Lake 儀表板，您可以視覺化事件資料存放區中的事件，並查看事件趨勢，例如頂端 AWS 服務、使用者和錯誤。如需詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

儀表板類型

事件資料存放區可用的儀表板類型取決於該事件資料存放區的進階事件選取器組態。例如，如果儀表板類型顯示有關 CloudTrail 管理事件的資訊，則只有當目前選取的事件資料存放區收集 CloudTrail 管理事件時，您才能選取儀表板。

以下是可用的儀表板類型：

- 概觀儀表板 — 顯示最活躍的使用者 AWS 區域，以及 AWS 服務 按事件計數。您還可以檢視有關 `read` 和 `write` 管理事件活動、最常調節事件和常見錯誤的資訊。此儀表板適用於收集管理事件的事件資料存放區。
- 管理事件儀表板 – 依使用者顯示主控台登入事件、存取遭拒事件、破壞性動作和常見錯誤。您還可以檢視有關 TLS 版本以及使用者的過期 TLS 呼叫的資訊。此儀表板適用於收集管理事件的事件資料存放區。
- S3 資料事件儀表板 – 顯示 Amazon S3 帳戶活動、最常存取的 S3 物件、常見的 S3 使用者，以及最常執行的 S3 動作。此儀表板適用於收集 Amazon S3 資料事件的事件資料存放區。
- Insights 事件儀表板 - 依 Insights 類型顯示 Insights 事件的總體比例，依最常使用的使用者和服務的 Insights 類型顯示 Insights 事件的比例，以及顯示每天的 Insights 事件數量。此儀表板還包含一個小工具，可列出最多 30 天的 Insights 事件。它僅適用於收集 Insights 事件的事件資料存放區。

> **Note**
>
> - 在來源事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天才能傳遞第一個 Insights 事件。如需詳細資訊，請參閱 了解 Insights 事件傳遞。

- Insights 事件儀表板僅顯示由所選事件資料存放區收集的 Insights 事件的相關資訊，這取決於來源事件資料存放區的組態。例如，如果您設定來源事件資料存放區啟用 `ApiCallRateInsight` 的 Insights 事件，而不啟用 `ApiErrorRateInsight` 的 Insights 事件，您將不會看到有關 `ApiErrorRateInsight` 的 Insights 事件的資訊。

小工具

小工具是組成儀表板的元件並可提供視覺化效果，例如折線圖或長條圖。每個小工具都代表一個基礎查詢。當您選擇「執行查詢」時， CloudTrail 會執行系統產生的查詢，以填入每個 Widget 的資料。

CloudTrail 湖泊事件資料存放區

系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。

在 CloudTrail Lake 中建立事件資料倉庫時，您可以選擇要包含在事件資料倉庫中的事件類型。您可以建立事件資料存放區，以包含外部的 CloudTrail資料或管理事件、 CloudTrail Insights 事件、AWS Config 組態項目或事件 AWS。每個事件資料存放區類型只能包含特定的事件類別 (例如， AWS Config 組態項目)，因為事件結構描述對事件類別來說是唯一的。您可以使用支援的 SQL JOIN 關鍵字，跨多個事件資料存放區執行 SQL 查詢。如需跨多個事件資料存放區執行查詢的詳細資訊，請參閱進階的多重資料表查詢支援。

下表顯示每種事件資料存放區類型的受支援事件類別。eventCategory 欄顯示您要在進階事件選取器中指定的值，以便收集該類型的事件。

事件類型 (主控台)	eventCategory (API)	描述

CloudTrail 事件	`Management`
	
	`Data`
		此事件資料存放區類型可以收集 CloudTrail 管理和資料事件。如需詳細資訊，請參閱為 CloudTrail 事件建立事件資料存放區。

CloudTrail 洞察活動	`Insight`	此事件資料存放區類型可以收集 CloudTrail 見解事件。若要接收 Insights 事件，您需要一個來源事件資料存放區來記錄 CloudTrail 管理事件並啟用見解。如需有關建立來源和目標事件資料存放

事件類型 (主控台)	eventCategory (API)	描述
		區的詳細資訊，請參閱建立 CloudTrail Insights 事件的事件資料存放區。
組態項目	`ConfigurationItem`	此事件資料存放區類型可以收集 AWS Config 組態項目。如需詳細資訊，請參閱建立 AWS Config 組態項目的事件資料存放區。
來自整合的事件	`ActivityAuditLog`	此事件資料存放區類型可以從整合收集非AWS 事件。如需詳細資訊，請參閱為以外的事件建立事件資料存放區 AWS。

您也可以使用 Audit Manager 主控台建立 AWS Audit Manager 證據的事件資料存放區。如需有關使用 Audit Manager 彙總 CloudTrail Lake 中證據的詳細資訊，請參閱《使用AWS Audit Manager 者指南》中的瞭解證據尋找器如何與 CloudTrail Lake 搭配使用。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

以下各節說明如何建立、更新和管理事件資料存放區。

主題

- 使用主控台建立、更新和管理事件資料存放區
- 建立、更新和管理事件資料存放區 AWS CLI
- 管理事件資料存放區生命週期
- 將追蹤事件複製到事件資料存放區
- 聯合事件資料存放區
- 組織事件資料存放區

使用主控台建立、更新和管理事件資料存放區

您可以使用 CloudTrail 主控台建立、更新和管理事件資料存放區。您也可以在事件資料存放區上啟動和停止事件擷取，以及使用主控台啟用 Lake 查詢聯合。

使用主 CloudTrail 控台建立或更新事件資料存放區可提供下列優點：

- 如果這是您第一次建立事件資料存放區，使用 CloudTrail 主控台可讓您檢視可用的功能和選項。
- 如果您將事件資料存放區設定為記錄資料事件，則使用 CloudTrail 控制台可讓您檢視可用的資料類型。如需詳細資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區 及 記錄資料事件。
- 如果您將事件資料存放區設定為記錄以外的事件 AWS，使用 CloudTrail 主控台可讓您檢視可用合作夥伴的相關資訊。如需詳細資訊，請參閱 AWS 使用主控台為外部事件建立事件資料存放區。

主題

使用主控台為 CloudTrail事件建立事件資料存放區

事件的事件資料 CloudTrail 存放區可以記錄 CloudTrail 管理和資料事件。如果您選擇一年可延長保留定價選項，則可將事件資料保留在事件資料存放區中最多 3,653 天 (約 10 年)；如果您選擇七年保留定價選項，則最多可保留 2,557 天 (約 7 年)。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

建立 CloudTrail 管理或資料事件的事件資料倉庫

使用此程序可建立記錄管理事件、資料事件或同時記錄 CloudTrail 管理和資料事件的事件資料存放區。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在設定事件資料存放區頁面上的一般詳細資訊中，輸入事件資料存放區的名稱。名稱為必填。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

   > **Note**
   >
   > 如果您要 CloudTrail 將追蹤事件複製到此事件資料存放區，如果事件早於指定的保留期間，`eventTime`則不會複製該事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*)。例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。

7. (選擇性) 若要啟用加密方式 AWS Key Management Service，請選擇 [使用我自己的] AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/MyAliasName`。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

   > **Note**
   >
   > 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在 Tags (標籤) 區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對事件資料存放區的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用指南》中的〈標記 AWS 資源〉。

10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在 [選擇事件] 頁面上，選擇AWS 事件，然後選擇CloudTrail事件。

12. 對於CloudTrail 事件，請至少選擇一個事件類型。根據預設，管理事件已選取。您可以將管理事件和資料事件新增到事件資料存放區中。如需有關管理事件的詳細資訊，請參閱 記錄管理事件。如需有關資料事件的詳細資訊，請參閱 記錄資料事件。

13. (選擇性) 如果您要從現有追蹤複製事件，以對過去事件執行查詢，請選擇 Copy trail events (複製追蹤事件)。若要將追蹤事件複製到組織事件資料存放區，您必須使用組織的管理帳戶。委派的管理員帳戶無法將追蹤事件複製到組織事件資料存放區。如需複製追蹤事件考量事項的詳細資訊，請參閱 複製追蹤事件的考量。
14. 若要讓事件資料存放區從 AWS Organizations 組織中的所有帳戶收集事件，請選取 Enable for all accounts in my organization (啟用我組織中的所有帳戶)。您必須登入到組織的管理帳戶或委派的管理員帳戶，才能建立為組織收集事件的事件資料存放區。

> **Note**
>
> 若要複製追蹤事件或啟用 Insights 事件，您必須登入到組織的管理帳戶。

15. 展開其他設定以選擇是要讓事件資料存放區收集所有事件 AWS 區域，還是僅收集目前事件的事件 AWS 區域，然後選擇事件資料儲存庫是否擷取事件。依預設，您的事件資料存放區會從帳戶的所有區域收集事件，而且會在建立時開始擷取事件。

    a. 選取在我的事件資料存放區中僅包含目前區域以僅包括在目前區域中記錄的事件。如果未選擇此選項，則您的事件資料存放區將包含來自所有區域的事件。

    b. 如果您不希望事件資料存放區開始擷取事件，則取消選取擷取事件。例如，如果您要複製追蹤事件，並且不希望事件資料存放區包含任何未來事件，您可能想要取消選取擷取事件。依預設，事件資料存放區會在建立時開始擷取事件。

16. 如果您的事件資料存放區包括管理事件，您可以選擇下列選項。如需有關管理事件的詳細資訊，請參閱 記錄管理事件。

    a. 選擇是否要包含讀取事件、寫入事件或兩者。至少需要選取一個。

    b. 選擇是否要從事件資料存放區中排除 AWS Key Management Service 或將 Amazon RDS 資料 API 事件排除在外。

    c. 選擇是否啟用 Insights。若要啟用 Insights，您需要設定目的地事件資料存放區，以便依據此事件資料存放區中的管理事件活動收集 Insights 事件。

       如果您選擇啟用 Insights，請執行下列動作。

       i. 在啟用 Insights 中，選擇記錄見 Insights 事件的目的地事件存放區。目的地事件資料存放區將依據此事件資料存放區中的管理事件活動收集 Insights 事件。如需有關如何建立目的地事件資料存放區的資訊，請參閱 若要建立會記錄 Insights 事件的目的地事件資料存放區。

ii. 選擇 Insights 類型。您可以選擇 API 呼叫率、API 錯誤率，或兩者。您必須記錄寫入管理事件，以便記錄 API 呼叫率的 Insights 事件。您必須記錄讀取或寫入管理事件，以便記錄 API 錯誤率的 Insights 事件。

17. 若要在事件資料存放區中包含資料事件，請執行以下操作。

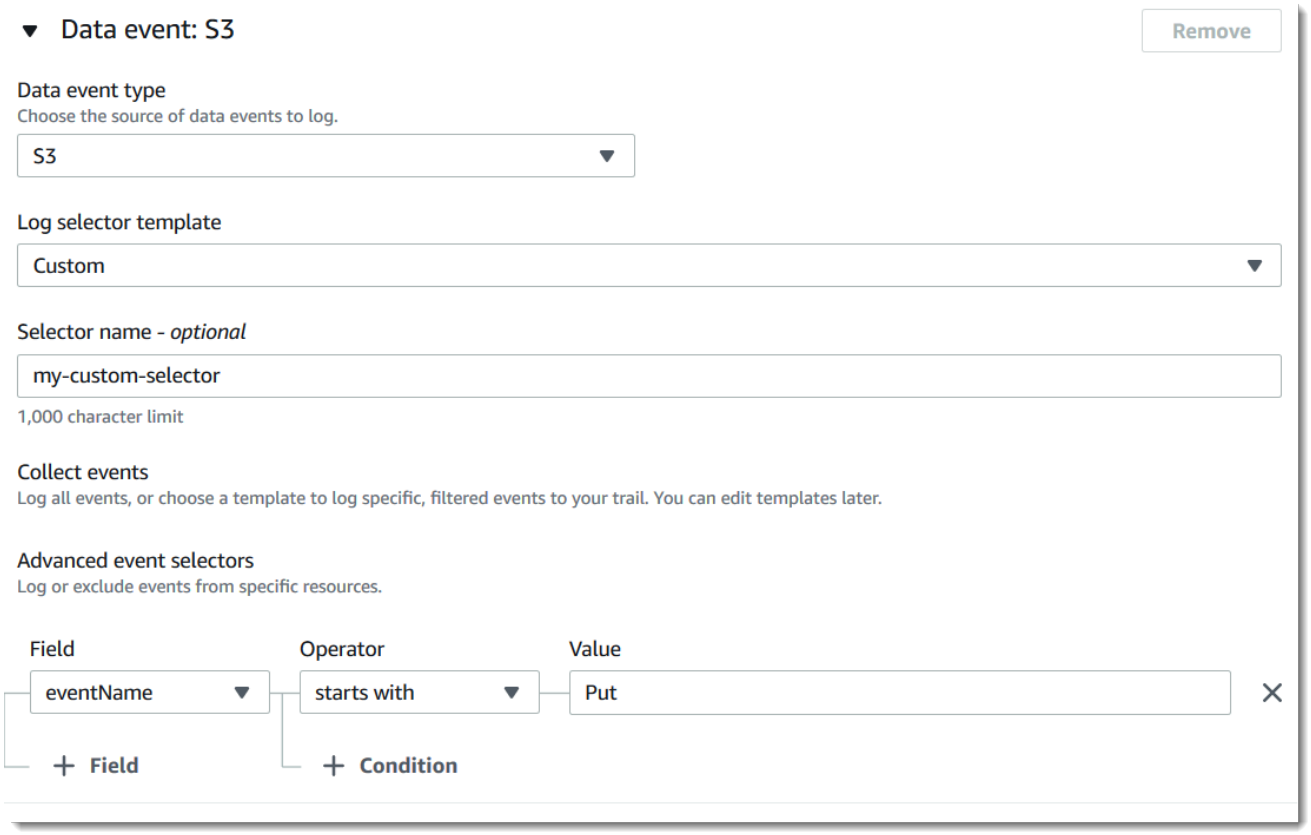
a. 選擇資料事件類型。這是記錄 AWS 服務 資料事件的和資源。若要記錄由 Lake Formation 所建立之 AWS Glue 表格的資料事件，請為資料類型選擇「Lake Formation」。

b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有資料事件、`readOnly` 事件、`writeOnly` 事件或自訂來建置自訂日誌選取器。

c. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 `Name` 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。

d. 在進階事件選取器中，選擇欄位、運算子和值的值來建置表達式 事件資料存放區的進階事件選取器與套用於追蹤的進階事件選取器所運作的方式相同。如需如何建置進階事件選取器的詳細資訊，請參閱使用進階事件選取器篩選資料事件。

以下範例使用自訂日誌選取器範本，只從 S3 物件中選擇以`Put` (例如 `PutObject`) 開頭的事件名稱。由於進階事件選取器不包括或排除其他任何事件類型或資源 ARN，因此事件名稱開頭為 `Put` 的所有 S3 資料事件 (包括讀取和寫入) 都會儲存在事件資料存放區中。



> **Important**
>
> 若要透過使用 S3 儲存貯體 ARN 排除或包含進階事件選取器的資料事件，請始終使用開頭為運算子。

e. 也可選擇展開 JSON 檢視畫面將進階事件選取器視為 JSON 區塊。

f. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。重複步驟 a 到此步驟，以設定資料事件類型的進階事件選取器。

18. 若要將現有追蹤事件複製到您的事件資料存放區，請執行下列操作。

a. 選擇您要複製的追蹤。根據預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前綴。如果您要複製其他前置詞中包含的 CloudTrail 事件，請選擇 [輸入 S3 URI]，然後選擇 [瀏覽 S3] 以瀏覽至首碼。如果追蹤的來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策 CloudTrail 允許解密資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策， CloudTrail 以允許解密儲存貯體中的資料。如需更新 KMS 金鑰政策的詳細資訊，請參閱 用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策。

b. 選擇複製事件的時間範圍。 CloudTrail 在嘗試複製追蹤事件之前，先檢查字首和記錄檔名稱，以確認名稱包含在所選開始日期與結束日期之間的日期。您可以選擇 Relative range (相對範圍) 或 Absolute range (絕對範圍)。若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請選擇早於事件資料存放區建立日期的時間範圍。

> **Note**
>
> CloudTrail 僅複製在事件資料存放區保留期`eventTime`內的追蹤事件。例如，如果事件資料存放區的保留期為 90 天，則不 CloudTrail 會複製任何`eventTime`超過 90 天的追蹤事件。

- 如果您選擇「相對範圍」，則可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。 CloudTrail 複製所選期間內記錄的事件。
- 如果選擇「絕對範圍」，則可以選擇特定的開始和結束日期。 CloudTrail 複製所選開始日期和結束日期之間發生的事件。

c. 對於 Permissions (許可)，從下列 IAM 角色選項中選擇。如果您選擇現有的 IAM 角色，請確認 IAM 角色政策提供必要的許可。如需更新 IAM 角色許可的詳細資訊，請參閱複製追蹤事件的 IAM 許可。

- 選擇 Create a new role (recommended) (建立新角色 (建議使用)) 以建立新的 IAM 角色。在「輸入 IAM 角色名稱」中，輸入角色的名稱。 CloudTrail 會自動為此新角色建立必要的權限。
- 選擇「使用自訂 IAM 角色 ARN」以使用未列出的自訂 IAM 角色。對於 Enter IAM role ARN (輸入 IAM 角色 ARN)，輸入 IAM ARN。
- 從下拉式清單中選擇現有的 IAM 角色。

19. 選擇 Next (下一步) 以檢閱您的選項。
20. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
21. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

    從此開始，事件資料存放區將擷取與其進階事件選取器相符的事件 (如果您保持選取擷取事件選項)。建立事件資料存放區之前發生的事件，不會儲存在事件資料存放區中，除非您選擇複製現有追蹤事件。

您現在可以對新事件資料存放區執行查詢。Sample queries (範例查詢) 索引標籤提供範例查詢，以協助您開始使用。如需建立及編輯查詢的詳細資訊，請參閱 建立或編輯查詢。

您也可以檢視 CloudTrail Lake 儀表板，以視覺化方式呈現事件資料存放區中的事件。如需有關 Lake 儀表板的詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

範例：建立管理事件的事件資料存放區

本逐步解說說明如何建立事件資料存放區，以記錄所有 AWS 區域中的所有管理事件，而且不會記錄任何資料事件。管理事件的範例包括安全事件 (例如 IAM `CreateUser` 和 `AttachRolePolicy` 事件)、資源事件 (例如 `RunInstances` 和 `CreateBucket`) 等等。

若要為管理事件建立事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在「設定事件資料存放區」頁面的「一般」詳細資料中，為您的事件資料存放區命名，例如*`my-management-events-eds`*。根據最佳實務，請使用可快速識別事件資料存放區目的的名稱。如需 CloudTrail 命名需求的資訊，請參閱命名要求。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天

6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

7. (選用) 在加密中，選擇您是否想要使用自己的 KMS 金鑰加密事件資料存放區。依預設，事件資料存放區中的所有事件都會 CloudTrail 使用為您 AWS 擁有和管理的 KMS 金鑰加密。

   若要啟用使用您自己的 KMS 金鑰加密，請選擇使用我自己的 AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

   > **Note**
   >
   > 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

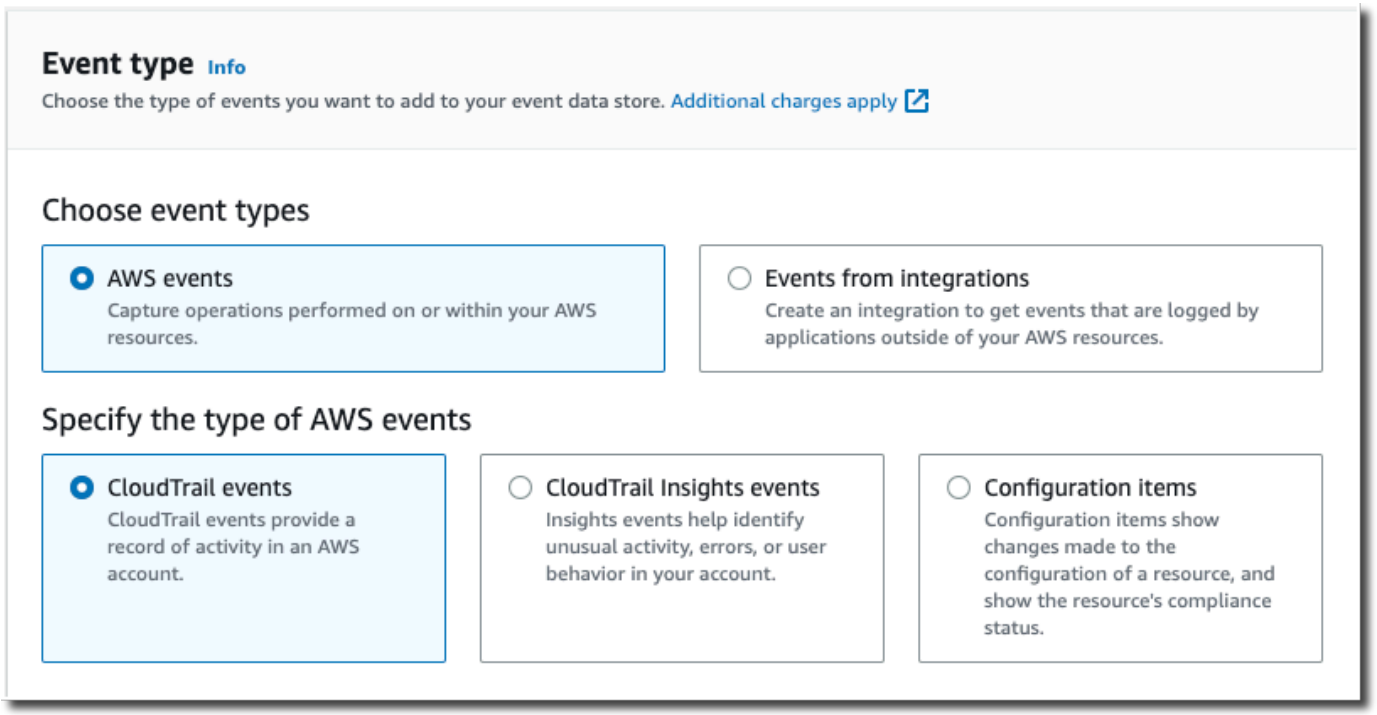
   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的事件資料存放區。標籤可協助您識別 CloudTrail 事件資料存放區。例如，您可以附加名稱為 **`stage`**，值為 **`prod`** 的標籤。您可以使用

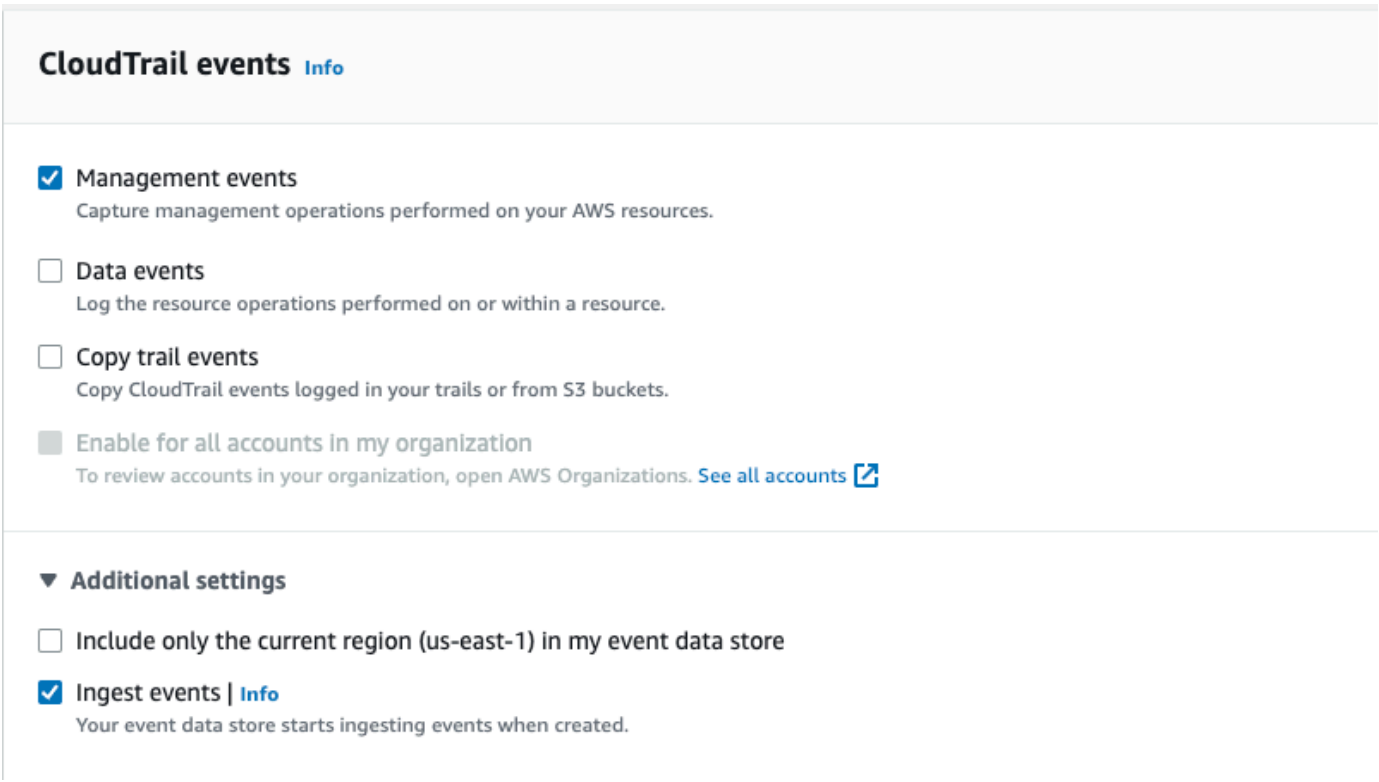
標籤來限制對事件資料存放區的存取。您還可以使用標籤來追蹤事件資料存放區的查詢和擷取成本。

如需有關如何使用標籤追蹤成本的資訊，請參閱 為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置。如需有關如何使用 IAM 政策，對以標籤為基礎的事件資料存放區授予存取權的資訊，請參閱 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱《標記資 AWS 源使用指南》中的〈標記 AWS 資源〉。

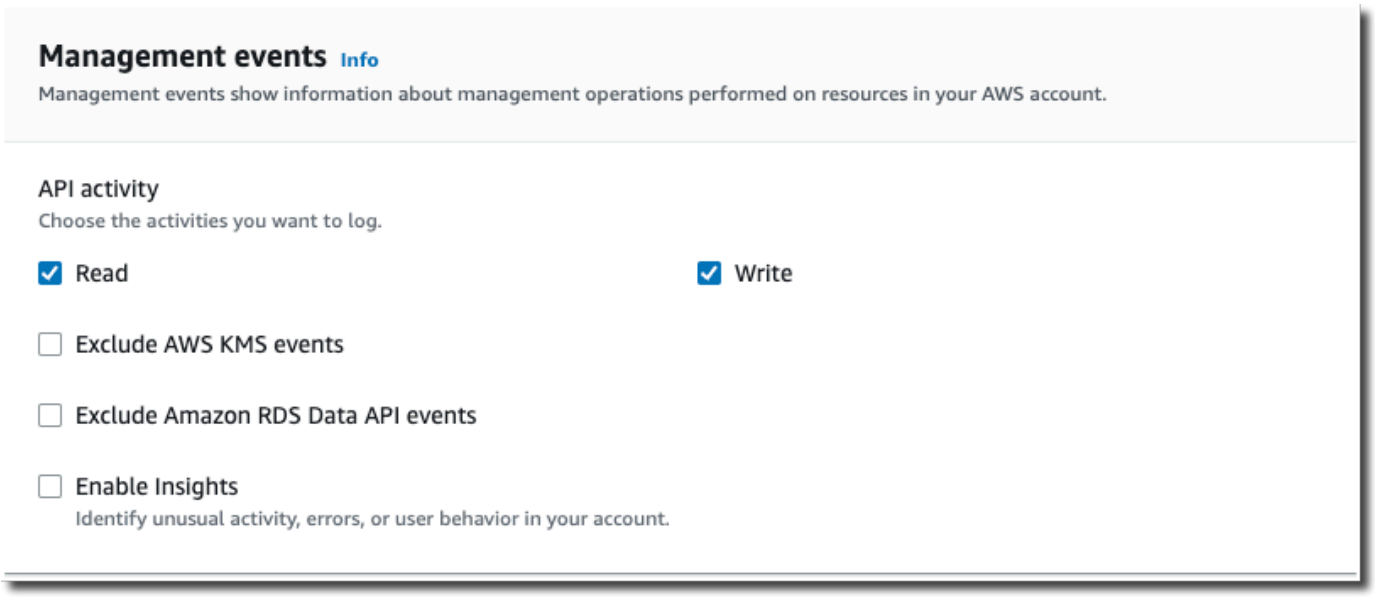
10. 選擇 Next (下一步) 以設定事件資料存放區。
11. 在選擇事件頁面上，保留事件類型的預設選項。



12. 對於CloudTrail 事件，請保留預設選項。依預設， CloudTrail 事件資料儲存區會收集管理事件，而不會收集資料事件。如需有關管理事件的詳細資訊，請參閱 記錄管理事件。如需有關資料事件的詳細資訊，請參閱 記錄資料事件。



13. 保留複製追蹤事件的預設設定。您可以使用此選項，將現有追蹤事件複製到您的事件資料存放區。如需詳細資訊，請參閱 將追蹤事件複製到事件資料存放區。
14. 如果這是組織事件資料存放區，選擇針對組織中的所有帳戶啟用。除非您已在 AWS Organizations 中設定帳戶，否則此選項將無法變更。
15. 對於其他設定，保留預設選項。依預設，事件資料存放區會為所有人收集事件， AWS 區域 並在建立事件時開始擷取事件。
16. 在管理事件中，選擇同時收集讀取和寫入事件。將排除 AWS KMS 事件和排除 Amazon RDS 資料 API 事件的核取方塊保留空白，以收集所有管理事件。不勾選啟用 Insights 事件核取方塊。



17. 選擇 Next (下一步) 以檢閱您的選項。
18. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
19. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

    從此開始，事件資料存放區將擷取與其進階事件選取器相符的事件。建立事件資料存放區之前發生的事件，不會儲存在事件資料存放區中，除非您選擇複製現有追蹤事件。

範例：為 S3 資料事件建立事件資料存放區

本逐步解說說明如何為 Amazon S3 資料事件建立事件資料存放區。在此案例中，我們不會記錄所有 Amazon S3 資料事件，而是選擇自訂日誌選取器範本，僅在從特定 S3 儲存貯體刪除物件時記錄事件。

若要為 S3 資料事件建立事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在 [設定事件資料存放區] 頁面的 [一般詳細資料] 中，為您的事件資料存放區命名，例如 *s3-data-events-eds*。根據最佳實務，請使用可快速識別事件資料存放區目的的名稱。如需 CloudTrail 命名需求的資訊，請參閱命名要求。

5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`
7. (選用) 在加密中，選擇您是否想要使用自己的 KMS 金鑰加密事件資料存放區。依預設，事件資料存放區中的所有事件都會 CloudTrail 使用為您 AWS 擁有和管理的 KMS 金鑰加密。

   若要啟用使用您自己的 KMS 金鑰加密，請選擇使用我自己的 AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

> **Note**
>
> 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

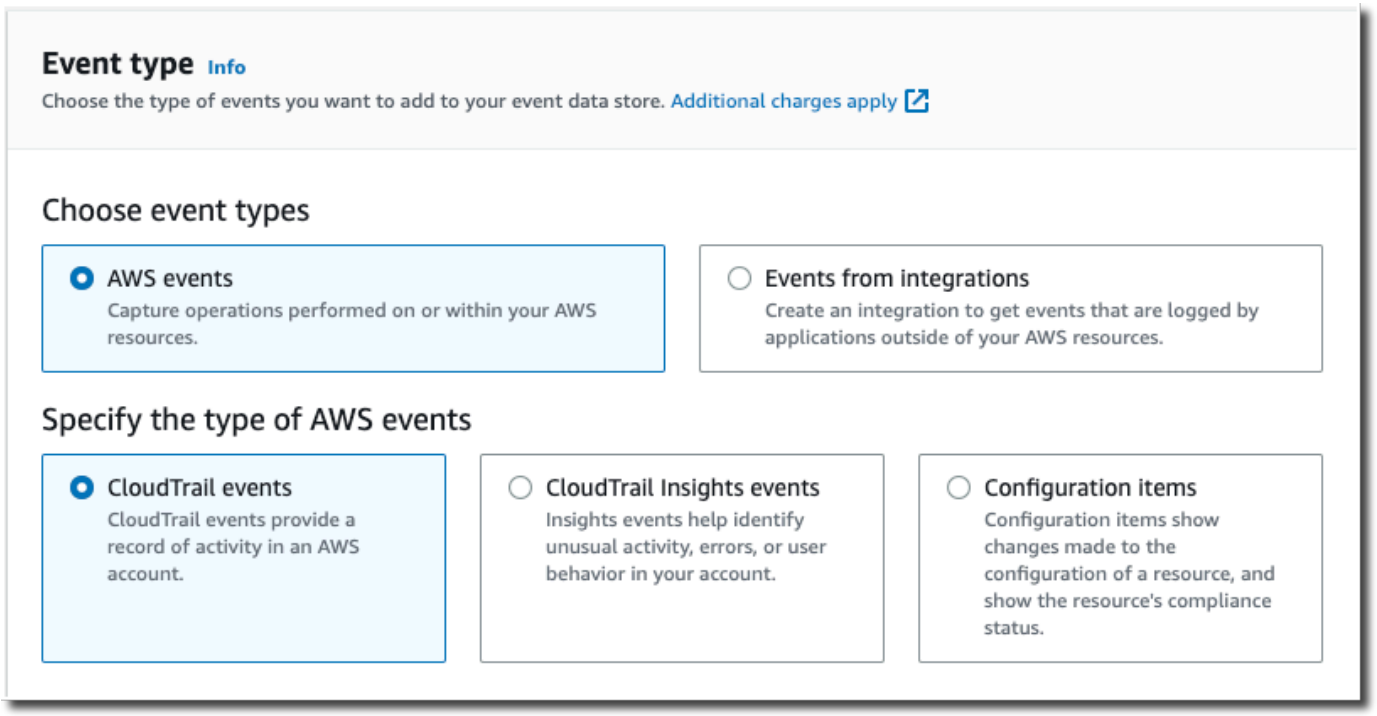
   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的事件資料存放區。標籤可協助您識別 CloudTrail 事件資料存放區。例如，您可以附加名稱為 **`stage`**，值為 **`prod`** 的標籤。您可以使用標籤來限制對事件資料存放區的存取。您還可以使用標籤來追蹤事件資料存放區的查詢和擷取成本。

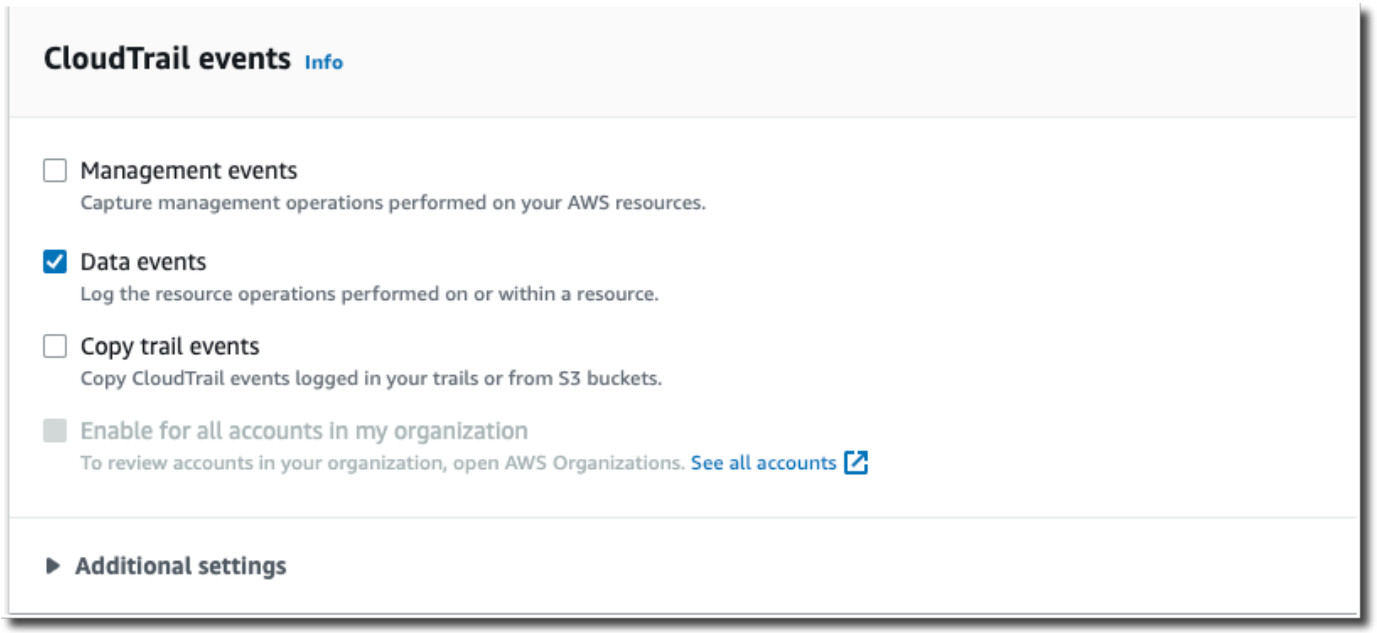
   如需有關如何使用標籤追蹤成本的資訊，請參閱 為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置。如需有關如何使用 IAM 政策，對以標籤為基礎的事件資料存放區授予存取權的資訊，請參閱 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱《標記資 AWS 源使用指南》中的〈標記 AWS 資源〉。

10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在選擇事件頁面上，保留事件類型的預設選項。



12. 對於CloudTrail 事件，請選擇資料事件並取消選取管理事件。如需有關資料事件的詳細資訊，請參閱 記錄資料事件。



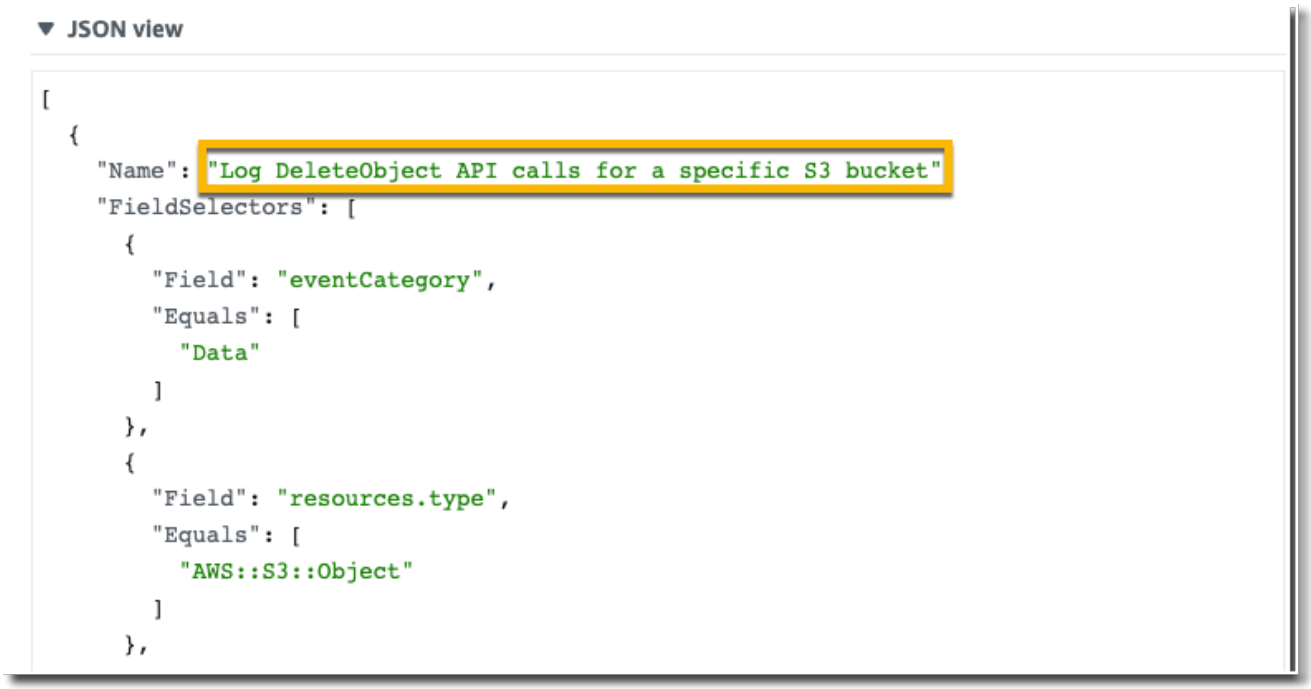
13. 保留複製追蹤事件的預設設定。您可以使用此選項，將現有追蹤事件複製到您的事件資料存放區。如需詳細資訊，請參閱 將追蹤事件複製到事件資料存放區。
14. 如果這是組織事件資料存放區，選擇針對組織中的所有帳戶啟用。除非您已在 AWS Organizations 中設定帳戶，否則此選項將無法變更。

15. 對於其他設定，保留預設選項。依預設，事件資料存放區會為所有人收集事件， AWS 區域 並在建立事件時開始擷取事件。
16. 對於資料事件，請執行下列選擇：

    a. 在資料事件類型中，選擇 S3。資料事件類型可識別記錄資料事件的 AWS 服務 和資源。

    b. 在日誌選取器範本中，選擇自訂。選擇自訂讓您可以定義用於篩選 `eventName`、`resources.ARN` 和 `readOnly` 欄位的自訂事件選取器。如需這些欄位的詳細資訊，請AdvancedFieldSelector參閱 AWS CloudTrail API 參考中的。

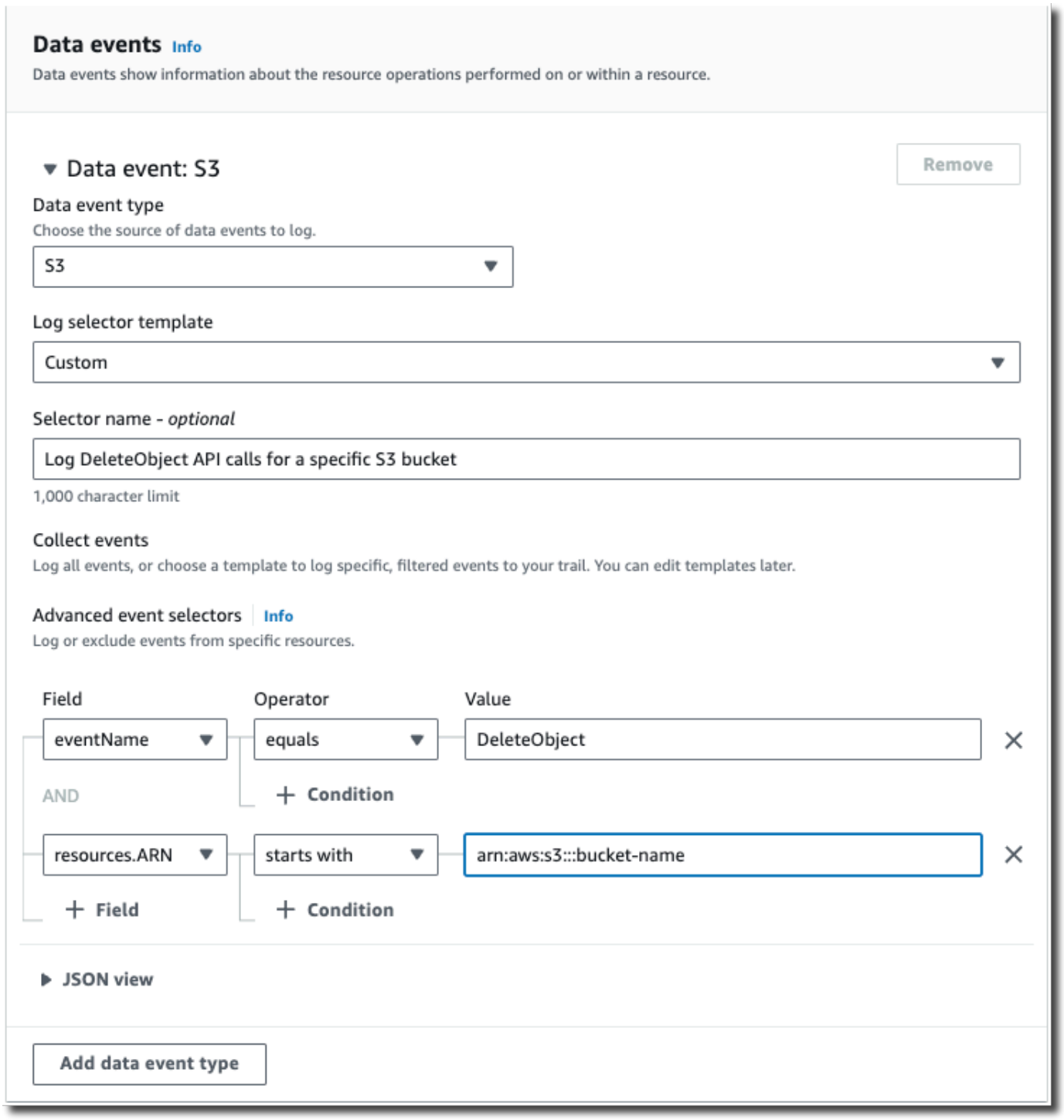
    c. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選取器的描述性名稱，例如「特定 S3 儲存貯體的記錄 DeleteObject API 呼叫」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。



    d. 在高級事件選擇器中，我們將構建自定義事件選擇器以對`eventName`和`resources.ARN`字段進行過濾。事件資料存放區的進階事件選取器與套用於追蹤的進階事件選取器所運作的方式相同。如需建立進階事件選取器的詳細資訊，請參閱使用進階事件選取器記錄資料事件。

        i. 對於欄位，選擇 eventName。對於運算子，選擇 equals。針對數值，輸入 **`DeleteObject`**。選擇 [+ 欄位] 以篩選另一個欄位。

        ii. 對於欄位，選擇 resources.ARN。對於「運算子」，選擇StartsWith。對於值，輸入您的儲存貯體的 ARN (例如 *`arn:aws:s3:::bucket-name`*)。如需有關如何取得 ARN 的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 資源。



17. 選擇 Next (下一步) 以檢閱您的選項。
18. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
19. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

從此開始，事件資料存放區將擷取與其進階事件選取器相符的事件。建立事件資料存放區之前發生的事件，不會儲存在事件資料存放區中，除非您選擇複製現有追蹤事件。

使用主控台為 CloudTrail Insights 事件建立事件資料存放區

AWS CloudTrail 透過持續分析 CloudTrail 管理事件，深入解析可協助 AWS 使用者識別並回應與 API 呼叫和 API 錯誤率相關的異常活動。 CloudTrail 洞察分析您的 API 呼叫量和 API 錯誤率的正常模式（也稱為基準），並在呼叫量或錯誤率超出正常模式時生成 Insights 事件。其會針對 `write` 管理 API 產生 API 呼叫量的 Insights 事件，並針對 `read` 和 `write` 管理 API 產生 API 錯誤率的 Insights 事件。

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要記錄 Insights 事件的目標事件資料存放區，以及啟用見解和記錄管理事件的來源事件資料存放區。

> **Note**
>
> 若要在 API 呼叫量上記錄 Insights 事件，來源事件資料存放區必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，來源事件資料存放區必須記錄 `read` 或 `write` 管理事件。

如果您在來源事件資料存放區上啟用了 CloudTrail Insights 並 CloudTrail 偵測到異常活動，則會將 Insights 事件 CloudTrail 傳送至目的地事件資料存放區。與 CloudTrail 事件資料存放區中擷取的其他類型事件不同，Insights 事件只有在 CloudTrail 偵測到帳戶 API 使用量與帳戶的典型使用模式明顯不同時，才會記錄 Insights 事件。

在事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能傳遞第一個 Insights 事件。

CloudTrail Insights 會分析單一區域 (而非全球) 中發生的管理事件。In CloudTrail sights 事件會在與產生其支援管理事件的相同區域中產生。

對於組織事件資料存放區，分 CloudTrail 析來自每個成員帳戶的管理事件，而不是分析組織所有管理事件的彙總。

在 CloudTrail 湖泊擷取見解事件需要支付額外費用。如果您同時針對追蹤和 CloudTrail Lake 事件資料存放區啟用深入解析，則需另行付費。如需 CloudTrail 定價的相關資訊，請參閱AWS CloudTrail 定價。

主題

- 若要建立會記錄 Insights 事件的目的地事件資料存放區
- 若要建立會啟用 Insights 事件的來源事件資料存放區

若要建立會記錄 Insights 事件的目的地事件資料存放區

在建立 Insights 事件資料存放區時，您可以選擇一個記錄管理事件的現有來源事件資料存放區，然後指定想要接收的 Insights 類型。或者，您也可以在建立 Insights 事件資料存放區後啟用新的或現有事件資料存放區上的 Insights，然後選擇此事件資料存放區作為目的地事件資料存放區。

此程序將向您說明如何建立記錄 Insights 事件的目的地事件資料存放區。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，開啟 Lake 子選單，然後選擇 Event data stores (事件資料存放區)。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在設定事件資料存放區頁面上的一般詳細資訊中，輸入事件資料存放區的名稱。名稱為必填。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期間 (以天為單位)。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。事件資料存放區會在指定的天數內保留事件資料。
7. (選擇性) 若要啟用加密方式 AWS Key Management Service，請選擇 [使用我自己的] AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS

別名中，以格式指定別名`alias/MyAliasName`。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

> **Note**
>
> 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在 Tags (標籤) 區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對事件資料存放區的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱標記資 AWS 源使用指南中的標記 AWS 資源。

10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在 [選擇事件] 頁面上，選擇AWS 事件，然後選擇 [CloudTrail見解事件]。

12. 在CloudTrail 深入解析事件中，執行下列動作。

    a. 如果您想要為組織的委派管理員授予存取此事件資料存放區的權限，則選擇允許委派管理員存取權。只有當您使用 AWS Organizations 組織的管理帳戶登入時，才能使用此選項。

    b. (選用) 選擇記錄管理事件的現有來源事件資料存放區，並指定您想要接收的 Insights 類型。

若要新增來源事件資料存放區，請執行下列動作。

i. 選擇新增來源事件資料存放區。

ii. 選擇來源事件資料存放區。

iii. 選擇您想要接收的 Insights 類型。

- `ApiCallRateInsight` – `ApiCallRateInsight` Insights 類型會分析針對基準 API 呼叫量彙總的每分鐘唯寫管理 API 呼叫。若要接收 `ApiCallRateInsight` 上的 Insights，來源事件資料存放區必須記錄寫入管理事件。
- `ApiErrorRateInsight` – `ApiErrorRateInsight` Insights 類型會分析導致錯誤碼的管理 API 呼叫。如果 API 呼叫失敗，則顯示錯誤。若要接收 `ApiErrorRateInsight` 上的 Insights，來源事件資料存放區必須記錄寫入或讀取管理事件。

iv. 重複前兩個步驟 (ii 和 iii)，以新增任何您想要接收的其他 Insights 類型。

13. 選擇 Next (下一步) 以檢閱您的選項。
14. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
15. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。
16. 如果您在步驟 10 中未選擇來源事件資料存放區，請依照 若要建立會啟用 Insights 事件的來源事件資料存放區 中的步驟來建立一個來源事件資料存放區。

若要建立會啟用 Insights 事件的來源事件資料存放區

此程序將向您說明如何建立會啟用 Insights 事件並記錄管理事件的來源事件資料存放區。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，開啟 Lake 子選單，然後選擇 Event data stores (事件資料存放區)。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在設定事件資料存放區頁面上的一般詳細資訊中，輸入事件資料存放區的名稱。名稱為必填。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

- 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
  - 預設保留期：366 天
  - 最長保留期：3,653 天
- 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
  - 預設保留期：2,557 天
  - 最長保留期：2,557 天

6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

7. (選擇性) 若要啟用加密方式 AWS Key Management Service，請選擇 [使用我自己的] AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/MyAliasName`。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

   > **Note**
   >
   > 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

b. 如果您要建立新角色，請輸入名稱以識別角色。

c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在 Tags (標籤) 區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對事件資料存放區的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱標記資 AWS 源使用指南中的標記 AWS 資源。

10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在 [選擇事件] 頁面上，選擇AWS 事件，然後選擇CloudTrail事件。

12. 在CloudTrail 事件中，保持選取「管理」事件。

13. 若要讓事件資料存放區從 AWS Organizations 組織中的所有帳戶收集事件，請選取 Enable for all accounts in my organization (啟用我組織中的所有帳戶)。您必須登入到組織的管理帳戶，才能建立會啟用 Insights 的事件資料存放區。

14. 展開其他設定以選擇是要讓事件資料存放區收集所有事件 AWS 區域，還是僅收集目前事件的事件 AWS 區域，然後選擇事件資料儲存庫是否擷取事件。依預設，您的事件資料存放區會從帳戶的所有區域收集事件，而且會在建立時開始擷取事件。

    a. 如果您希望僅包括目前區域中記錄的事件，請選擇在我的事件資料存放區中僅包含目前區域。如果未選擇此選項，則您的事件資料存放區將包含來自所有區域的事件。

    b. 維持選取擷取事件。

15. 選擇您想要包含在事件資料存放區內的管理事件類型。您可以選擇讀取、寫入，或兩者。至少需要選取一個。

    > **Note**
    >
    > 若要在 API 呼叫量上記錄 Insights 事件，事件資料存放區必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，事件資料存放區必須記錄 `read` 或 `write` 管理事件。

16. 您可以選擇從事件資料存放區中排除 AWS Key Management Service 或從事件資料存放區排除 Amazon RDS 資料 API 事件。如需關於這些選項的詳細資訊，請參閱 記錄管理事件。

17. 選擇啟用 Insights。

18. 在啟用 Insights 中，選擇記錄見 Insights 事件的目的地事件存放區。目的地事件資料存放區將依據此事件資料存放區中的管理事件活動收集 Insights 事件。如需有關如何建立目的地事件資料存放區的資訊，請參閱 若要建立會記錄 Insights 事件的目的地事件資料存放區。
19. 選擇 Insights 類型。您可以選擇 API 呼叫率、API 錯誤率，或兩者。您必須記錄寫入管理事件，以便記錄 API 呼叫率的 Insights 事件。您必須記錄讀取或寫入管理事件，以便記錄 API 錯誤率的 Insights 事件。
20. 選擇 Next (下一步) 以檢閱您的選項。
21. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
22. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

    從此開始，事件資料存放區將擷取與其進階事件選取器相符的事件。在來源事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間，才能將第一個 Insights 事件傳送至目的地事件資料存放區。

    您可以檢視 CloudTrail Lake 儀表板，以視覺化方式呈現目標事件資料存放區中的 Insights 事件。如需有關 Lake 儀表板的詳細資訊，請參閱 檢視 CloudTrail 湖泊儀表板。

在 CloudTrail 湖泊擷取見解事件需要支付額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需 CloudTrail 定價的相關資訊，請參閱AWS CloudTrail 定價。

使用主控台建立 AWS Config 組態項目的事件資料存放區

您可以建立事件資料存放區以包含 AWS Config 組態項目，並使用事件資料存放區來調查您生產環境的不合規變更。使用事件資料存放區，您可以將不合規的規則，和與變更相關的使用者和資源建立關聯。組態項目代表您帳號中存在之受支援 AWS 資源的屬性 point-in-time 檢視。 AWS Config 每當它偵測到它正在記錄的資源類型的變更時，就會建立組態項目。 AWS Config 也會在擷取組態快照時建立組態項目。

您可以同時使用 AWS Config 和 CloudTrail Lake 來針對組態項目執行查詢。您可以使 AWS Config 用根據單一和 (或) 跨多個帳戶 AWS 帳戶 和 AWS 區域區域的組態屬性來查詢 AWS 資源的目前組態狀態。相反地，您可以使用 CloudTrail Lake 查詢各種資料來源，例如 CloudTrail 事件、設定項目和規則評估。 CloudTrail Lake 查詢涵蓋所有 AWS Config 組態項目，包括資源組態和符合性歷程記錄

為設定項目建立事件資料存放區不會影響現有的 AWS Config 進階查詢或任何設定的 AWS Config 彙總工具。您可以繼續使用執行進階查詢 AWS Config，並繼 AWS Config 續將歷史檔案傳遞至 S3 儲存貯體。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

限制

以下限制適用於組態項目的事件資料存放區。

- 不支援自訂組態項目
- 不支援使用進階事件選取器進行事件篩選

必要條件

建立活動資料存放區之前，請先為您的所有帳戶和區域設定 AWS Config 記錄。您可以使用「快速設定」功能 AWS Systems Manager，快速建立搭載的組態記錄程式 AWS Config。

> **Note**
>
> AWS Config 開始錄製配置時，您需要支付服務使用費。如需定價的詳細資訊，請參閱 AWS Config 定價。如需管理組態記錄器的詳細資訊，請參閱《AWS Config 開發人員指南》中的管理組態記錄器。

此外，建立事件資料存放區時，建議您執行下列動作，但並非必要。

- 設定 Amazon S3 儲存貯體於請求時接收組態快照及組態歷史記錄。如需快照的詳細資訊，請參閱《AWS Config 開發人員指南》中的管理交付通道和將組態快照交付至 Amazon S3 儲存貯體。
- 指定您要用 AWS Config 來評估已記錄資源類型之符合性資訊的規則。 AWS Config 要 AWS Config 規則 求評估 AWS 資源合規狀態的幾個 CloudTrail Lake 範例查詢。如需詳細資訊 AWS Config 規則，請參閱AWS Config 開發人員指南 AWS Config 規則中的使用評估資源。

若要為組態項目建立事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。

3. 選擇 Create event data store (建立事件資料存放區)。
4. 在設定事件資料存放區頁面上的一般詳細資訊中，輸入事件資料存放區的名稱。名稱為必填。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`
7. (選擇性) 若要啟用加密方式 AWS Key Management Service，請選擇 [使用我自己的] AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

   > **Note**
   >
   > 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在 Tags (標籤) 區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對事件資料存放區的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱標記資 AWS 源使用指南中的標記 AWS 資源。

10. 選擇下一步。

11. 在選擇事件頁面上，選擇 AWS 事件，然後選擇組態項目。

12. CloudTrail 將事件資料倉庫資源儲存在您建立該資源的「區域」中，但依預設，在資料倉庫中收集的組態項目來自您帳戶中啟用記錄的所有區域。或者，您也可以選擇 Include only the current region in my event data store (在我的事件資料存放區中僅包含目前區域) 以僅包括在目前區域中擷取的組態項目。如果未選擇此選項，則事件資料存放區將包含來自已啟用記錄的所有區域的事件。

13. 若要讓您的事件資料儲存庫從 AWS Organizations 組織中的所有帳戶收集組態項目，請選取為組織中的所有帳戶啟用。您必須登入到組織的管理帳戶或委派的管理員帳戶，才能建立為組織收集組態項目的事件資料存放區。

14. 選擇 Next (下一步) 以檢閱您的選項。

15. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。

16. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

    從此時開始，事件資料存放區將擷取組態項目。建立事件資料存放區之前發生的組態項目，不會儲存在事件資料存放區中。

範例查詢

您現在可以對新事件資料存放區執行查詢。 CloudTrail 主控台上的 [範例查詢] 索引標籤提供範例查詢以協助您開始使用。以下是一些您可針對組態項目事件資料存放區執行的範例查詢。

描述	Query
透過將組態項目事件資料存放區與事件資料存放區加入組態項目事件資料存放區，以尋找執行導致不合規狀態的動作。 CloudTrail	SELECT element_at(config1.eventDat a.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventDat a.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM *config_event_data_store_ID* as config1 JOIN *config_event_data_store_ID* as config2 on element_at(config1 .eventData.configuration, 'targetRe sourceId') = config2.eventData. resourceId JOIN *cloudtrail_event_data_store_ID* as cloudtrail on config2.eventData. arn = element_at(cloudtrail.resou rces, 1).arn WHERE element_at(config1.eventDat a.configuration, 'configRuleList') is not null AND element_at(config1.eventDat a.configuration, 'complianceType') = 'NON_COMPLIANT' AND cloudtrail.eventTime > '2022-11- 14 00:00:00' AND

描述	Query
	`config2.eventData.resourceType = 'AWS::DynamoDB::Table'`
尋找所有 AWS Config 規則，並從過去一天內產生的組態項目傳回符合性狀態。	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceName, eventData.resourceCreationTime, element_at(eventData.configuration,'complianceType') AS complianceType, element_at(eventData.configuration, 'configRuleList') AS configRuleList, element_at(eventData.configuration, 'resourceId') AS resourceId, element_at(eventData.configuration, 'resourceType') AS resourceType FROM config_event_data_store_ID WHERE eventData.resourceType = 'AWS::Config::ResourceCompliance' AND eventTime > '2022-11-22 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10`

描述	Query
依 AWS Config 資源類型、帳號 ID 和區域來搜尋資源總數。	`SELECT eventData.resourceType, eventData.awsRegion, eventData.accountId, COUNT (*) AS resourceCount FROM config_event_data_store_ID WHERE eventTime > '2022-11-22 00:00:00' GROUP BY eventData.resourceType, eventData.awsRegion, eventData.accountId`
尋找在特定日期產生之所有 AWS Config 組態料號的資源建立時間。	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceId, eventData.resourceName, eventData.resourceType, eventData.availabilityZone, eventData.resourceCreationTime FROM config_event_data_store_ID WHERE eventTime > '2022-11-16 00:00:00' AND eventTime < '2022-11-17 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10;`

如需建立及編輯查詢的詳細資訊，請參閱 建立或編輯查詢。

組態項目結構描述

下表說明符合組態項目記錄中的必要和選用結構描述元素。的內容由您eventData的組態項目提供；其他欄位則由擷取 CloudTrail 後提供。

CloudTrail 事件記錄內容在中有更詳細的說明CloudTrail 記錄內容。

- 擷取 CloudTrail 後提供的欄位
- 您的事件提供的欄位

擷取 CloudTrail 後提供的欄位

欄位名稱	輸入類型	需求	描述
eventVersion	string	必要	AWS 事件格式的版本。
eventCategory	string	必要	事件類別。對於組態項目，有效值為 ConfigurationItem 。
eventType	string	必要	事件類型。對於組態項目，有效值為 AwsConfigurationItem 。
eventID	string	必要	事件的唯一 ID。
eventTime	string	必要	事件時間戳記，採用 yyyy-MM-DDTHH:mm:ss 格式和國際標準時間 (UTC)。
awsRegion	string	必要	AWS 區域 要指派事件的目標。

欄位名稱	輸入類型	需求	描述
recipientAccountId	string	必要	表示接收此事件的 AWS 帳戶 ID。
附錄	附錄	選用	顯示事件延遲原因的相關資訊。如果現有事件中缺少資訊，則附錄區塊會包含缺少的資訊，以及缺失的原因。

`eventData` 中的欄位由您的組態項目提供

欄位名稱	輸入類型	需求	描述
eventData	-	必要	eventData 中的欄位由您的組態項目提供。
• configurationItemVersion	string	選用	來自其來源的組態項目版本。
• configurationItemCapture時間	string	選用	初始化組態記錄的時間。
• configurationItemStatus	string	選用	組態項目狀態。有效值為OK、ResourceDiscovered 、ResourceNotRecorded 、 ResourceDeleted 、ResourceDeletedNotRecorded 。
• accountId	string	選用	與資源關聯的 12 位數 AWS 帳戶 ID。

欄位名稱	輸入類型	需求	描述
• resourceType	string	選用	AWS 資源的類型。如需有效資源類型的詳細資訊，請參閱 AWS Config API 參考ConfigurationItem中的。
• resourceId	string	選用	資源的 ID (例如，sg-*xxxxxx*)。
• resourceName	string	選用	資源的自訂名稱 (若有)。
• arn	string	選用	與資源關聯的 Amazon Resource Name (ARN)。
• awsRegion	string	選用	資源所 AWS 區域 在的位置。
• availabilityZone	string	選用	與資源關聯的可用區域。
• resourceCreationTime	string	選用	建立資源時的時間戳記。
• 組態	JSON	選用	資源組態的描述。
• supplementaryConfiguration	JSON	選用	針對特定資源類型傳 AWS Config 回的組態屬性，以補充組態參數傳回的資訊。
• relatedEvents	string	選用	CloudTrail 事件識別碼的清單。
• relationships	-	選用	相關資 AWS 源清單。

欄位名稱	輸入類型	需求	描述
• • name	string	選用	與相關資源的關係類型。
• • resourceType	string	選用	相關資源的資源類型。
• • resourceId	string	選用	相關資源的 ID (例如，sg-*xxxxxx*)。
• • resourceName	string	選用	相關資源的自訂名稱 (若有)。
• 標籤	JSON	選用	與資源相關聯的鍵值標籤對應。

以下範例說明與組態項目記錄相符的結構描述元素的階層。

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
```

```
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
       JSON
     }
    }
  }
}
```

AWS 使用主控台為外部事件建立事件資料存放區

您可以建立事件資料倉庫以包括以外的事件 AWS，然後使用 CloudTrail Lake 搜尋、查詢和分析從應用程式記錄的資料。

您可以使用 CloudTrail Lake 整合功能，從混合式環境中的 AWS任何來源記錄和儲存使用者活動資料，例如內部部署或雲端中託管的 SaaS 應用程式、虛擬機器或容器。

當您為整合建立事件資料存放區時，也會建立通道，並將資源政策連接到通道。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

若要為以外的事件建立事件資料倉庫 AWS

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。

2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在設定事件資料存放區頁面上的一般詳細資訊中，輸入事件資料存放區的名稱。名稱為必填。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`
7. (選擇性) 若要啟用加密方式 AWS Key Management Service，請選擇 [使用我自己的] AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

> **Note**
>
> 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

   a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

   b. 如果您要建立新角色，請輸入名稱以識別角色。

   c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

9. (選用) 在 Tags (標籤) 區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對事件資料存放區的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱標記資 AWS 源使用指南中的標記 AWS 資源。

10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在 Choose events (選擇事件) 頁面上，選擇 Events from integrations (來自整合的事件)。

12. 從 Events from integration (來自整合的事件) 中，選擇要將事件傳送至事件資料存放區的來源。

13. 提供名稱以識別整合的通道。名稱長度範圍是 3-128 個字元。只能使用字母、數字、句號、底線和破折號。

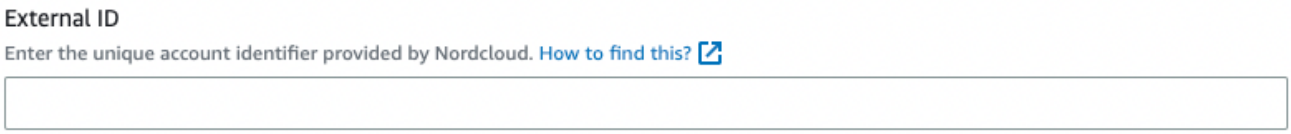
14. 在 Resource policy (資源政策) 中，為整合的通道設定資源政策。資源政策是 JSON 政策文件，這些文件會指出指定的主體可對資源執行哪些動作以及相關條件。在資源政策中定義為主體的帳戶可以呼叫 `PutAuditEvents` API，將事件傳送至您的通道。如果資源擁有者的 IAM 政策允許 `cloudtrail-data:PutAuditEvents` 動作，則資源擁有者對資源具有隱含存取權。

    政策所需的資訊取決於整合類型。若要進行方向整合， CloudTrail 會自動新增合作夥伴的 AWS 帳戶 ID，並要求您輸入合作夥伴提供的唯一外部 ID。對於解決方案整合，您必須至少指定一個 AWS 帳戶 ID 作為主體，並且可以選擇性地輸入外部 ID 以防止混淆的副手。

> **Note**
>
> 如果您沒有為通道建立資源政策，則只有通道擁有者可以在通道上呼叫 `PutAuditEvents` API。

a. 對於直接整合，請輸入合作夥伴提供的外部 ID。整合合作夥伴提供唯一外部 ID，例如帳戶 ID 或隨機產生的字串，以供整合用於預防混淆代理人。合作夥伴負責建立並提供唯一外部 ID。

   您可以選擇 How to find this? (如何尋找此資訊？) 以檢視合作夥伴有關描述如何尋找外部 ID 的文件。



> **Note**
>
> 如果資源政策包含外部 ID，則對 `PutAuditEvents` API 的所有呼叫都必須包含外部 ID。不過，如果政策未定義外部 ID，合作夥伴仍可呼叫 `PutAuditEvents` API 並指定 `externalId` 參數。

b. 對於解決方案整合，請選擇 [新增 AWS 帳戶] 以指定要新增為策略中主體的每個 AWS 帳戶 ID。

15. 選擇 Next (下一步) 以檢閱您的選項。
16. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
17. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。
18. 提供通道 Amazon Resource Name (ARN) 給合作夥伴應用程式。如需將通道 ARN 提供給合作夥伴應用程式的說明，請參閱合作夥伴文件網站。如需詳細資訊，請在 Integrations (整合) 頁面的 Available sources (可用來源) 索引標籤中選擇合作夥伴的 Learn more (進一步了解) 連結，以在 AWS Marketplace中開啟合作夥伴的頁面。

當您、合作夥伴或合作夥伴應用程式呼叫 CloudTrail 通道上的 `PutAuditEvents` API 時，事件資料存放區就會開始透過整合的通道擷取合作夥伴事件。

使用主控台更新事件資料存放區

本節說明如何使用 AWS Management Console更新事件資料存放區的設定。若要取得有關如何使用更新事件資料倉庫的資訊 AWS CLI，請參閱使用更新事件資料倉庫 AWS CLI。

更新事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇您要更新的事件資料存放區。此動作會開啟事件資料存放區的詳細資訊頁面。
4. 在一般詳細資訊中，選擇編輯以變更下列設定：

   - 事件資料存放區名稱 – 變更可識別事件資料存放區的名稱。
   - 定價選項 – 對於使用七年保留定價選項的事件資料存放區，您可以改為選擇使用一年可延長保留定價。如果事件資料存放區每月擷取的事件資料少於 25 TB，建議您使用一年可延長保留定價。如果您需要長達 10 年的彈性保留期，同樣建議您使用一年可延長保留定價。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

     > **Note**
     >
     > 對於使用一年可延長保留定價的事件資料存放區，您無法變更其定價選項。如果您要使用七年保留定價，請在事件資料存放區上停止擷取。然後，使用七年保留定價選項建立新的事件資料存放區。

   - 保留期 – 變更事件資料存放區的保留期。保留期將決定事件資料保留在事件資料存放區中的時間長度。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

     > **Note**
     >
     > 如果您縮短事件資料存放區的保留期間， CloudTrail 將會移除任何`eventTime`早於新保留期的事件。例如，如果先前的保留期為 365 天，而您將其減少到 100 天，則 CloudTrail 會移除`eventTime`超過 100 天的事件。

   - 加密 – 若要使用您自己的 KMS 金鑰來加密事件資料存放區，請選擇使用我自己的 AWS KMS key。依預設，事件資料存放區中的所有事件均由加密 CloudTrail。使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。

> **Note**
>
> 將事件資料存放區與 KMS 金鑰建立關聯後，您便無法移除或變更 KMS 金鑰。

- 若只要包含目前 AWS 區域中記錄的事件，請選擇在我的事件資料存放區中僅包含目前區域。如果您未選擇此選項，則事件資料存放區將包含來自所有區域的事件。
- 若要讓您的事件資料存放區從 AWS Organizations 組織中的所有帳戶收集事件，請選擇 [針對組織中的所有帳戶啟用]。僅當您使用組織的管理帳戶登入，且事件資料存放區的事件類型為事件或設定項目時，才CloudTrail能使用此選項。

完成後，請選擇儲存變更。

5. 在 Lake 查詢聯合中，選擇編輯以啟用或停用 Lake 查詢聯合。啟用 Lake 查詢聯合可讓您在資料目錄中檢視事件資料存放區的中繼 AWS Glue 資料，並使用 Amazon Athena 對事件資料執行 SQL 查詢。停用湖泊查詢聯合會停用與 AWS Glue AWS Lake Formation、和 Amazon Athena 的整合。停用 Lake 查詢聯合後，您將無法再於 Athena 中查詢資料。當您停用聯合時，不會刪除任何 CloudTrail Lake 資料，而且您可以繼續在 CloudTrail Lake 中執行查詢。

   若要啟用聯合，請執行下列動作：

   a. 選擇 啟用 。

   b. 選擇是要建立新的 IAM 角色，還是使用現有角色。當您建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您使用現有角色，請確認該角色的政策可提供所需的最低許可。

   c. 如果您要建立新的 IAM 角色，請輸入角色的名稱。

   d. 如果您要選擇現有的 IAM 角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

   完成時，請選擇儲存變更。

6. 編輯事件類型的任何其他設定。

事件類型	可編輯設定
CloudTrail 事件	您可以編輯 CloudTrail事件的下列設定： • 若要變更事件資料存放區記錄檔的事件，請選擇 「在CloudTrail 事件中編輯」。

事件類型	可編輯設定
	• 在管理事件中，選擇編輯以變更管理事件的設定。如需詳細資訊，請參閱記錄管理事件 AWS Management Console (步驟 3)。 • 在資料事件中，選擇編輯以變更資料事件的設定。您可以選擇要記錄的資料事件類型，然後選擇要使用的日誌選取器範本。如需詳細資訊，請參閱 更新現有事件資料存放區以記錄 AWS Management Console。 完成後，請選擇儲存變更。
來自整合的事件	在整合中，選擇您的整合。然後，選擇編輯以變更下列設定： • 在整合詳細資訊中，變更可識別整合通道的名稱。 • 在事件交付位置中，選擇事件的目的地。 • 在 Resource policy (資源政策) 中，為整合的通道設定資源政策。 完成後，請選擇儲存變更。 如需這些設定的詳細資訊，請參閱 建立與事件來源以外的整合 AWS。

7. 若要新增、變更或移除標籤，請在標籤中選擇編輯。您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制事件資料存放區的存取權限。完成後，請選擇儲存變更。

使用主控台停止和開始事件擷取

依預設，事件資料存放區設定為擷取事件。您可以使用主控台、 AWS CLI或 API 停止事件資料存放區擷取事件。

只有包含事件 (管理和資料事件) 或 AWS Config 設定項目的事件資料存放區才能使用「 CloudTrail 開始擷取」和「停止擷取」選項。

當您停止事件資料存放區的擷取時，該事件資料存放區的狀態變更為 STOPPED_INGESTION。您仍然可以對已在事件資料存放區內的任何事件執行查詢。您也可以將追蹤事件複製到事件資料存放區 (如果僅包含 CloudTrail 管理或資料事件)。

若要使事件資料存放區停止擷取事件

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 在動作中，選擇停止擷取。
5. 出現確認提示時，選擇停止擷取。事件資料存放區將停止擷取即時事件。
6. 若要繼續擷取，選擇開始擷取。

重新開始事件擷取

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 在動作中，選擇開始擷取。

使用主控台變更終止保護

根據預設， AWS CloudTrail Lake 中的事件資料存放區設定為啟用終止保護。終止保護可防止意外刪除事件資料存放區。如果您要刪除事件資料存放區，必須停用終止保護。您可以使用 AWS Management Console、 AWS CLI或 API 作業停用終止保護。

關閉終止保護

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 在動作中，選擇變更終止保護。

5. 選擇停用。
6. 選擇儲存。您現在可以刪除事件資料存放區。

開啟終止保護

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 在動作中，選擇變更終止保護。
5. 若要開啟終止保護，請選擇啟用。
6. 選擇儲存。

使用主控台刪除事件資料存放區

本節說明如何使用 AWS CloudTrail 主控台刪除事件資料存放區。若要取得有關如何使用刪除事件資料倉庫的資訊 AWS CLI，請參閱刪除事件資料倉庫 AWS CLI。

> **Note**
>
> 如果已啟用終止保護或 Lake 查詢聯合，則無法刪除事件資料存放區。依預設， CloudTrail 啟用終止保護，以防止意外刪除事件資料倉庫。
> 若要刪除事件類型為來自整合的事件的事件資料存放區，您必須先刪除整合的通道。您可以從整合的詳細資訊頁面或使用 aws cloudtrail delete-channel 命令刪除通道。如需更多資訊，請參閱刪除頻道以刪除與 AWS CLI

刪除事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 對於 Actions (動作)，選擇 Delete (刪除)。
5. 輸入事件資料存放區的名稱，以確認您要將其刪除。

6. 選擇刪除。

刪除事件資料存放區後，該事件資料存放區的狀態會變更為 PENDING_DELETION，並維持在該狀態 7 天。您可以在 7 天等待期內還原事件資料存放區。事件資料存放區處於 PENDING_DELETION 狀態時無法用於查詢，而且除了還原操作外，您不能對事件資料存放區執行其他任何操作。待刪除的事件資料存放區不會擷取事件，也不會產生費用。擱置刪除的事件資料存放區會計入可存在於一個事件資料存放區的配額中 AWS 區域。

使用主控台還原事件資料存放區

刪除 AWS CloudTrail Lake 中的事件資料倉庫後，其狀態會變更為，PENDING_DELETION並保持該狀態 7 天。在此期間，您可以使用、或 RestoreEventDataStoreAPI 作業還原事件資料存放區。 AWS Management Console AWS CLI

本節說明如何使用主控台還原事件資料存放區。若要取得有關如何使用還原事件資料倉庫的資訊 AWS CLI，請參閱還原事件資料倉庫 AWS CLI。

還原事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 在動作中，選擇還原。

建立、更新和管理事件資料存放區 AWS CLI

您可以使用建 AWS CLI 立、更新和管理您的事件資料存放區。使用時 AWS CLI，請記住您的命令會在為您的設定檔所 AWS 區域 設定的中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

事件資料倉庫的可用指令

在 CloudTrail Lake 中建立和更新事件資料倉庫的指令包括：

- `create-event-data-store`以建立事件資料倉庫。
- `get-event-data-store`以傳回事件資料存放區的相關資訊，包括為事件資料存放區設定的進階事件選取器。

- update-event-data-store以變更現有事件資料倉庫的組態。
- list-event-data-stores以列出事件資料儲存區。
- delete-event-data-store以刪除事件資料倉庫。
- restore-event-data-store，以還原待刪除的事件資料存放區。
- start-import以開始將追蹤事件匯入至事件資料倉庫，或重試失敗的匯入。
- get-import以傳回有關特定匯入的資訊。
- stop-import，以停止將追蹤事件匯入至事件資料倉庫。
- list-imports以傳回有關所有匯入的資訊，或按ImportStatus或傳回選取的匯入集Destination。
- list-import-failures以列出指定匯入的匯入失敗。
- stop-event-data-store-ingestion以停止事件資料存放區的事件擷取。
- start-event-data-store-ingestion以重新啟動事件資料存放區上的事件擷取。
- enable-federation，在事件資料存放區上啟用聯合，以查詢 Amazon Athena 中的事件資料存放區。
- disable-federation以停用事件資料存放區上的聯合。停用聯合後，您將無法再查詢 Amazon Athena 中的事件資料存放區的資料。您可以繼續在 CloudTrail 湖中查詢。
- put-insight-selectors新增或修改現有事件資料存放區的 Insights 事件選取器，以及啟用或停用 Insights 事件。
- get-insight-selectors，以傳回針對事件資料存放區設定的 Insights 事件選取器的相關資訊。
- add-tags將一個或多個標籤（鍵值對）添加到現有的事件數據存儲中。
- remove-tags，從事件資料倉庫中移除一個或多個標籤。
- list-tags以傳回與事件資料存放區相關聯的標籤清單。

如需 CloudTrail Lake 查詢的可用指令清單，請參閱〈 CloudTrail 湖泊查詢的可用指令。

如需 CloudTrail Lake 整合的可用命令清單，請參閱 CloudTrail 湖泊整合的可用命令。

建立事件資料倉庫 AWS CLI

使用 create-event-data-store 命令建立事件資料存放區。

建立事件資料存放區時，唯一需要使用的參數為 --name，此參數可用來識別事件資料存放區。您可以配置其他選用參數，包括：

- `--advanced-event-selectors` – 指定要包含在事件資料存放區中的事件類型。依預設，事件資料存放區會記錄所有管理事件。如需進階事件選取器的詳細資訊，請參閱 CloudTrail API 參考AdvancedEventSelector中的。
- `--kms-key-id`-指定用來加密交付事件的 AWS KMS 金鑰 ID CloudTrail。值可以是加上 `alias/` 字首的別名名稱、指向別名的完整指定 ARN、指向金鑰的完整指定 ARN，或是全域唯一識別碼。
- `--multi-region-enabled`-建立多區域事件資料存放區，以記錄帳戶 AWS 區域 中所有人的事件。依預設，即使未新增參數，系統也會設定 `--multi-region-enabled`。
- `--organization-enabled` – 啟用事件資料存放區來收集組織中所有帳戶的事件。依預設，未針對組織中的所有帳戶啟用事件資料存放區。
- `--billing-mode` – 決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。

  以下為可能值：

  - `EXTENDABLE_RETENTION_PRICING` – 如果您每月擷取的事件資料少於 25 TB，並且需要長達 3,653 天 (約 10 年) 的彈性保留期，通常建議使用此計費模式。此計費模式的預設保留期為 366 天。
  - `FIXED_RETENTION_PRICING` – 如果您預期每月擷取的事件資料超過 25 TB，並且需要長達 2,557 天 (約 7 年) 的彈性保留期，則建議使用此計費模式。此計費模式的預設保留期為 2,557 天。

  預設值為 `EXTENDABLE_RETENTION_PRICING`。
- `--retention-period` – 將事件保留在事件資料存放區中的天數。如果 `--billing-mode` 為 `EXTENDABLE_RETENTION_PRICING`，則有效值為介於 7 到 3,653 之間的整數；如果 `--billing-mode` 設定為 `FIXED_RETENTION_PRICING`，則為介於 7 到 2,557 之間的整數。如果未指定`--retention-period`，請 CloudTrail 使用的預設保留期間`--billing-mode`。
- `--start-ingestion` – `--start-ingestion` 參數會在建立時開始事件資料存放區的事件擷取。即使未新增參數，系統也會設定此參數。

  如果您不希望事件資料存放區擷取即時事件，請指定 `--no-start-ingestion`。舉例來說，如果您要將事件複製到事件資料存放區，並且只打算使用事件資料來分析過往事件，您可能需要設定此參數。只有在 `eventCategory` 為 `Management`、`Data` 或 `ConfigurationItem` 時，`--no-start-ingestion` 參數才有效。

下列範例展示如何建立不同類型的事件資料存放區。

主題

- 建立 S3 資料事件的事件資料存放區， AWS CLI

- 建立組 AWS Config 態項目的事件資料存放區， AWS CLI
- 建立管理事件的組織事件資料存放區 AWS CLI
- 使用 AWS CLI

建立 S3 資料事件的事件資料存放區， AWS CLI

下列範例 AWS Command Line Interface (AWS CLI) create-event-data-store 命令會建立名為的事件資料存放區，`my-event-data-store`該存放區選取所有 Amazon S3 資料事件並使用 KMS 金鑰加密。

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
    ]'
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
```

```
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

建立組 AWS Config 態項目的事件資料存放區， AWS CLI

下列範例 AWS CLI create-event-data-store命令會建立名為的事件資料倉庫config-items-eds，該存放區可選取 AWS Config 組態項目。若要收集組態項目，請在進階事件選取器中指定 eventCategory 欄位等於 ConfigurationItem。

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

建立管理事件的組織事件資料存放區 AWS CLI

下列範例 AWS CLI create-event-data-store命令會建立收集所有管理事件並將--billing-mode參數設定為的組織事件資料存放區FIXED_RETENTION_PRICING。

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
```

```
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

使用 AWS CLI

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要收集 Insights 事件的目標事件資料存放區，以及啟用見解和記錄管理事件的來源事件資料存放區。

此程序將向您說明如何建立目的地和來源事件資料存放區，然後啟用 Insights 事件。

1. 執行 aws cloudtrail create-event-data-store 命令來建立會收集 Insights 事件的目的地事件資料存放區。eventCategory 的值必須為 Insight。取代*retention-period-days*為您希望在事件資料存放區中保留事件的天數。如果 --billing-mode 為 EXTENDABLE_RETENTION_PRICING，則有效值為介於 7 到 3,653 之間的整數；如果 --billing-mode 設定為 FIXED_RETENTION_PRICING，則為介於 7 到 2,557 之間的整數。如果未指定--retention-period，請 CloudTrail 使用的預設保留期間--billing-mode。

   如果您使用 AWS Organizations 組織的管理帳戶登入，如果您想要授予委派管理員對事件資料存放區的存取權，請包含--organization-enabled參數。

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   ```

```
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

以下是回應範例。

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

您將使用來自回應的 ARN (或 ARN 的 ID 尾碼)，作為步驟 3 中 `--insights-destination` 參數的值。

2. 執行 aws cloudtrail create-event-data-store 命令以建立記錄管理事件的來源事件資料存放區。依預設，事件資料存放區會記錄所有管理事件。如果想要記錄所有管理事件，您不需要指定進階事件選取器。取代*retention-period-days*為您希望在事件資料存放區中保留事件的天數。如果 --billing-mode 為 EXTENDABLE_RETENTION_PRICING，則有效值為介於 7 到 3,653 之間的整數；如果 --billing-mode 設定為 FIXED_RETENTION_PRICING，則為介於 7 到 2,557 之間的整數。如果未指定--retention-period，請 CloudTrail 使用的預設保留期間--billing-mode。若您要建立組織事件資料存放區，請加入 --organization-enabled 參數。

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

您將使用來自回應的 ARN (或 ARN 的 ID 尾碼)，作為步驟 3 中 `--event-data-store` 參數的值。

3. 執行 put-insight-selectors 命令以啟用 Insights 事件。Insights 選取器值可以是 `ApiCallRateInsight` 或 `ApiErrorRateInsight` (或兩者)。對於 `--event-data-store` 參數，指定來源事件資料存放區的 ARN (或 ARN 的 ID 尾碼)，該存放區會記錄管理事件並且將啟用 Insights。對於 `--insights-destination` 參數，指定目的地事件資料存放區的 ARN (或 ARN 的 ID 尾碼)，該存放區將會記錄 Insights 事件。

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

下列結果顯示針對事件資料存放區設定的 Insights 事件選取器。

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

在事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能傳遞第一個 Insights 事件。

CloudTrail Insights 會分析單一區域 (而非全球) 中發生的管理事件。In CloudTrail sights 事件會在與產生其支援管理事件的相同區域中產生。

對於組織事件資料存放區，分 CloudTrail 析來自每個成員帳戶的管理事件，而不是分析組織所有管理事件的彙總。

在 CloudTrail 湖泊擷取見解事件需要支付額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需 CloudTrail 定價的相關資訊，請參閱AWS CloudTrail 定價。

將追蹤事件匯入至事件資料倉庫 AWS CLI

在中 AWS CLI，您可以將軌跡事件匯入事件資料倉庫。本節中的程序示範如何執行 create-event-data-store 命令來建立和設定事件資料存放區，然後使用 start-import 命令將事件匯入至該事件資料存放區。如需有關匯入追蹤事件的詳細資訊 (包括考量事項和所需許可的相關資訊)，請參閱將追蹤事件複製到事件資料存放區。

準備匯入追蹤事件

匯入追蹤事件之前，請進行以下準備工作。

- 確認您的角色具有所需的許可，能夠將追蹤事件匯入至事件資料存放區。
- 決定您要為事件資料存放區指定的 --billing-mode 值。`--billing-mode` 將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。

  當您將追蹤事件匯入 CloudTrail Lake 時，會 CloudTrail 解壓縮以 gzip (壓縮) 格式儲存的記錄檔。然後 CloudTrail 將記錄檔中包含的事件複製到您的事件資料存放區。未壓縮資料的大小可能大於實際的 Amazon S3 儲存大小。若要取得未壓縮資料大小的一般估計值，請將 S3 儲存貯體中的日誌大小乘以 10。您可以使用此預估來選擇適合您使用案例的 `--billing-mode` 值。
- 決定您要為 `--retention-period` 指定的值。 CloudTrail 如果事件早於指定的`eventTime`保留期間，則不會複製該事件。

  若要確定適當的保留期，請計算您要複製的最舊事件所經歷的天數，以及要將事件保留在事件資料存放區中的天數，並將兩者加總，如以下等式所示：

  保留期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*

  例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。
- 決定是否要使用事件資料存放區來分析任何未來事件。如果您不想擷取任何未來事件，請在建立事件資料存放區時包含 `--no-start-ingestion` 參數。依預設，事件資料存放區會在建立時開始擷取事件。

建立事件資料存放區並將追蹤事件匯入至該事件資料存放區

1. 執行 create-event-data-store 命令來建立新的事件資料存放區。在此範例中，--retention-period 設定為 120，因為要複製的最舊事件已超過 90 天，而且我們想要將事件保留 30 天。我們不想擷取任何未來事件，因此設定了 --no-start-ingestion 參數。在此範例中，我們使用的是預設值 EXTENDABLE_RETENTION_PRICING，因此並未設定 --billing-mode，這是因為我們預期擷取的事件資料少於 25 TB。

   > **Note**
   >
   > 如果您要建立事件資料存放區來取代追蹤，建議您設定 --advanced-event-selectors 以符合追蹤的事件選取器，進而確保您擁有相同的事件涵蓋範圍。依預設，事件資料存放區會記錄所有管理事件。

```
aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
 120 --no-start-ingestion
```

以下是回應範例：

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
```

```
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

初始 Status 為 CREATED，因此我們會執行 get-event-data-store 命令來驗證擷取是否已停止。

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

回應會顯示 Status 現在為 STOPPED_INGESTION，這表示事件資料存放區未擷取事件。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. 執行 start-import 命令，將追蹤事件匯入至步驟 1 中建立的事件資料存放區。指定事件資料存放區的 ARN (或 ARN 的 ID 尾碼) 作為參數 --destinations 的值。針對 --start-event-time，

指定要複製之最舊事件的 eventTime，並針對 --end-event-time，指定要複製之最新事件的 eventTime。用於--import-source指定包含追蹤日誌的 S3 儲存貯體的 S3 URI、S3 儲存貯體，以及用於匯入追蹤事件之角色的 ARN。 AWS 區域

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

以下是回應範例。

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
   "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
   "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. 執行 get-import 命令，以取得與該匯入相關的資訊。

```
aws cloudtrail get-import --import-id import-id
```

以下是回應範例。

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

如果未發生失敗，則匯入完成時會顯示 `ImportStatus` 為 `COMPLETED`；如果發生失敗，則會顯示 `FAILED`。

如果該匯入具有 `FailedEntries`，您可以執行 list-import-failures 命令來傳回失敗清單。

```
aws cloudtrail list-import-failures --import-id import-id
```

若要重試失敗的匯入，請僅使用 `--import-id` 參數執行 start-import 命令。當您重試匯入時，會在發生失敗的位置 CloudTrail 繼續匯入。

```
aws cloudtrail start-import --import-id import-id
```

取得事件資料存放區 AWS CLI

下列範例 AWS CLI get-event-data-store命令會傳回必要--event-data-store參數所指定之事件資料存放區的相關資訊，該資料存放區接受 ARN 或 ARN 的 ID 尾碼。

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下是回應範例。建立時間和上次更新時間的格式為 timestamp。

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::bucketName"
                    ]
                },
```

```
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

列出帳戶中的所有事件資料存放區 AWS CLI

下列範例 AWS CLI list-event-data-stores命令會傳回目前 Region 中帳戶中所有事件資料存放區的相關資訊。選用參數包括--max-results，藉以指定想要命令在單一頁面上傳回的最大結果數。如果結果多於您指定的 --max-results 值，請再次執行命令，新增傳回的 NextToken 值以取得下一頁的結果。

```
aws cloudtrail list-event-data-stores
```

以下是回應範例。

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
```

```
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
}
```

使用更新事件資料倉庫 AWS CLI

下列範例展示如何更新事件資料存放區。

主題

- 使用更新計費模式 AWS CLI
- 更新保留模式、啟用終止保護，並使 AWS KMS key 用 AWS CLI
- 停用終止保護 AWS CLI

使用更新計費模式 AWS CLI

事件資料存放區的 `--billing-mode` 將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如果將事件資料存放區的 `--billing-mode` 設為 `FIXED_RETENTION_PRICING`，您可以將值變更為 `EXTENDABLE_RETENTION_PRICING`。如果您的事件資料存放區每月擷取的事件資料少於 25 TB，而且您需要長達 3,653 天的彈性保留期，通常建議使用 `EXTENDABLE_RETENTION_PRICING`。如需定價的詳細資訊，請參閱 AWS CloudTrail 定價和管理 CloudTrail 湖泊成本。

> **Note**
>
> 您無法將 `--billing-mode` 值從 `EXTENDABLE_RETENTION_PRICING` 變更為 `FIXED_RETENTION_PRICING`。如果事件資料存放區的計費模式設定為 `EXTENDABLE_RETENTION_PRICING`，而您想改為使用 `FIXED_RETENTION_PRICING`，您可以在事件資料存放區上停止擷取，並建立使用 `FIXED_RETENTION_PRICING` 的新事件資料存放區。

下列範例 AWS CLI update-event-data-store指令會將事件--billing-mode資料倉庫的從變更FIXED_RETENTION_PRICING為EXTENDABLE_RETENTION_PRICING。必要的 --event-data-store 參數值是 ARN (或 ARN 的 ID 尾碼) 而且為必填；其他參數為選填。

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

以下是回應範例。

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

更新保留模式、啟用終止保護，並使 AWS KMS key 用 AWS CLI

下列範例 AWS CLI update-event-data-store命令會更新事件資料存放區，將其保留期限變更為 100 天，並啟用終止保護。必要的 `--event-data-store` 參數值是 ARN (或 ARN 的 ID 尾碼) 而且為必填；其他參數為選填。在此範例中新增了 `--retention-period` 參數，以將保留期間變更為 100 天。或者，您可以選擇啟用 AWS Key Management Service 加密，並 AWS KMS key 透過新增`--kms-key-id`至命令並指定 KMS 金鑰 ARN 作為值來指定。 `--termination-protection-enabled`已新增以在未啟用終止保護的事件資料存放區上啟用終止保護。

從外部記錄事件的事件資料存放區 AWS 無法更新為記錄 AWS 事件。同樣地，記錄 AWS 事件的事件資料存放區無法更新為從外部記錄事件 AWS。

> **Note**
>
> 如果您縮短事件資料存放區的保留期間， CloudTrail 將會移除任何`eventTime`早於新保留期的事件。例如，如果先前的保留期為 365 天，而您將其減少到 100 天，則 CloudTrail 會移除`eventTime`超過 100 天的事件。

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

停用終止保護 AWS CLI

依預設，系統會在事件資料存放區上啟用終止保護，以防止意外刪除事件資料存放區。啟用終止保護時，您無法刪除事件資料存放區。如果您要刪除事件資料存放區，必須先停用終止保護。

下列範例 AWS CLI update-event-data-store命令會藉由傳遞`--no-termination-protection-enabled`參數來停用終止保護。

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

停止擷取事件資料存放區，使用 AWS CLI

下列範例 AWS CLI stop-event-data-store-ingestion命令可停止事件資料存放區擷取事件。若要停止擷取，事件資料存放區 `Status` 必須為 `ENABLED`，且 `eventCategory` 必須是 `Management`、`Data` 或 `ConfigurationItem`。由 `--event-data-store` 指定的事件資料存放區，它接受事件資料存放區 ARN 或 ARN 的 ID 尾碼。執行 stop-event-data-store-ingestion 後，事件資料存放區的狀態變更為 `STOPPED_INGESTION`。

事件資料存放區處於 `STOPPED_INGESTION` 狀態時，最多十個事件資料存放區會計入您的帳戶。

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

如果操作成功，則不會有回應。

在事件資料存放區上開始擷取 AWS CLI

下列範例 AWS CLI start-event-data-store-ingestion命令會在事件資料存放區上啟動事件擷取。若要開始擷取，事件資料存放區 `Status` 必須為 `STOPPED_INGESTION`，且 `eventCategory` 必須是 `Management`、`Data` 或 `ConfigurationItem`。由 `--event-data-store` 指定的事件資料存放區，它接受事件資料存放區 ARN 或 ARN 的 ID 尾碼。執行 start-event-data-store-ingestion 後，事件資料存放區的狀態變更為 `ENABLED`。

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

如果操作成功，則不會有回應。

在事件資料存放區上啟用聯合

若要啟用聯合，請執行 aws cloudtrail enable-federation 命令，並提供必要的 `--event-data-store` 和 `--role` 參數。針對 `--event-data-store`，提供事件資料存放區 ARN (或 ARN 的 ID 尾碼)。針對 `--role`，提供您的聯合角色 ARN。該角色必須存在於您的帳戶中，並提供所需的最低許可。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

此範例展示委派管理員如何在管理帳戶中指定事件資料存放區的 ARN，以及在委派管理員帳戶中指定聯合角色的 ARN，進而在組織事件資料存放區上啟用聯合。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-
id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

在事件資料存放區上停用聯合

若要在事件資料存放區上停用聯合，請執行 aws cloudtrail disable-federation 命令。由 `--event-data-store` 指定的事件資料存放區，它接受事件資料存放區 ARN 或 ARN 的 ID 尾碼。

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> 如果這是組織事件資料存放區，請使用管理帳戶的帳戶 ID。

刪除事件資料倉庫 AWS CLI

下列範例 AWS CLI delete-event-data-store 命令停用由 `--event-data-store` 指定的事件資料存放區，它接受事件資料存放區 ARN 或 ARN 的 ID 尾碼。執行 delete-event-data-store 後，事件資料存放區的最終狀態為 `PENDING_DELETION`，而且事件資料存放區將在 7 天的等待期後自動刪除。

在事件資料存放區上執行 delete-event-data-store 後，無法對於使用已停用的資料存放區進行的查詢執行 list-queries、describe-query 或 get-query-results。事件資料存放區處於待刪除狀態時，最多十個事件資料存放區會計入您的帳戶。

> **Note**
>
> 如果已設定 `--termination-protection-enabled` 或其 `FederationStatus` 為 `ENABLED`，則無法刪除事件資料存放區。

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

如果操作成功，則不會有回應。

還原事件資料倉庫 AWS CLI

下列範例 AWS CLI restore-event-data-store 命令會還原待刪除的事件資料存放區。由 `--event-data-store` 指定的事件資料存放區，它接受事件資料存放區 ARN 或 ARN 的 ID 尾碼。您只能在刪除後的七天等待期間內還原已刪除的事件資料存放區。

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

回應包括有關事件資料存放區的資訊，包括其 ARN、進階事件選取器和還原狀態。

管理事件資料存放區生命週期

以下是事件資料存放區的生命週期階段。

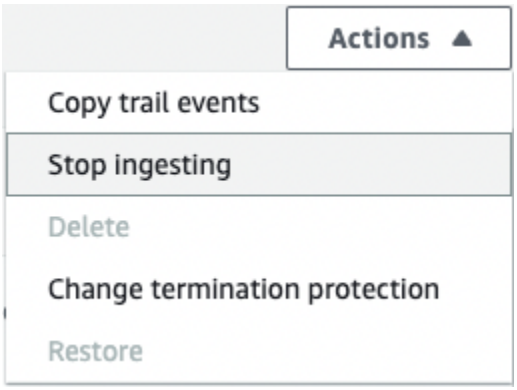
- CREATED – 指示已建立事件資料存放區的短期狀態。
- ENABLED – 事件資料存放區在作用中並擷取事件。您可以執行查詢並將追蹤事件複製到事件資料存放區。
- STARTING_INGESTION – 短期狀態指示事件資料存放區將開始擷取即時事件。
- STOPPING_INGESTION – 短期狀態指示事件資料存放區將停止擷取即時事件。
- STOPPED_INGESTION – 事件資料存放區不在擷取事件。您仍然可以對已在事件資料存放區內的任何事件執行查詢，並將追蹤事件複製到事件資料存放區。
- PENDING_DELETION – 事件資料存放區處於 ENABLED 或 STOPPED_INGESTION 狀態並且已遭刪除，但在永久刪除之前，該存放區仍在 7 天等待期內。您不能在事件資料存放區上執行查詢，除了還原之外，不能對事件資料存放區執行任何操作。

只有在聯合和終止保護都停用時，您才能刪除事件資料存放區。終止保護可防止意外刪除事件資料存放區。根據預設，事件資料存放區的終止保護功能為啟用。聯合可讓您在 Athena 中查詢事件資料存放區資料，而且其預設為停用。

刪除事件資料存放區後，該存放區會維持 PENDING_DELETION 狀態長達 7 天，然後才會永久刪除。您可以在 7 天等待期內還原事件資料存放區。事件資料存放區處於 PENDING_DELETION 狀態時無法用於查詢，除了還原操作外，不能對事件資料存放區執行其他任何操作。待刪除的事件資料存放區不會擷取事件，也不會產生費用。但是，擱置刪除的事件資料存放區會計入可存在於一個事件資料存放區的配額中 AWS 區域。

事件資料存放區上的可用動作

若要刪除或還原事件資料存放區、複製追蹤事件、開始或停止擷取事件，或者開啟或關閉事件資料存放區的終止保護，請在事件資料存放區的詳細資訊頁面中，使用動作功能表上的命令。



複製追蹤事件的選項僅適用於包含 CloudTrail 管理和資料事件的事件資料存放區。只有包含事件 (管理和資料事件) 或 AWS Config 設定項目的事件資料存放區才能使用「 CloudTrail 開始擷取」和「停止擷取」選項。

將追蹤事件複製到事件資料存放區

您可以將追蹤事件複製到 CloudTrail Lake 事件資料存放區，以建立記錄至追蹤的事件 point-in-time 快照。複製追蹤的事件不會干擾追蹤記錄事件的功能，也不會以任何方式修改追蹤。

您可以將追蹤事件複製到針 CloudTrail 對事件設定的現有事件資料存放區，也可以建立新的 CloudTrail 事件資料存放區並選擇「複製追蹤事件」選項作為事件資料存放區建立的一部分。如需有關將追蹤事件複製到現有事件資料存放區的詳細資訊，請參閱 將追蹤事件複製到現有的事件資料存放區。如需有關建立新的事件資料存放區的詳細資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區。

如果您要將追蹤事件複製到組織事件資料存放區，您必須使用組織的管理帳戶。您無法使用組織的委派管理員帳戶複製追蹤事件。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

將追蹤事件複製到 CloudTrail Lake 事件資料存放區時，會根據事件資料存放區擷取的未壓縮資料量產生費用。

當您將追蹤事件複製到 CloudTrail Lake 時，會 CloudTrail 解壓縮以 gzip (壓縮) 格式儲存的記錄檔，然後將記錄中包含的事件複製到您的事件資料存放區。未壓縮資料的大小可能大於實際的 S3 儲存大小。若要取得未壓縮資料大小的一般估計值，您可以將 S3 儲存貯體中的日誌大小乘以 10。

您可以縮小指定的複製事件的時間範圍，來降低該費用。如果您計劃只使用事件資料存放區來查詢複製的事件，可以關閉事件擷取以避免因未來事件而產生費用。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

案例

下表描述一些複製追蹤事件的常見案例，以及您可以如何使用主控台應對每個案例。

案例	我可以如何在主控台中加以應對？
分析和查詢 CloudTrail 湖泊中的歷史跟踪事件，而無需攝入新事件	建立一個新的事件資料存放區，並且在建立事件資料存放區的過程中選擇複製追蹤事件選項。在建立事件資料存放區時，取消選取擷取事件 (程序中的步驟 15)，以確保事件資料存放區僅包含追蹤的歷史事件而不包含未來事件。
使用 CloudTrail Lake 事件資料存放區取代您現有的追蹤	使用與建立追蹤時所使用的相同事件選取器來建立事件資料存放區，以確保事件資料存放區與您的追蹤有相同的覆蓋範圍。 若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請為複製的事件選擇早於事件資料存放區建立日期的日期範圍。 在建立您的事件資料存放區後，您可以關閉追蹤記錄，以避免產生額外費用。

主題

複製追蹤事件的考量

複製追蹤事件時，請考慮下列因素。

- 複製追蹤事件時， CloudTrail 會使用 S3 `GetObject`API 操作擷取來源 S3 儲存貯體中的追蹤事件。一些 S3 已封存儲存類別無法透過使用 `GetObject` 存取，例如 S3 Glacier Flexible Retrieval、S3

Glacier Deep Archive、S3 Outposts 和 S3 Intelligent-Tiering Deep Archive 層。若要複製儲存在這些已封存儲存類別中的追蹤事件，您必須先使用 S3 `RestoreObject` 操作還原一個複本。如需有關還原已封存物件的詳細資訊，請參閱《Amazon S3 使用者指南》中的還原已封存的物件。

- 將追蹤事件複製到事件資料存放區時， CloudTrail 不論目的地事件資料存放區的事件類型、進階事件選取器或 AWS 區域的組態為何，都會複製所有追蹤事件。
- 將追蹤事件複製到現有的事件資料存放區前，請務必先為您的使用案例妥善設定事件資料存放區的定價選項和保留期。
  - 定價選項：定價選項決定擷取和儲存事件的成本。如需更多關於定價選項的資訊，請參閱 AWS CloudTrail 定價和 事件資料存放區定價選項。
  - 保留期：保留期決定事件資料在事件資料存放區中保留的時間長度。 CloudTrail 僅複製在事件資料存放區保留期`eventTime`內的追蹤事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*)。例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。
- 如果您要複製追蹤事件到事件資料存放區以用於調查，而且不想擷取任何未來事件，您可以停止在事件資料存放區上的擷取。在建立事件資料存放區時，取消選取擷取事件選項 (程序中的步驟 15)，以確保事件資料存放區僅包含追蹤的歷史事件而不包含未來事件。
- 複製追蹤事件之前，請停用連接到來源 S3 儲存貯體的任何存取控制清單 (ACL)，並更新目的地事件資料存放區的 S3 儲存貯體政策。如需更新 S3 儲存貯體政策的詳細資訊，請參閱 複製追蹤事件的 Amazon S3 儲存貯體政策。如需有關停用 ACL 的詳細資訊，請參閱《Amazon S3 使用者指南》中的控制物件的所有權並停用儲存貯體的 ACL。
- CloudTrail 只會從來源 S3 儲存貯體中的 Gzip 壓縮日誌檔複製追蹤事件。 CloudTrail 不會從使用 Gzip 以外的格式壓縮的未壓縮記錄檔或記錄檔複製追蹤事件。
- 若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請為複製的事件選擇早於事件資料存放區建立日期的時間範圍。
- 根據預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前綴。如果您要複製其他前置詞中包含的 CloudTrail 事件，則必須在複製追蹤事件時選擇前置詞。
- 若要將追蹤事件複製到組織事件資料存放區，您必須使用組織的管理帳戶。委派的管理員帳戶無法將追蹤事件複製到組織事件資料存放區。

複製追蹤事件所需的許可

複製追蹤事件之前，請確定您擁有 IAM 角色的所有必要許可。如果您選擇現有的 IAM 角色來複製追蹤事件，則只需更新 IAM 角色許可。如果您選擇建立新的 IAM 角色，請 CloudTrail 提供該角色的所有必要許可。

如果來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策允許 CloudTrail 解密儲存貯體中的資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，您必須更新每個金鑰的政策，以允許 CloudTrail 解密儲存貯體中的資料。

主題

複製追蹤事件的 IAM 許可

複製追蹤事件時，您可以選擇建立新的 IAM 角色，也可以使用現有的 IAM 角色。當您選擇新的 IAM 角色時，請 CloudTrail 建立具有所需許可的 IAM 角色，您不需要進一步採取任何動作。

如果您選擇現有角色，請確保 IAM 角色的政策允許 CloudTrail 從來源 S3 儲存貯體複製追蹤事件。此區段提供所需 IAM 角色許可和信任政策的範例。

下列範例提供許可政策，允許 CloudTrail 從來源 S3 儲存貯體複製追蹤事件。使用適合您組態的值取代*myBucketName*、*MyAccountI eventDataStored*、*##*、*###*和 ID。*MyAccountId* 是用於 CloudTrail 湖泊的 AWS 帳戶識別碼，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

使用用於加密來源 S3 儲存貯體的 KMS 金鑰的值來取代 *key-region*、*keyAccountID* 和 *keyID*。如果來源 S3 儲存貯體不使用 KMS 金鑰進行加密，則您可以省略 `AWSCloudTrailImportKeyAccess` 陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
```

```
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

下列範例提供 IAM 信任政策，該政策 CloudTrail 允許假設 IAM 角色從來源 S3 儲存貯體複製追蹤事件。以適用於您的組態的適當值取代 *MyAccountId*、*##*和 *eventDataStoreArn*。*MyAccountId* 是用於 CloudTrail 湖泊的 AWS 帳戶 識別碼，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

複製追蹤事件的 Amazon S3 儲存貯體政策

根據預設，所有 Amazon S3 儲存貯體和物件皆為私有。只有資源擁有者 (建立儲存貯體的 AWS 帳戶)，可存取儲存貯體及其包含的物件。資源擁有者可藉由編寫存取政策，將存取許可授予其他資源和使用者。

在複製追蹤事件之前，您必須更新 S3 儲存貯體政策，以允許 CloudTrail 從來源 S3 儲存貯體複製追蹤事件。

您可以將下列陳述式新增至 S3 儲存貯體政策，以授予這些權限。取*# roleArn* 並*myBucketName*使用適合您組態的適當值。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
```

```
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策

如果來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策提 CloudTrail 供從已啟用 SSE-KMS 加密的 S3 儲存貯體複製追蹤事件所需的`kms:GenerateDataKey`權限。`kms:Decrypt`如果您的來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策。更新 KMS 金鑰政策允許解密 CloudTrail 來源 S3 儲存貯體中的資料、執行驗證檢查以確保事件符合 CloudTrail標準，以及將事件複製到 CloudTrail Lake 事件資料存放區。

下列範例提供 KMS 金鑰政策，可讓您解密 CloudTrail 來源 S3 儲存貯體中的資料。*# roleArn#myBucketName##### eventDataStore ID ##################MyAccountId* 是用於 CloudTrail 湖泊的 AWS 帳戶識別碼，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

將追蹤事件複製到現有的事件資料存放區

使用下列程序將追蹤事件複製到現有的事件資料存放區。如需有關如何建立新事件資料存放區的資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區。

> **Note**
>
> 將追蹤事件複製到現有的事件資料存放區前，請務必先為您的使用案例妥善設定事件資料存放區的定價選項和保留期。
>
> - 定價選項：定價選項決定擷取和儲存事件的成本。如需更多關於定價選項的資訊，請參閱 AWS CloudTrail 定價和 事件資料存放區定價選項。
> - 保留期：保留期決定事件資料在事件資料存放區中保留的時間長度。 CloudTrail 僅複製在事件資料存放區保留期`eventTime`內的追蹤事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*)。例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。

若要將追蹤事件複製到事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Copy trail events (複製追蹤事件)。
4. 在 Copy trail events (複製追蹤事件) 頁面上，對於 Event source (事件來源)，選擇您想要複製的追蹤。根據預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前綴。如果您要複製其他前置詞中包含的 CloudTrail 事件，請選擇 [輸入 S3 URI]，然後選擇 [瀏覽 S3] 以瀏覽至首碼。如果追蹤的來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策 CloudTrail 允許解密資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策， CloudTrail 以允許解密儲存貯體中的資料。如需更新 KMS 金鑰政策的詳細資訊，請參閱 用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策。

   S3 儲存貯體政策必須授予從 S3 儲 CloudTrail 存貯體複製追蹤事件的存取權。如需更新 S3 儲存貯體政策的詳細資訊，請參閱 複製追蹤事件的 Amazon S3 儲存貯體政策。

5. 對於指定事件的時間範圍，請選擇複製事件的時間範圍。 CloudTrail 在嘗試複製追蹤事件之前，先檢查字首和記錄檔名稱，以確認名稱包含在所選開始日期與結束日期之間的日期。您可以選擇 Relative range (相對範圍) 或 Absolute range (絕對範圍)。若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請選擇早於事件資料存放區建立日期的時間範圍。

   > **Note**
   >
   > CloudTrail 僅複製在事件資料存放區保留期`eventTime`內的追蹤事件。例如，如果事件資料存放區的保留期為 90 天，則不 CloudTrail 會複製任何`eventTime`超過 90 天的追蹤事件。

   - 如果您選擇「相對範圍」，則可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。 CloudTrail 複製所選期間內記錄的事件。
   - 如果選擇「絕對範圍」，則可以選擇特定的開始日期和結束日期。 CloudTrail 複製所選開始日期和結束日期之間發生的事件。
6. 對於 Delivery location (交付地點)，從下拉式清單中選擇目的地事件資料存放區。
7. 對於 Permissions (許可)，從下列 IAM 角色選項中選擇。如果您選擇現有的 IAM 角色，請確認 IAM 角色政策提供必要的許可。如需更新 IAM 角色許可的詳細資訊，請參閱複製追蹤事件的 IAM 許可。

   - 選擇 Create a new role (recommended) (建立新角色 (建議使用)) 以建立新的 IAM 角色。對於 Enter IAM role name (輸入 IAM 角色名稱)，請輸入角色的名稱。 CloudTrail 會自動為這個新角色建立必要的權限。
   - 選擇「使用自訂 IAM 角色 ARN」以使用未列出的自訂 IAM 角色。對於 Enter IAM role ARN (輸入 IAM 角色 ARN)，輸入 IAM ARN。
   - 從下拉式清單中選擇現有的 IAM 角色。
8. 選擇 Copy events (複製事件)。
9. 系統會提示您確認。當您就緒確認時，請選擇 Copy trail events to Lake (將追蹤事件複製到 Lake)，接著選擇 Copy events (複製事件)。
10. 在 Copy details (複製詳細資訊) 頁面中，您可檢視複製狀態並檢閱任何失敗。追蹤事件複製完成時，如果沒有錯誤，則其 Copy status (複製狀態) 設定為 Completed (完成)；如果發生錯誤，則設定為 Failed (失敗)。

> **Note**
>
> 事件複製詳細資訊頁面上顯示的詳細資訊不是即時的。實際的詳細資訊值 (例如 Prefixes copied (複製的字首)) 可能會高於頁面上顯示的值。 CloudTrail 在事件副本的過程中逐步更新詳細信息。

11. 如果 Copy status (複製狀態) 是 Failed (失敗)，修正 Copy failures (複製失敗) 中顯示的任何錯誤，接著選擇 Retry copy (重試複製)。當您重試副本時，會在發生失敗的位置 CloudTrail 繼續複製。

如需檢視追蹤事件複製之詳細資訊，請參閱 事件複製詳細資訊。

事件複製詳細資訊

追蹤事件複製開始之後，您可以檢視事件複製詳細資訊，包括複製的狀態，以及任何複製失敗的相關資訊。

> **Note**
>
> 事件複製詳細資訊頁面上顯示的詳細資訊不是即時的。實際的詳細資訊值 (例如 Prefixes copied (複製的字首)) 可能會高於頁面上顯示的值。CloudTrail 在事件副本的過程中逐步更新詳細信息。

存取事件複製詳細資訊頁面

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在左側導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區。
4. 在 Event copy status (事件複製狀態) 區段中選擇事件複製。

複製詳細資訊

從 Copy details (複製詳細資訊) 中，您可以檢視有關追蹤事件複製的下列詳細資訊。

- Event log S3 location (事件日誌 S3 位置) - 包含追蹤事件日誌檔案的來源 S3 儲存貯體位置。

- Copy ID (複製 ID) - 該複製的 ID。
- Prefixes copied (複製的字首) - 代表複製的 S3 字首數。在追蹤事件複製期間，會 CloudTrail 複製追蹤記錄檔中儲存在首碼中的事件。
- Copy status (複製狀態) - 複製的狀態。
  - Initializing (正在初始化) - 追蹤事件複製開始時顯示的初始狀態。
  - In progress (進行中) - 表示追蹤事件複製正在進行中。

    > **Note**
    >
    > 如果其他追蹤事件複製狀態為 In progress (進行中)，則無法複製追蹤事件。若要停止追蹤事件複製，請選擇 Stop copy (停止複製)。

  - Stopped (已停止) - 表示 Stop copy (停止複製) 動作已發生。若要重試追蹤事件複製，請選擇 Retry copy (重試複製)。
  - Failed (已失敗) - 複製已完成，但有些追蹤事件無法複製。檢閱 Copy failures (複製失敗) 中的錯誤訊息。若要重試追蹤事件複製，請選擇 Retry copy (重試複製)。當您重試副本時，會在發生失敗的位置 CloudTrail 繼續複製。
  - Completed (已完成) - 複製已完成且沒有錯誤。您可以在事件資料存放區中查詢複製的追蹤事件。
- Created time (建立時間) - 指出追蹤事件複製的開始時間。
- Finish time (完成時間) - 指出追蹤事件複製完成或停止的時間。

複製失敗

從 Copy failures (複製失敗) 中，您可以檢閱每個複製失敗的錯誤位置、錯誤訊息和錯誤類型。失敗的常見原因，包括 S3 前綴是否包含未壓縮的文件，或包含由非服務提供的文件。CloudTrail另一個可能的失敗原因與存取權問題有關。例如，如果事件資料存放區的 S3 儲存貯體未授與匯入事件的 CloudTrail 存取權，您將會收到`AccessDenied`錯誤訊息。

針對每個複製失敗，請檢閱下列錯誤資訊。

- Error location (錯誤位置) - 指出 S3 儲存貯體中發生錯誤的位置。如果因為來源 S3 儲存貯體包含未壓縮檔案而發生錯誤，Error location (錯誤位置) 將包含您可以在其中找到該檔案的字首。
- Error message (錯誤訊息) - 提供錯誤發生原因的說明。
- Error type (錯誤類型) - 提供錯誤類型。例如，Error type (錯誤類型) 為 `AccessDenied` 表示由於許可問題而發生錯誤。如需複製追蹤事件所需許可的詳細資訊，請參閱 複製追蹤事件所需的許可。

解決任何失敗後，請選擇 Retry copy (重試複製)。當您重試副本時，會在發生失敗的位置 CloudTrail 繼續複製。

範例：將追蹤事件複製到新事件資料存放區

本逐步解說說明如何將追蹤事件複製到新的 CloudTrail Lake 事件資料倉庫以進行歷史分析。如需有關複製追蹤事件的詳細資訊，請參閱 將追蹤事件複製到事件資料存放區。

若要將追蹤事件複製到新的事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇 Create event data store (建立事件資料存放區)。
4. 在「設定事件資料存放區」頁面的「一般」詳細資料中，為您的事件資料存放區命名，例如*my-management-events-eds*。根據最佳實務，請使用可快速識別事件資料存放區目的的名稱。如需 CloudTrail 命名需求的資訊，請參閱命名要求。
5. 選擇您想用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

   以下為可用的選項：

   - 一年可延長保留定價 – 如果您預期每月擷取的事件資料少於 25 TB，並需要長達 10 年的彈性保留期，則建議使用此選項。前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go 價格提供。此為預設選項。
     - 預設保留期：366 天
     - 最長保留期：3,653 天
   - 七年保留定價 – 如果您預期每月擷取的事件資料超過 25 TB，並需要長達 7 年的彈性保留期，則建議使用此選項。保留已包含在擷取定價中，無須額外付費。
     - 預設保留期：2,557 天
     - 最長保留期：2,557 天
6. 指定事件資料存放區的保留期。一年可延長保留定價選項的保留期可介於 7 天到 3,653 天 (約 10 年) 之間；或是七年保留定價選項，則可介於 7 天到 2,557 天 (約七年) 之間。

   CloudTrail Lake 會檢查事件是否在指定`eventTime`的保留期間內，以決定是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件超過 90 天時移除事件。`eventTime`

> **Note**
>
> CloudTrail 如果事件早於指定的`eventTime`保留期間，則不會複製該事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*)。例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。

7. (選用) 在加密中，選擇您是否想要使用自己的 KMS 金鑰加密事件資料存放區。依預設，事件資料存放區中的所有事件都會 CloudTrail 使用為您 AWS 擁有和管理的 KMS 金鑰加密。

   若要啟用使用您自己的 KMS 金鑰加密，請選擇使用我自己的 AWS KMS key。選擇 [新增] 為您 AWS KMS key 建立，或選擇現有以使用現有的 KMS 金鑰。在輸入 KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。使用自己的 KMS 金鑰時，您必須編輯 KMS 金鑰原則，以允許加密和解密 CloudTrail記錄。如需詳細資訊，請參閱設定 AWS KMS 金鑰原則 CloudTrail。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。

   > **Note**
   >
   > 若要為組織事件資料存放區啟用 AWS Key Management Service 加密，您必須為管理帳戶使用現有的 KMS 金鑰。

8. (選用) 如果您想使用 Amazon Athena 查詢自己的事件資料，請在 Lake 查詢聯合中選擇啟用。聯合可讓您在 AWS Glue Data Catalog 中檢視與事件資料存放區相關聯的中繼資料，並在 Athena 中對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱 聯合事件資料存放區。

   若要啟用 Lake 查詢聯合，請選擇啟用，然後執行下列動作：

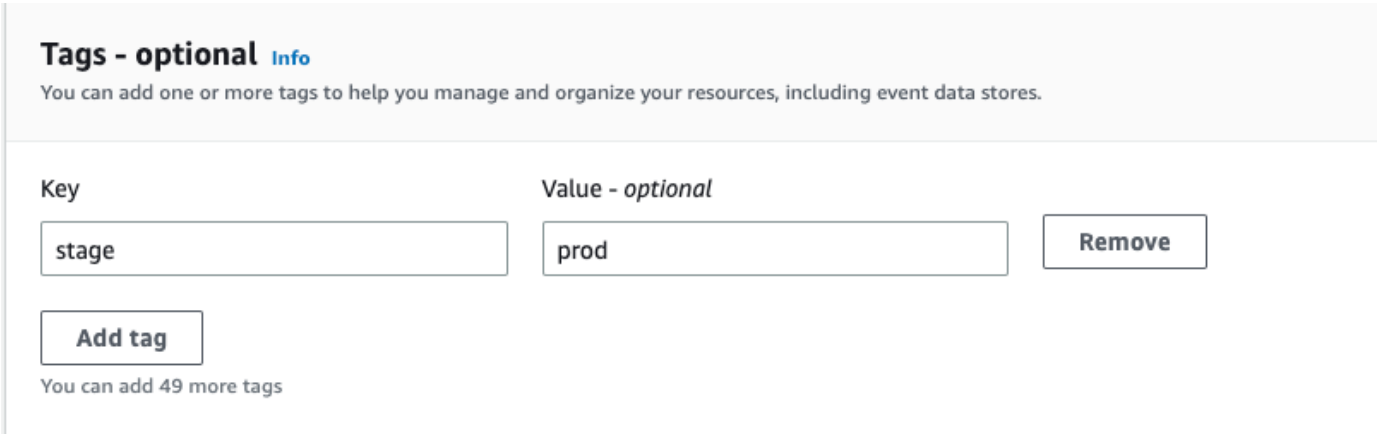
a. 選擇要建立新角色還是使用現有的 IAM 角色。AWS Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時，CloudTrail 會自動建立具有所需權限的角色。如果您選擇現有角色，請確認該角色的政策可提供必要的最低許可。

b. 如果您要建立新角色，請輸入名稱以識別角色。

c. 如果您要使用現有角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。

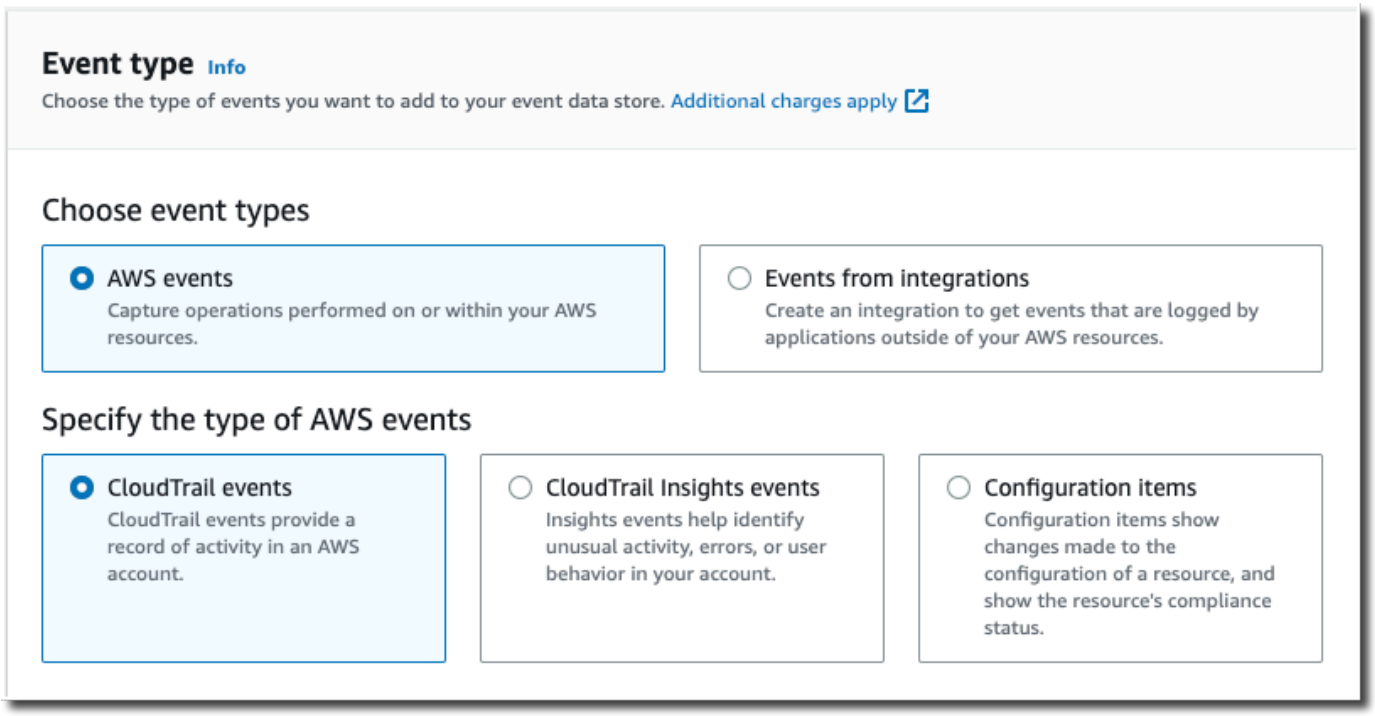
9. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的事件資料存放區。標籤可協助您識別 CloudTrail 事件資料存放區。例如，您可以附加名稱為 **`stage`**，值為 **`prod`** 的標籤。您可以使用標籤來限制對事件資料存放區的存取。您還可以使用標籤來追蹤事件資料存放區的查詢和擷取成本。

   如需有關如何使用標籤追蹤成本的資訊，請參閱 為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置。如需有關如何使用 IAM 政策，對以標籤為基礎的事件資料存放區授予存取權的資訊，請參閱 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。有關如何在中使用標籤的詳細資訊 AWS，請參閱《標記資 AWS 源使用指南》中的〈標記 AWS 資源〉。



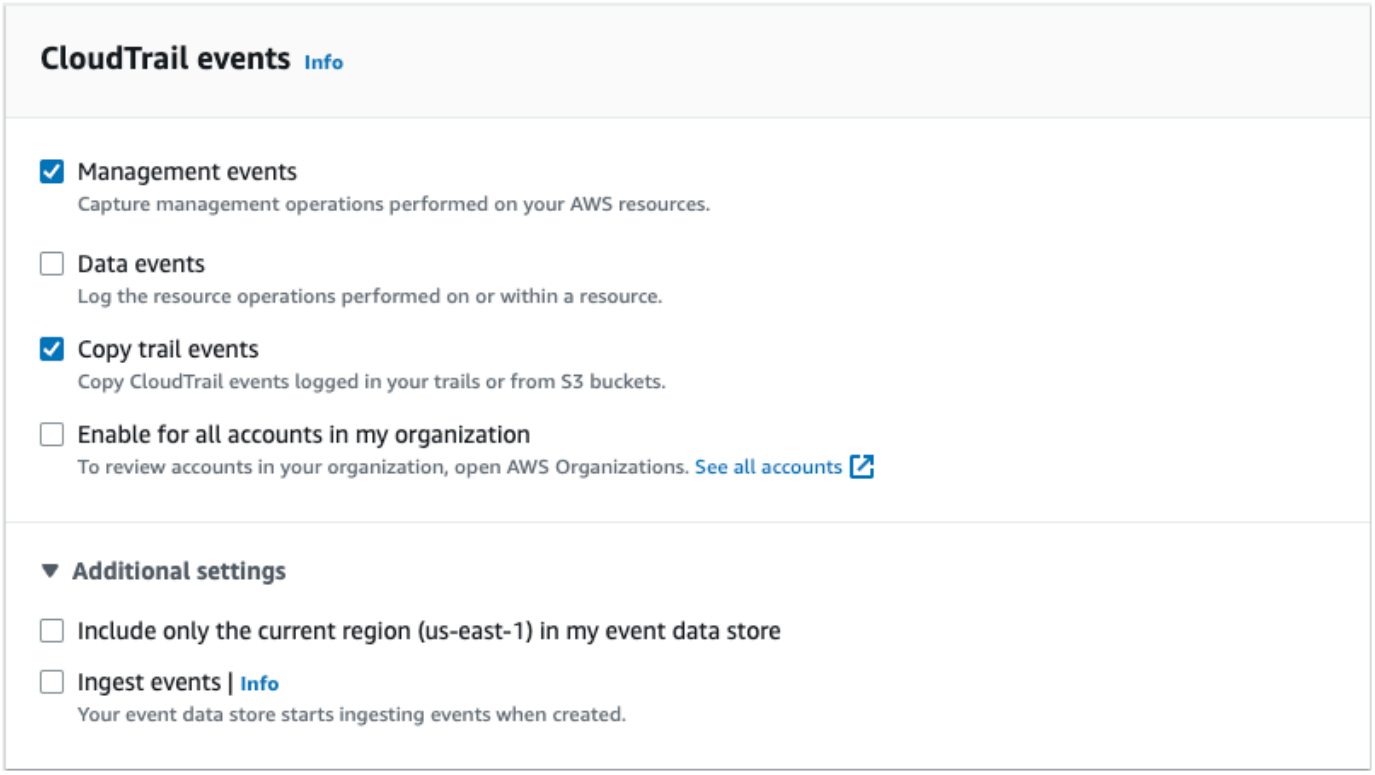
10. 選擇 Next (下一步) 以設定事件資料存放區。

11. 在選擇事件頁面上，保留事件類型的預設選項。



12. 對於CloudTrail 活動，我們將保留選取管理事件，然後選擇「複製追蹤事件」。在此範例中，我們不關心事件類型，因為我們只使用事件資料存放區來分析過往事件，而不會擷取未來事件。

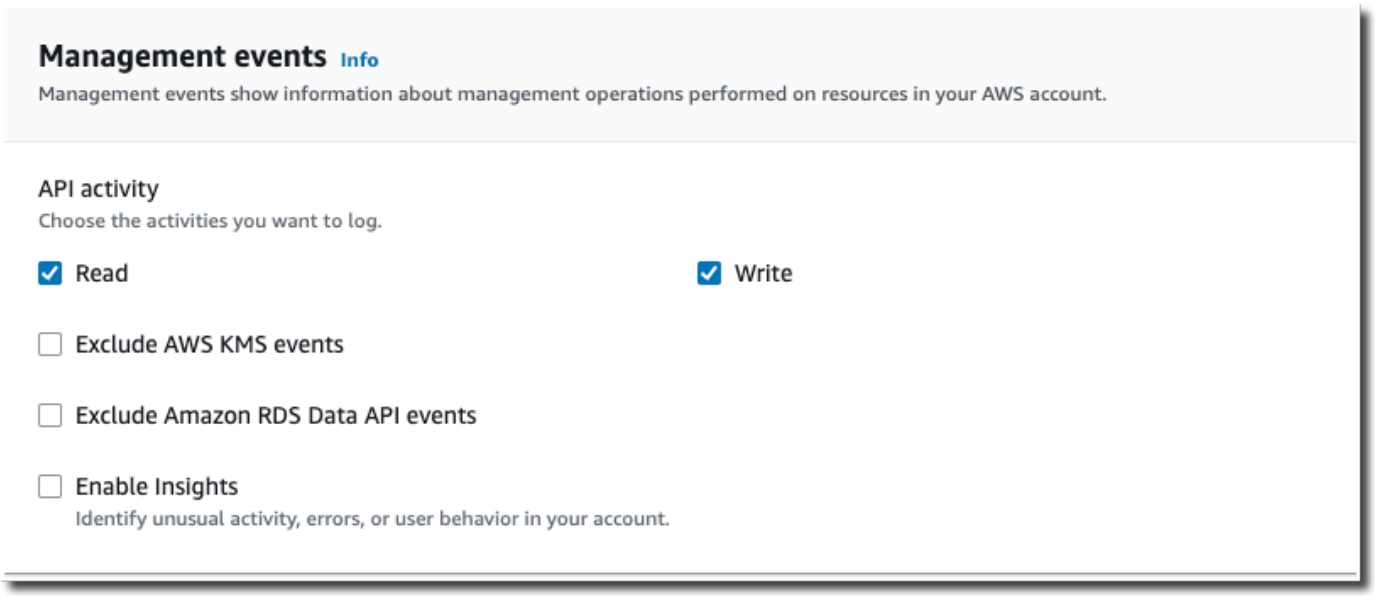
    如果您要建立事件資料存放區來取代現有的追蹤，選擇與追蹤相同的事件選取器，以確保事件資料存放區有相同的事件涵蓋範圍。



13. 如果這是組織事件資料存放區，選擇針對組織中的所有帳戶啟用。除非您已在 AWS Organizations 中設定帳戶，否則此選項將無法變更。

> **Note**
>
> 如果要建立組織事件資料存放區，您必須使用組織的管理帳戶登入，因為只有管理帳戶可以將追蹤事件複製到組織事件資料存放區。

14. 對於其他設定，我們將取消選取擷取事件，因為在此範例中，我們不希望事件資料存放區擷取任何未來事件，而且我們只對查詢複製的事件感興趣。依預設，事件資料存放區會為所有人收集事件，AWS 區域 並在建立事件時開始擷取事件。
15. 對於管理事件，我們將保留預設設定。



16. 在複製追蹤事件區域中，完成下列步驟。

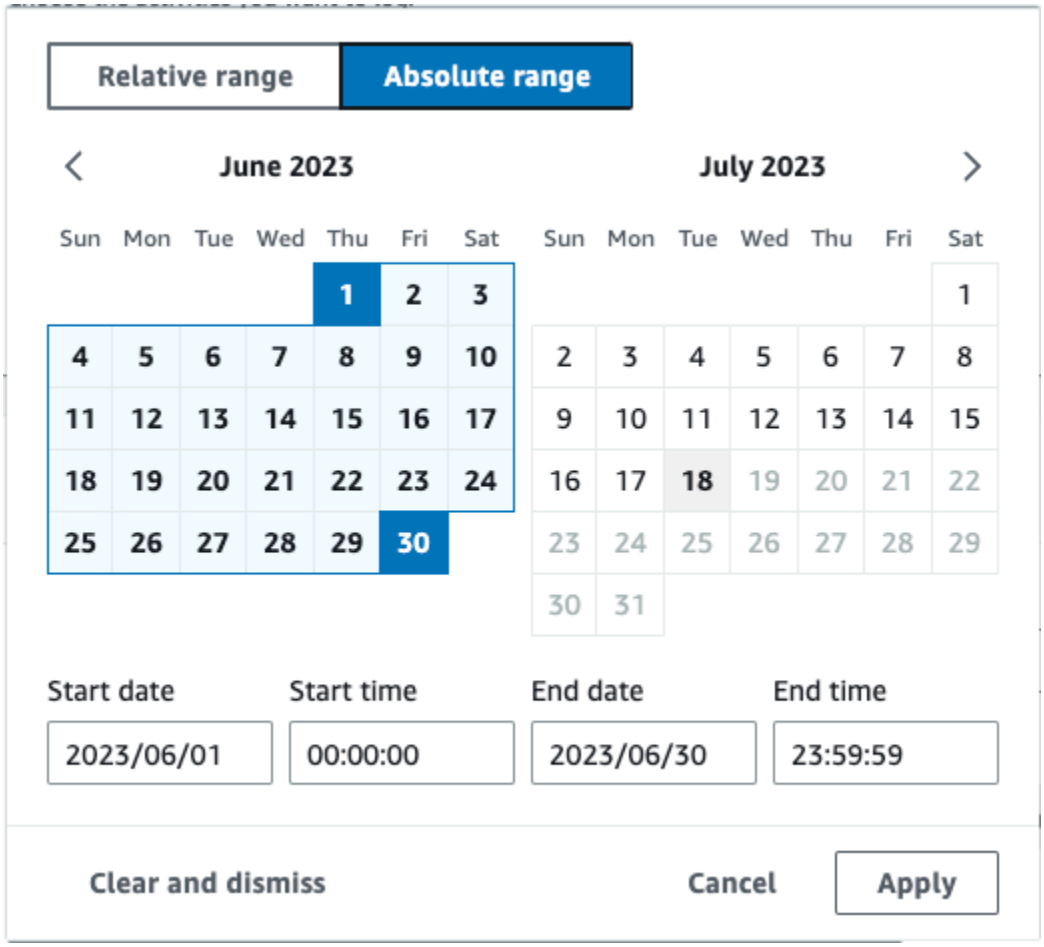
    a. 選擇您要複製的追蹤。在此範例中，我們將選擇名為 *`management-events`* 的追蹤。

    根據預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前綴。如果您要複製其他前置詞中包含的 CloudTrail 事件，請選擇 [輸入 S3 URI]，然後選擇 [瀏覽 S3] 以瀏覽至首碼。如果追蹤的來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策 CloudTrail 允許解密資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策，CloudTrail 以允許解密儲存貯體中的資料。如需更新 KMS 金鑰政策的詳細資訊，請參閱 用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策。

b. 選擇複製事件的時間範圍。 CloudTrail 在嘗試複製追蹤事件之前，先檢查字首和記錄檔名稱，以確認名稱包含在所選開始日期與結束日期之間的日期。您可以選擇 Relative range (相對範圍) 或 Absolute range (絕對範圍)。若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請選擇早於事件資料存放區建立日期的時間範圍。

- 如果您選擇「相對範圍」，則可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。 CloudTrail 複製所選期間內記錄的事件。
- 如果選擇「絕對範圍」，則可以選擇特定的開始日期和結束日期。 CloudTrail 複製所選開始日期和結束日期之間發生的事件。

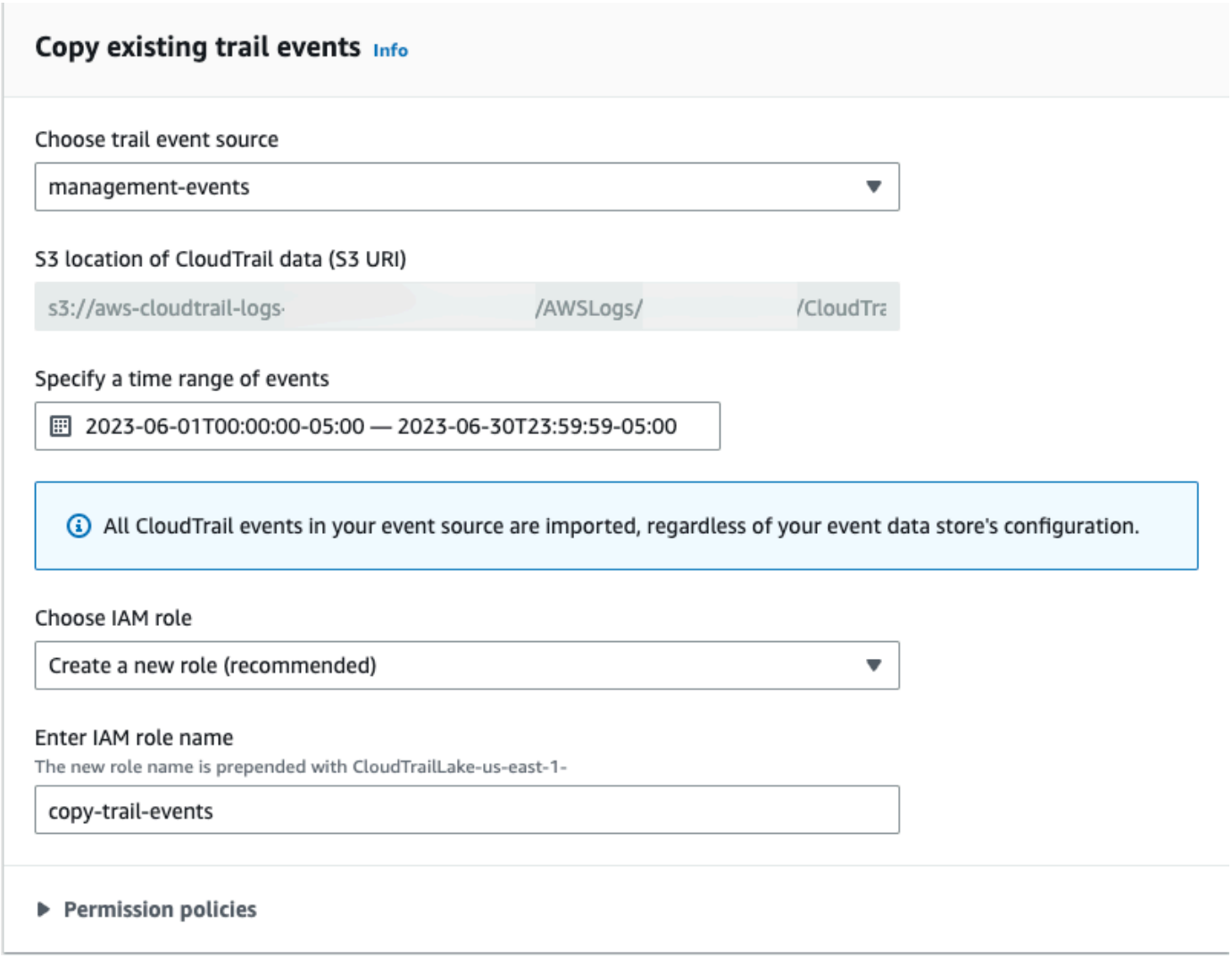
在此範例中，我們將選擇絕對範圍，然後選取整個六月份。



c. 對於 Permissions (許可)，從下列 IAM 角色選項中選擇。如果您選擇現有的 IAM 角色，請確認 IAM 角色政策提供必要的許可。如需更新 IAM 角色許可的詳細資訊，請參閱複製追蹤事件的 IAM 許可。

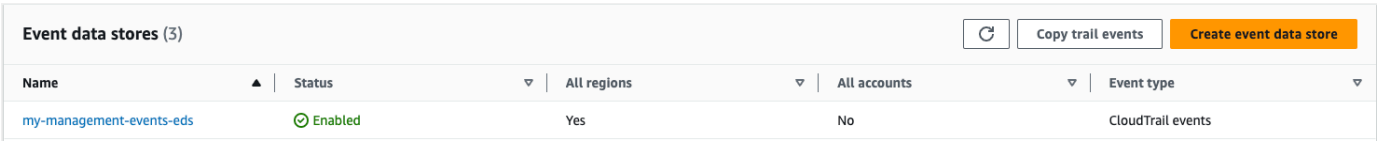
- 選擇 Create a new role (recommended) (建立新角色 (建議使用)) 以建立新的 IAM 角色。在「輸入 IAM 角色名稱」中，輸入角色的名稱。 CloudTrail 會自動為這個新角色建立必要的權限。
- 選擇「使用自訂 IAM 角色 ARN」以使用未列出的自訂 IAM 角色。對於 Enter IAM role ARN (輸入 IAM 角色 ARN)，輸入 IAM ARN。
- 從下拉式清單中選擇現有的 IAM 角色。

在此範例中，我們將選擇建立新角色 (建議)，並命名為 **`copy-trail-events`**。



17. 選擇 Next (下一步) 以檢閱您的選項。
18. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。

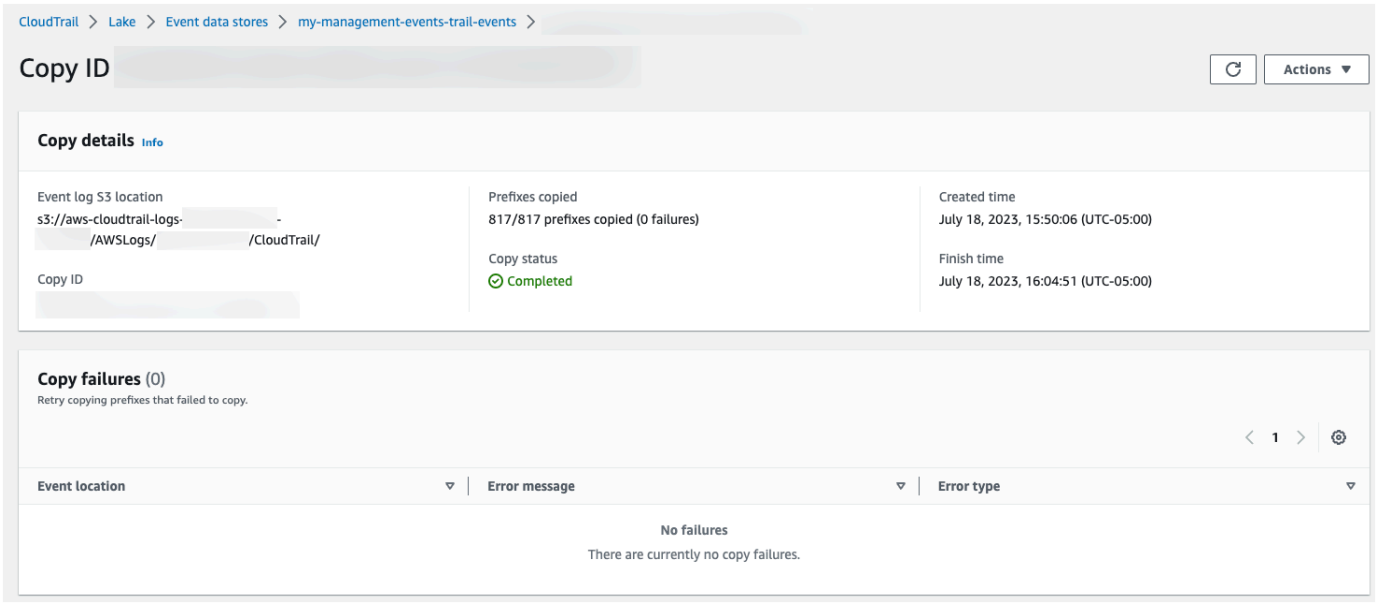
19. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。



20. 選擇事件資料存放區名稱，以檢視其詳細資訊頁面。詳細資訊頁面顯示您的事件資料存放區的詳細資訊以及複製狀態。事件複製狀態顯示在事件複製狀態區域中。

    追蹤事件複製完成時，如果沒有錯誤，則其 Copy status (複製狀態) 設定為 Completed (完成)；如果發生錯誤，則設定為 Failed (失敗)。

21. 若要檢視有關複製的詳細資訊，請在事件日誌 S3 位置欄中選擇複製名稱，或者選擇動作選單中檢視詳細資訊選項。如需檢視追蹤事件複製之詳細資訊，請參閱 事件複製詳細資訊。



22. 複製失敗區域會顯示複製追蹤事件時發生的任何錯誤。如果 Copy status (複製狀態) 是 Failed (失敗)，修正 Copy failures (複製失敗) 中顯示的任何錯誤，接著選擇 Retry copy (重試複製)。當您重試副本時，會在發生失敗的位置 CloudTrail 繼續複製。

聯合事件資料存放區

聯合事件資料存放區可讓您在資料目錄中檢視與事件資料存放區相關聯的中繼 AWS Glue 資料、向資料目錄註冊 AWS Lake Formation，以及讓您使用 Amazon Athena 針對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。

您可以使用 CloudTrail 主控台或 EnableFederationAPI 作業來啟用聯合。 AWS CLI啟用 Lake 查詢聯合時，會在「資料目錄」中 CloudTrail建立名為 `aws:cloudtrail` (如果資料庫尚未存在) 的受管理資料庫和受管理的聯合 AWS Glue 資料表。事件資料存放區 ID 用於表格名稱。 CloudTrail 在中註冊聯合角色 ARN 和事件資料存放區 AWS Lake Formation，該服務負責允許對資料目錄中聯合資源進行精細存取控制。 AWS Glue

若要啟用 Lake 查詢聯合，您必須建立新的 IAM 角色或選擇現有角色。Lake Formation 會使用此角色來管理聯合事件資料存放區的許可。當您使用 CloudTrail 主控台建立新角色時， CloudTrail 會自動為該角色建立必要的權限。如果您選擇現有角色，請確認該角色可提供最低許可。

您可以使用 CloudTrail 主控台或 DisableFederationAPI 作業停用聯合。 AWS CLI當您停用聯合時，請CloudTrail停用與 AWS Glue AWS Lake Formation、和 Amazon Athena 的整合。停用 Lake 查詢聯合後，您將無法再於 Athena 中查詢事件資料。當您停用聯合時，不會刪除任何 CloudTrail Lake 資料，而且您可以繼續在 CloudTrail Lake 中執行查詢。

聯合 CloudTrail Lake 事件資料存放區不 CloudTrail 收取任何費用。在 Amazon Athena 中執行查詢會產生費用。如需 Athena 定價的詳細資訊，請參閱 Amazon Athena 定價。

使用 AWS CloudTrail 湖泊和 Amazon Athena 分析活動日誌

主題

考量事項

聯合事件資料存放區時，請考量下列因素：

- 聯合 CloudTrail Lake 事件資料存放區不 CloudTrail 收取任何費用。在 Amazon Athena 中執行查詢會產生費用。如需 Athena 定價的詳細資訊，請參閱 Amazon Athena 定價。
- Lake Formation 可用來管理聯合資源的許可。如果您刪除聯合角色，或從 Lake Formation 撤銷資源的權限 AWS Glue，或者，您無法從 Athena 執行查詢。如需有關使用 Lake Formation 的詳細資訊，請參閱管理 CloudTrail 湖泊聯合資源 AWS Lake Formation。
- 使用 Amazon Athena 查詢向 Lake Formation 註冊之資料的任何人，都必須擁有允許 `lakeformation:GetDataAccess` 動作的 IAM 許可政策。受 AWS 管理策略：AmazonAthenaFullAccess允許此處理行動。如果您使用內嵌政策，請務必更新許可政策來允許此動作。如需詳細資訊，請參閱管理 Lake Formation 和 Athena 使用者許可。
- 若要在 Athena 中建立聯合資料表的檢視，您需要 `aws:cloudtrail` 以外的目的地資料庫。這是因為資`aws:cloudtrail`料庫是由 CloudTrail.
- 若要在 Amazon 中建立資料集 QuickSight，您必須選擇使用自訂 SQL 選項。如需詳細資訊，請參閱使用 Amazon Athena 資料建立資料集。
- 如果已啟用聯合，則無法刪除事件資料存放區。若要刪除聯合事件資料存放區，您必須先停用聯合和終止保護 (若已啟用)。
- 下列考量適用於組織事件資料存放區：
  - 只有一個委派管理員帳戶或管理帳戶可以在組織事件資料存放區上啟用聯合。其他委派管理員帳戶仍可使用 Lake Formation 資料共用功能來查詢和共用資訊。
  - 任何委派管理員帳戶或組織的管理帳戶都能停用聯合。

聯合的所需許可

聯合事件資料存放區之前，請確認您擁有聯合角色以及啟用和停用聯合所需的所有許可。如果您選擇現有的 IAM 角色來啟用聯合，則只需要更新 IAM 角色許可。如果您選擇使用 CloudTrail 主控台建立新的 IAM 角色，請 CloudTrail 提供該角色的所有必要許可。

主題

- 用於聯合事件資料存放區的 IAM 許可
- 啟用聯合所需的許可
- 停用聯合所需的許可

用於聯合事件資料存放區的 IAM 許可

啟用聯合時，您可以選擇建立新的 IAM 角色，也可以使用現有的 IAM 角色。當您選擇新的 IAM 角色時，請 CloudTrail 建立具有所需許可的 IAM 角色，您不需要進一步採取任何動作。

如果您選擇現有角色，請確保 IAM 角色的政策可提供啟用聯合所需的許可。此區段提供所需 IAM 角色許可和信任政策的範例。

下列範例提供聯合角色的許可政策。對於第一個陳述式，請為 Resource 提供事件資料存放區的完整 ARN。

此政策中的第二個陳述式，可讓 Lake Formation 為使用 KMS 金鑰加密的事件資料存放區解密資料。將 *key-region*、*account-id* 和 *key-id* 取代為 KMS 金鑰的值。如果您的事件資料存放區不會使用 KMS 金鑰進行加密，您可以省略此陳述式。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

下列範例提供 IAM 信任政策，此政策可讓 AWS Lake Formation 擔任 IAM 角色來管理聯合事件資料存放區的許可。

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

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

啟用聯合所需的許可

下列範例政策提供在事件資料存放區上啟用聯合所需的最低許可。此原則 CloudTrail 允許在事件資料存放區上啟用聯合、 AWS Glue 在資料目錄中建立聯合資源， AWS Lake Formation 以及管理資源註冊。 AWS Glue

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
```

```
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

停用聯合所需的許可

下列範例政策提供在事件資料存放區上停用聯合所需的最少資源。此原則允許停 CloudTrail 用事件資料存放區上的聯合、 AWS Glue 刪除資料目錄中受管理的聯合 AWS Glue 資料表，以及 Lake Formation 以取消註冊聯合資源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "Allow Lake Formation to deregister the resource",
```

```
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

啟用 Lake 查詢聯合

您可以使用 CloudTrail 主控台或 EnableFederationAPI 作業來啟用 Lake 查詢聯合。 AWS CLI啟用 Lake 查詢聯合時，會在「資料目錄」中 CloudTrail 建立名為 `aws:cloudtrail` (如果資料庫尚未存在) 的受管理資料庫和受管理的聯合 AWS Glue 資料表。事件資料存放區 ID 用於表格名稱。CloudTrail 在中註冊聯合角色 ARN 和事件資料存放區 AWS Lake Formation，該服務負責允許對資料目錄中聯合資源進行精細存取控制。 AWS Glue

本節說明如何使用 CloudTrail 主控台和啟用聯合 AWS CLI。

CloudTrail console

下列程序展示如何在現有事件資料存放區上啟用 Lake 查詢聯合。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇您要更新的事件資料存放區。這會開啟事件資料存放區的詳細資訊頁面。
4. 在 Lake 查詢聯合中，選擇編輯，然後選擇啟用。
5. 選擇是要建立新的 IAM 角色，還是使用現有角色。當您建立新角色時， CloudTrail 會自動建立具有所需權限的角色。如果您使用現有角色，請確認該角色的政策可提供所需的最低許可。
6. 如果您要建立新的 IAM 角色，請輸入角色的名稱。
7. 如果您要選擇現有的 IAM 角色，請選擇想使用的角色。該角色必須存在於您的帳戶中。
8. 選擇儲存變更。聯合狀態會變更為 `Enabled`。

AWS CLI

若要啟用聯合，請執行 aws cloudtrail enable-federation 命令，並提供必要的 --event-data-store 和 --role 參數。針對 --event-data-store，提供事件資料存放區 ARN (或 ARN 的 ID 尾碼)。針對 --role，提供您的聯合角色 ARN。該角色必須存在於您的帳戶中，並提供所需的最低許可。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

此範例展示委派管理員如何在管理帳戶中指定事件資料存放區的 ARN，以及在委派管理員帳戶中指定聯合角色的 ARN，進而在組織事件資料存放區上啟用聯合。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

停用 Lake 查詢聯合

您可以使用 CloudTrail 主控台或 DisableFederationAPI 作業停用聯合。 AWS CLI當您停用聯合時，請 CloudTrail 停用與 AWS Glue AWS Lake Formation、和 Amazon Athena 的整合。停用 Lake 查詢聯合後，您將無法再於 Athena 中查詢事件資料。當您停用聯合時，不會刪除任何 CloudTrail Lake 資料，而且您可以繼續在 CloudTrail Lake 中執行查詢。

本節說明如何使用 CloudTrail 主控台和停用聯合 AWS CLI。

CloudTrail console

下列程序展示如何在現有事件資料存放區上停用 Lake 查詢聯合。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇您要更新的事件資料存放區。這會開啟事件資料存放區的詳細資訊頁面。
4. 在 Lake 查詢聯合中，選擇編輯，然後選擇停用。
5. 選擇儲存變更。聯合狀態會變更為 Disabled。

AWS CLI

若要在事件資料存放區上停用聯合，請執行 aws cloudtrail disable-federation 命令。由 --event-data-store 指定的事件資料存放區，它接受事件資料存放區 ARN 或 ARN 的 ID 尾碼。

```
aws cloudtrail disable-federation
```

```
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> 如果這是組織事件資料存放區，請使用管理帳戶的帳戶 ID。

管理 CloudTrail 湖泊聯合資源 AWS Lake Formation

聯合事件資料存放區時，會在中 CloudTrail 註冊聯合角色 ARN 和事件資料存放區 AWS Lake Formation，該服務負責允許對資料目錄中聯合資源進行精細存取控制。 AWS Glue 本節說明如何使用 Lake Formation 來管理 CloudTrail 湖泊聯合資源。

啟用聯合時，會在資 AWS Glue 料目錄中 CloudTrail 建立下列資源。

- 受管理的資料庫 — CloudTrail 使用`aws:cloudtrail`每個帳戶的名稱建立 1 個資料庫。 CloudTrail 管理數據庫。您無法刪除或修改中的資料庫 AWS Glue。
- 受管理的聯合資料表 — 為每個聯合事件資料存放區 CloudTrail 建立 1 個表格，並將事件資料存放區 ID 用於表格名稱。 CloudTrail 管理表格。您無法刪除或修改中的表格 AWS Glue。若要刪除資料表，您必須在事件資料存放區上停用聯合。

控制聯合資源的存取權限

您可以使用以下兩種許可方法之一來控制受管資料庫和資料表的存取權限。

- 僅限 IAM 存取控制 – 透過僅限 IAM 存取控制，帳戶中具有所需 IAM 許可的所有使用者均有權存取所有 Data Catalog 資源。如需如何使 AWS Glue 用 IAM 的詳細資訊，請參閱如 AWS Glue 何使用 IAM。

  在 Lake Formation 主控台上，此方法會顯示為僅限 IAM 存取控制。

  > **Note**
  >
  > 如果您要建立資料篩選條件並使用其他 Lake Formation 功能，則必須使用 Lake Formation 存取控制。

- Lake Formation 存取控制 – 此方法具備下列優點。
  - 您可以建立資料篩選條件，來實作資料欄層級、資料列層級和儲存格層級安全性。

- 只有 Lake Formation 管理員與資料庫和資源的建立者可以看到資料庫和資料表。如果其他使用者需要存取這些資源，您必須明確使用 Lake Formation 許可授予存取權限。

如需存取控制的詳細資訊，請參閱精細存取控制的方法。

決定聯合資源的許可方法

首次啟用聯合時，會使用 Lake Formation 資料湖設定 CloudTrail 建立受管理的資料庫和受管理的聯合表格。

CloudTrail 啟用聯合之後，您可以檢查這些資源的權限，以確認受管理資料庫和受管理的聯合資料表使用的權限方法。如果資源存在 ALL (Super) 至 IAM_ALLOWED_PRINCIPALS 的設定，則資源僅能由 IAM 許可管理。如果缺少該設定，則資源將由 Lake Formation 許可管理。如需 Lake Formation 許可的詳細資訊，請參閱 Lake Formation 許可參考。

受管資料庫和受管聯合資料表的許可方法可能不同。舉例來說，如果您檢查資料庫和資料表的值，可能會看到下列內容：

- 若為資料庫，則指派 ALL (Super) 至 IAM_ALLOWED_PRINCIPALS 的值會顯示在許可中，表示您正在對資料庫使用僅限 IAM 存取控制。
- 若為資料表，則不會顯示指派 ALL (Super) 至 IAM_ALLOWED_PRINCIPALS 的值，這表示透過 Lake Formation 許可進行存取控制。

您可以在 Lake Formation 中對任何聯合資源新增或移除 ALL (Super) 至 IAM_ALLOWED_PRINCIPALS 的許可，藉此隨時切換存取方法。

使用 Lake Formation 進行跨帳戶共用

本節說明如何使用 Lake Formation 跨帳戶共用受管資料庫和受管聯合資料表。

您可以執行下列步驟，以跨帳戶共用受管資料庫：

1. 將跨帳戶資料共用版本更新至第 4 版。
2. 從資料庫移除 Super 至 IAM_ALLOWED_PRINCIPALS 的許可 (如有)，以切換至 Lake Formation 存取控制。
3. 將 Describe 許可授予資料庫上的外部帳戶。
4. 如果資料目錄資源已與您共用， AWS 帳戶 且您的帳號與共用帳號不在同一個 AWS 組織中，請接受來自 AWS Resource Access Manager (AWS RAM) 的資源共用邀請。如需詳細資訊，請參閱接受來自 AWS RAM 的資源共用邀請。

完成這些步驟後，外部帳戶應該可以看到資料庫。依預設，共用資料庫未授予資料庫中任何資料表的存取權限。

您可以執行下列步驟，與外部帳戶共用所有或個別的受管聯合資料表：

1. 將跨帳戶資料共用版本更新至第 4 版。
2. 從資料表移除 `Super` 至 `IAM_ALLOWED_PRINCIPALS` 的許可 (如有)，以切換至 Lake Formation 存取控制。
3. (選用) 指定任何資料篩選條件，以限制資料欄或資料列。
4. 將 `Select` 許可授予資料表上的外部帳戶。
5. 如果資料目錄資源已與您共用， AWS 帳戶 且您的帳號與共用帳號不在同一個 AWS 組織中，請接受來自 AWS Resource Access Manager (AWS RAM) 的資源共用邀請。對於組織，您可以使用 RAM 設定來自動接受。如需詳細資訊，請參閱接受來自 AWS RAM 的資源共用邀請。
6. 您現在應該可以看到資料表。若要在此資料表上啟用 Amazon Athena 查詢，請在此帳戶中使用共用資料表建立資源連結。

擁有帳戶可以隨時撤銷共用，方法是從 Lake Formation 移除外部帳戶的權限，或停用中的聯合 CloudTrail。

組織事件資料存放區

如果您已在中建立組織 AWS Organizations，則可以建立一個組織事件資料存放區，以記錄該組織 AWS 帳戶 中所有人的所有事件。組織事件資料倉庫可套用至所有 AWS 區域或目前的「區域」。您無法使用組織事件資料存放區來收集 AWS外部事件。

您可以使用管理帳戶或委派的管理員帳戶來建立組織事件資料存放區。委派管理員建立組織事件資料存放區後，該組織事件資料存放區會存在於組織的管理帳戶中。採用此方法是因為管理帳戶會維護所有組織資源的擁有權。

組織的管理帳戶可以更新帳戶層級事件資料倉庫，以將其套用至組織。

組織事件資料存放區在獲指定套用至組織後，將會自動套用至組織中的所有成員帳戶。成員帳戶無法查看組織事件資料存放區，也無法加以修改或刪除。在預設情況下，成員帳戶無法存取組織事件資料存放區，也無法在事件資料存放區上執行查詢。

下表顯示 AWS Organizations 組織內管理帳戶和委派管理員帳戶的權能。

功能	管理帳戶	委派管理員帳戶
註冊或移除委派管理員帳戶。	是	否
為 AWS CloudTrail 事件或組 AWS Config 態項目建立組織事件資料存放區。	是	是
啟用組織事件資料存放區上的 Insights。	是	否
更新組織事件資料存放區。	是	是 [1]
在組織事件資料存放區上啟用 Lake 查詢聯合。[2]	是	是
停用組織事件資料存放區上的 Lake 查詢聯合。	是	是
刪除組織事件資料存放區。	是	是
將追蹤事件複製到事件資料存放區。	是	否
對組織事件資料存放區執行查詢。	是	是
檢視組織事件資料存放區的 CloudTrail Lake 儀表板。	是	是

[1] 只有管理帳戶可以將組織事件資料倉庫轉換為帳戶層級事件資料倉庫，或將帳戶層級事件資料倉庫轉換為組織事件資料存放區。委派管理員無法執行這些動作，因為組織事件資料存放區僅存在於管理帳戶中。將組織事件資料倉庫轉換為帳戶層級事件資料存放區時，只有管理帳戶可以存取事件資料倉庫。同樣地，只有管理帳戶中的帳戶層級事件資料存放區才能轉換為組織事件資料存放區。

[2]只有一個委派管理員帳戶或管理帳戶可以在組織事件資料存放區上啟用聯合。其他委派管理員帳戶可以使用 Lake Formation 資料共用功能查詢和共享資訊。任何委派管理員帳戶和組織的管理帳戶都能停用聯合。

建立組織事件資料倉庫

組織的管理帳戶或委派管理員帳戶可以建立組織事件資料存放區，以收集 CloudTrail 事件 (管理事件、資料事件) 或組 AWS Config 態項目。

> **Note**
>
> 只有組織的管理帳戶可以將追蹤事件複製到事件資料存放區。

CloudTrail console

若要使用主控台建立組織事件資料存放區

1. 遵循為 CloudTrail 事件建立事件資料存放區程序中的步驟，為 CloudTrail 管理或資料事件建立組織事件資料存放區。

   或

   請遵循建立組態項目的事件資料存放區程序中的步驟，為組 AWS Config 態項目建立組 AWS Config 態事件資料存放區。
2. 在 [選擇事件] 頁面上，選擇 [為組織中的所有帳戶啟用]。

AWS CLI

若要建立組織事件資料倉庫，請執行create-event-data-store指令並包含選`--organization-enabled`項。

下列範例 AWS CLI `create-event-data-store`命令會建立收集所有管理事件的組織事件資料存放區。由於預設為記 CloudTrail 錄管理事件，因此如果您的事件資料存放區正在記錄所有管理事件且未收集任何資料事件，則不需要指定進階事件選取器。

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
```

```
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

下一個範例 AWS CLI `create-event-data-store`指令會建立名為收集組 AWS Config 態項目`config-items-org-eds`的組織事件資料倉庫。若要收集組態項目，請在進階事件選取器`ConfigurationItem`中指定`eventCategory`欄位等於。

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

將帳戶層級事件資料存放區套用至組織

組織的管理帳戶可以轉換帳戶層級事件資料存放區，以將其套用至組織。

CloudTrail console

使用主控台更新帳戶層級事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇您要更新的事件資料存放區。此動作會開啟事件資料存放區的詳細資訊頁面。
4. 在 General details (一般詳細資訊) 中，選擇 Edit (編輯)。
5. 針對組織中的所有帳戶選擇 [啟用]。
6. 選擇儲存變更。

如需更新事件資料倉庫的其他資訊，請參閱使用主控台更新事件資料存放區。

AWS CLI

若要更新帳戶層級事件資料倉庫以將其套用至組織，請執行指update-event-data-store令並包含選--organization-enabled項。

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

另請參閱

- 組織委派的管理員
- 新增 CloudTrail 委派管理員
- 移除 CloudTrail 委派管理員

建立與事件來源以外的整合 AWS

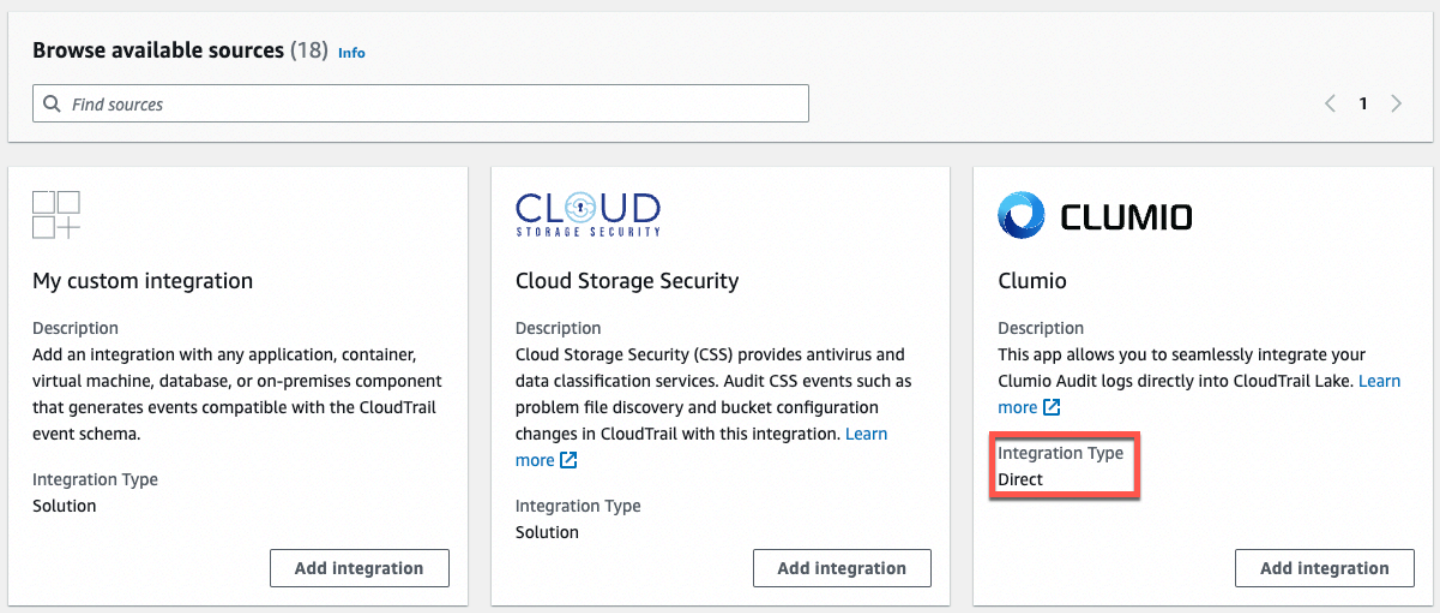
您可以用 CloudTrail 來記錄和儲存混合式環境中任何來源的使用者活動資料，例如內部部署或雲端中託管的 SaaS 應用程式、虛擬機器或容器。您可以針對此資料進行儲存、存取、分析、疑難排解和採取行動，而不需維護多個日誌彙總工具和報告工具。

來自非來AWS 源的活動活動是使用管道將活動從與 CloudTrail之合作的外部合作夥伴或從您自己的來源引入 CloudTrail Lake。建立通道時，您可以選擇一或多個事件資料存放區，以儲存從通道來源到達的事件。只要目的地事件資料存放區設定為記錄 `eventCategory="ActivityAuditLog"` 事件，您就可以視需要變更通道的目的地事件資料存放區。當您為來自外部合作夥伴的事件建立通道時，您會將通道 ARN 提供給合作夥伴或來源應用程式。連接至通道的資源政策允許來源透過通道傳輸事件。如果通道沒有資源政策，則只有通道擁有者可以在通道上呼叫 `PutAuditEvents` API。

CloudTrail 已與許多事件來源供應商合作，例如 Okta 和。 LaunchDarkly當您與外部事件來源建立整合時 AWS，您可以選擇其中一個合作夥伴作為您的事件來源，或選擇 [我的自訂整合]，將您自己來源的事件整合至中 CloudTrail。每個來源最多可有一個通道。

整合有兩種類型：直接和解決方案。透過直接整合，合作夥伴會呼叫 `PutAuditEvents` API，將事件傳送至您 AWS 帳戶的事件資料存放區。透過解決方案整合，應用程式會在您的 AWS 帳戶中執行，而應用程式會呼叫 `PutAuditEvents` API，將事件傳送至您 AWS 帳戶的事件資料存放區。

在 Integrations (整合) 頁面中，您可以選擇 Available sources (可用來源) 索引標籤，以檢視合作夥伴的 Integration type (整合類型)。



若要開始使用，請使用 CloudTrail 主控台建立整合，以記錄來自夥伴或其他應用程式來源的事件。

主題

- 透過主控台與合作 CloudTrail 夥伴建立整合
- 使用主控台建立自訂整合
- 建立、更新和管理 CloudTrail 湖泊整合 AWS CLI

- 整合合作夥伴的其他資訊
- CloudTrail 湖集成事件架構

透過主控台與合作 CloudTrail 夥伴建立整合

當您與外部事件來源建立整合時 AWS，您可以選擇其中一個合作夥伴作為您的事件來源。當您在 CloudTrail 與合作夥伴應用程式中建立整合時，合作夥伴需要您在此工作流程中建立的通道的 Amazon 資源名稱 (ARN)，以便將事件傳送至其中。 CloudTrail建立整合之後，您可以依照合作夥伴的指示，將所需的通道 ARN 提供給合作夥伴，以完成整合的設定。`PutAuditEvents`在合作夥伴撥打整合的通道 CloudTrail 後，整合便會開始將合作夥伴事件導入其中。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的整合。
3. 在 Add integration (新增整合) 頁面上，輸入通道的名稱。名稱長度範圍是 3-128 個字元。只能使用字母、數字、句號、底線和破折號。
4. 選擇您要從中取得事件的合作夥伴應用程式來源。如果您要與內部部署或雲端中託管的自有應用程式的事件整合，請選擇 My custom integration (我的自訂整合)。
5. 在 Event delivery location (事件傳送位置) 中，選擇將相同的活動事件記錄到現有事件資料存放區，或建立新的事件資料存放區。

   如果您選擇建立新的事件資料存放區，請輸入事件資料存放區的名稱，選擇定價選項，並指定保留期間 (以天為單位)。事件資料存放區會在指定的天數內保留事件資料。

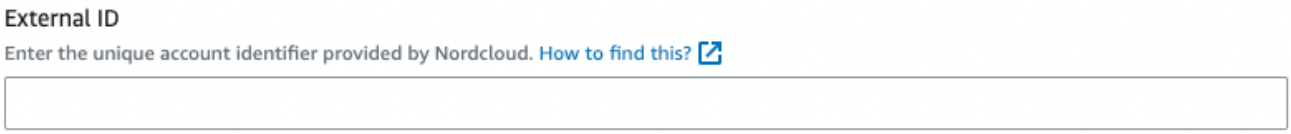
   如果您選擇將活動事件記錄到一或多個現有事件資料存放區，請從清單中選擇事件資料存放區。事件資料存放區只能包含活動事件。主控台中的事件類型必須是 Events from integrations (來自整合的事件)。在 API 中，`eventCategory` 值必須是 `ActivityAuditLog`。
6. 在 Resource policy (資源政策) 中，為整合的通道設定資源政策。資源政策是 JSON 政策文件，這些文件會指出指定的主體可對資源執行哪些動作以及相關條件。在資源政策中定義為主體的帳戶可以呼叫 `PutAuditEvents` API，將事件傳送至您的通道。如果資源擁有者的 IAM 政策允許 `cloudtrail-data:PutAuditEvents` 動作，則資源擁有者對資源具有隱含存取權。

   政策所需的資訊取決於整合類型。若要進行方向整合， CloudTrail 會自動新增合作夥伴的 AWS 帳戶 ID，並要求您輸入合作夥伴提供的唯一外部 ID。對於解決方案整合，您必須至少指定一個 AWS 帳戶 ID 作為主體，並且可以選擇性地輸入外部 ID 以防止混淆的副手。

> **Note**
>
> 如果您沒有為通道建立資源政策，則只有通道擁有者可以在通道上呼叫 `PutAuditEvents` API。

a. 對於直接整合，請輸入合作夥伴提供的外部 ID。整合合作夥伴提供唯一外部 ID，例如帳戶 ID 或隨機產生的字串，以供整合用於預防混淆代理人。合作夥伴負責建立並提供唯一外部 ID。

   您可以選擇 How to find this? (如何尋找此資訊？) 以檢視合作夥伴有關描述如何尋找外部 ID 的文件。



> **Note**
>
> 如果資源政策包含外部 ID，則對 `PutAuditEvents` API 的所有呼叫都必須包含外部 ID。不過，如果政策未定義外部 ID，合作夥伴仍可呼叫 `PutAuditEvents` API 並指定 `externalId` 參數。

b. 對於解決方案整合，請選擇 [新增 AWS AWS 帳戶] 以指定要新增為策略中主體的帳戶 ID。

7. (選用) 在 Tags (標籤) 區域中，您最多可以新增 50 個標籤索引鍵和值組，以協助您識別、排序和控制對事件資料存放區及通道的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。如需有關如何在中使用標籤的詳細AWS 資訊 AWS，請參閱 AWS 一般參考.

8. 當您準備好建立新整合時，請選擇 Add integration (新增整合)。沒有評論頁面。 CloudTrail 建立整合，但您必須向合作夥伴應用程式提供管道 Amazon 資源名稱 (ARN)。如需將通道 ARN 提供給合作夥伴應用程式的說明，請參閱合作夥伴文件網站。如需詳細資訊，請在 Integrations (整合) 頁面的 Available sources (可用來源) 索引標籤中選擇合作夥伴的 Learn more (進一步了解) 連結，以在 AWS Marketplace中開啟合作夥伴的頁面。

若要完成整合的設定，請將通道 ARN 提供給合作夥伴或來源應用程式。視整合類型而定，您、合作夥伴或應用程式會執行 `PutAuditEvents` API，將活動事件傳送至您 AWS 帳戶的事件資料存放區。傳

送活動事件後，您可以使用 CloudTrail Lake 搜尋、查詢和分析應用程式記錄的資料。您的事件資料包含符合 CloudTrail事件裝載的欄位`eventVersion`，例如`eventSource`、和`userIdentity`。

使用主控台建立自訂整合

您可以用 CloudTrail 來記錄和儲存混合式環境中任何來源的使用者活動資料，例如內部部署或雲端中託管的 SaaS 應用程式、虛擬機器或容器。在 CloudTrail Lake 主控台中執行此程序的前半部分，然後呼叫 `PutAuditEvents`API 以擷取事件，提供您的頻道 ARN 和事件承載。使用 `PutAuditEvents` API 擷取應用程式活動後 CloudTrail，您可以使用 CloudTrail Lake 搜尋、查詢和分析應用程式記錄的資料。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的整合。
3. 在 Add integration (新增整合) 頁面上，輸入通道的名稱。名稱長度範圍是 3-128 個字元。只能使用字母、數字、句號、底線和破折號。
4. 選擇 My custom integration (我的自訂整合)。
5. 在 Event delivery location (事件傳送位置) 中，選擇將相同的活動事件記錄到現有事件資料存放區，或建立新的事件資料存放區。

   如果您選擇建立新的事件資料存放區，請輸入事件資料存放區的名稱，並指定保留期間 (以天為單位)。如果您選擇一年可延長保留定價選項，則可將事件資料保留在事件資料存放區中最多 3,653 天 (約 10 年)；如果您選擇七年保留定價選項，則最多可保留 2,557 天 (約 7 年)。

   如果您選擇將活動事件記錄到一或多個現有事件資料存放區，請從清單中選擇事件資料存放區。事件資料存放區只能包含活動事件。主控台中的事件類型必須是 Events from integrations (來自整合的事件)。在 API 中，`eventCategory` 值必須是 `ActivityAuditLog`。
6. 在 Resource policy (資源政策) 中，為整合的通道設定資源政策。資源政策是 JSON 政策文件，這些文件會指出指定的主體可對資源執行哪些動作以及相關條件。在資源政策中定義為主體的帳戶可以呼叫 `PutAuditEvents` API，將事件傳送至您的通道。

> **Note**
>
> 如果您沒有為通道建立資源政策，則只有通道擁有者可以在通道上呼叫 `PutAuditEvents` API。

a. (選用) 輸入唯一外部 ID，多提供一層保護。外部 ID 是唯一字串，例如帳戶 ID 或隨機產生的字串，用於預防混淆代理人。

> **Note**
>
> 如果資源政策包含外部 ID，則對 PutAuditEvents API 的所有呼叫都必須包含外部 ID。不過，如果政策未定義外部 ID，您仍可呼叫 PutAuditEvents API 並指定 externalId 參數。

b. 選擇 [新增 AWS 帳號] 以指定要新增為通道資源策略中主參與者的每個 AWS 帳號 ID。

7. (選用) 在 Tags (標籤) 區域中，您最多可以新增 50 個標籤索引鍵和值組，以協助您識別、排序和控制對事件資料存放區及通道的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。如需有關如何在中使用標籤的詳細AWS 資訊 AWS，請參閱 AWS 一般參考.

8. 當您準備好建立新整合時，請選擇 Add integration (新增整合)。沒有評論頁面。 CloudTrail 建立整合，但若要整合您的自訂事件，您必須在PutAuditEvents請求中指定通道 ARN。

9. 呼叫 PutAuditEvents API 以擷取您的活動事件 CloudTrail。每個 PutAuditEvents 請求最多可供新增 100 個活動事件 (或最多 1 MB 大小)。您需要在先前步驟中建立的通道 ARN、要 CloudTrail 新增的事件承載，以及外部 ID (如果為您的資源策略指定)。請確定事件裝載中沒有任何敏感或個人識別資訊，然後再將其導入。 CloudTrail您內CloudTrail 湖集成事件架構嵌的事件 CloudTrail 必須遵循.

> **Tip**
>
> 用AWS CloudShell來確保您執行的是最新的 AWS API。

下列範例顯示如何使用 put-audit-events CLI 命令。--audit-events 和 --channel-arn 是必要參數。您需要在先前步驟中建立的通道 ARN (可以從整合詳細資訊頁面複製)。的值--audit-events是事件物件的 JSON 陣列。 --audit-events包含來自事件的必要 ID、事件的必要裝載作為的值EventData，以及可在擷取到之後協助驗證事件完整性的選用總和檢查碼。 CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
```

```
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

以下是包含兩個事件範例的範例命令。

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

下列範例命令會新增 `--cli-input-json` 參數，以指定事件承載的 JSON 檔案 (`custom-events.json`)。

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

以下是範例 JSON 檔案 `custom-events.json` 的範例內容。

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
```

```
        "id": "1"
      }
   ]
}
```

(選用) 計算總和檢查碼值

您EventDataChecksum在PutAuditEvents要求中指定為值的總和檢查碼，可協助您驗證是否 CloudTrail 接收到符合總和檢查碼的事件；它有助於驗證事件的完整性。總和檢查碼值是您執行下列命令來計算的 base64-SHA256 演算法。

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

命令會傳回總和檢查碼。以下是範例。

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

總和檢查碼值會成為 PutAuditEvents 請求中的 EventDataChecksum 值。如果總和檢查碼與所提供事件的總和檢查碼不相符，則會 CloudTrail 拒絕該事件並顯示錯誤InvalidChecksum。

建立、更新和管理 CloudTrail 湖泊整合 AWS CLI

您可以使用 AWS CLI 建立、更新和管理 L CloudTrail ake 整合。使用時 AWS CLI，請記住您的命令會在為您的設定檔所 AWS 區域 設定的中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

CloudTrail 湖泊整合的可用命令

在 CloudTrail Lake 中建立、更新和管理整合的指令包括：

- create-event-data-store，以建立外部事件的事件資料存放區 AWS。
- delete-channel以刪除用於整合的頻道。
- delete-resource-policy以刪除附加至 CloudTrail Lake 整合之通道的資源策略。
- get-channel以傳回有關 CloudTrail 頻道的資訊。
- get-resource-policy以擷取附加至 CloudTrail 通道的資源型政策文件的 JSON 文字。
- list-channels以列出目前帳戶中的頻道及其來源名稱。
- put-audit-events將您的應用程式事件擷取到 CloudTrail Lake。必要 CloudTrail 參數會接受您要擷取之事件的 JSON 記錄 (也稱為裝載)。auditEvents每個PutAuditEvents請求最多可以新增 100 個這些事件 (或最多 1 MB)。
- put-resource-policy，將以資源為基礎的權限原則附加至用於與外部事件來源整合的 CloudTrail AWS通道。如需以資源為基礎的原則的詳細資訊，請參閱以資AWS CloudTrail 源為基礎的政策
- update-channel更新由所需的通道 ARN 或 UUID 指定的信道。

若要取得 CloudTrail Lake 事件資料倉庫的可用指令清單，請參閱〈〉事件資料倉庫的可用指令。

如需 CloudTrail Lake 查詢的可用指令清單，請參閱〈〉 CloudTrail 湖泊查詢的可用指令。

建立整合以記錄外部 AWS 的事件 AWS CLI

在中 AWS CLI，您可以使用四個命令建立從外部記錄事件 AWS 的整合 (如果您已經有符合準則的事件資料存放區，則為三個命令)。您用作整合目的地的事件資料存放區必須適用於單一區域和單一帳戶；它們不能是多地區，也無法記錄中組織的事件 AWS Organizations，而且只能包含活動事件。主控台中的事件類型必須是 Events from integrations (來自整合的事件)。在 API 中，eventCategory 值必須是 ActivityAuditLog。如需有關整合的詳細資訊，請參閱建立與事件來源以外的整合 AWS。

1. 如果您還沒有可用於整合的一或多個事件資料存放區，請執行 create-event-data-store 以建立事件資料存放區。

   下列範例 AWS CLI 命令會建立從外部記錄事件的事件資料存放區 AWS。對於活動事件，eventCategory 欄位選取器值為 ActivityAuditLog。事件資料存放區的保留期間設定為 90 天。依預設，事件資料存放區會收集來自所有區域的事件，但由於這是收集非AWS 事件，所以請新增--no-multi-region-enabled選項將其設定為單一「區域」。依預設會啟用終止保護，且事件資料存放區不會針對組織中的帳戶收集事件。

   ```
   aws cloudtrail create-event-data-store \
   --name my-event-data-store \
   ```

```
--no-multi-region-enabled \
--retention-period 90 \
--advanced-event-selectors '[
    {
      "Name": "Select all external events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
             ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

您需要事件資料存放區 ID (ARN 的字尾或前面回應範例中的 EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE)，才能繼續進行下一個步驟並建立通道。

2. 執行命create-channel令以建立允許合作夥伴或來源應用程式將事件傳送至中的事件資料存放區的通道 CloudTrail。

   通道具有下列元件：

   來源

   CloudTrail 使用此資訊來判斷代表您傳送事件資料給 CloudTrail 的合作夥伴。來源是必要元件，可以是 Custom (針對所有有效的非AWS 事件)，或合作夥伴事件來源的名稱。每個來源最多可有一個通道。

   如需可用合作夥伴的 Source 值的相關資訊，請參閱整合合作夥伴的其他資訊。

   擷取狀態

   通道狀態會顯示從通道來源接收到最後一個事件的時間。

   目的地

   目的地是從頻道接收事件的 CloudTrail Lake 事件資料存放區。您可以變更通道的目的地事件資料存放區。

   若要停止從來源接收事件，請刪除通道。

   您需要至少一個目的地事件資料存放區的 ID，才能執行此命令。目的地的有效類型為 EVENT_DATA_STORE。您可以將擷取的事件傳送至多個事件資料存放區。下列範例命令所建立的通道會將事件傳送至兩個事件資料存放區，以它們在 --destinations 參數的 Location 屬性中的 ID 表示。--destinations、--name 和 --source 是必要參數。若要擷取來自 CloudTrail 夥伴的事件，請將夥伴的名稱指定為的--source值。若要從外部您自己的應用程式內嵌事件 AWS，請指定Custom為的--source值。

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

   在 create-channel 命令的回應中，複製新通道的 ARN。您需要 ARN 才能在後續步驟中執行 put-resource-policy 和 put-audit-events 命令。

3. 執行命put-resource-policy令，將資源策略附加至通道。資源政策是 JSON 政策文件，這些文件會指出指定的主體可對資源執行哪些動作以及相關條件。在通道的資源政策中定義為主體的帳戶可以呼叫 `PutAuditEvents` API 以傳送事件。

> **Note**
>
> 如果您沒有為通道建立資源政策，則只有通道擁有者可以在通道上呼叫 `PutAuditEvents` API。

政策所需的資訊取決於整合類型。

- 若要進行方向整合， CloudTrail 需要政策包含合作夥伴的 AWS 帳號 ID，並要求您輸入合作夥伴提供的唯一外部 ID。 CloudTrail 當您使用 CloudTrail 主控台建立整合時，會自動將合作夥伴的 AWS 帳號 ID 新增至資源策略。請參閱合作夥伴的說明文件，以瞭解如何取得政策所需的 AWS 帳號。
- 對於解決方案整合，您必須至少指定一個 AWS 帳戶 ID 作為主體，並且可以選擇性地輸入外部 ID 以防止混淆的副手。

資源政策的需求如下：

- 政策中定義的資源 ARN 必須與政策所連接的通道 ARN 相符。
- 此原則僅包含一個動作：雲路資料：PutAuditEvents
- 政策至少包含一個陳述式。政策最多可以有 20 個陳述式。
- 每個陳述式至少包含一個主體。陳述式最多可以有 50 個主體。

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
```

```
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

如需資源政策的詳細資訊，請參閱AWS CloudTrail 資源型政策範例。

4. 執行 PutAuditEventsAPI 以擷取您的活動事件 CloudTrail。您將需要要新增之事件的裝載。CloudTrail 請確定事件裝載中沒有任何敏感或個人識別資訊，然後再將其導入。 CloudTrail請注意，PutAuditEvents API 使用 cloudtrail-data CLI 端點，而不是 cloudtrail 端點。

   下列範例顯示如何使用 put-audit-events CLI 命令。--audit-events 和 --channel-arn 是必要參數。如果在資源政策中定義了外部 ID，則需要 --external-id 參數。您需要在前一步驟中建立的通道 ARN。的值--audit-events是事件物件的 JSON 陣列。 --audit-events包含來自事件的必要 ID、事件的必要裝載作為的值EventData，以及可在擷取到之後協助驗證事件完整性的選用總和檢查碼。 CloudTrail

```
aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

   以下是包含兩個事件範例的範例命令。

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

下列範例命令會新增 `--cli-input-json` 參數，以指定事件承載的 JSON 檔案 (`custom-events.json`)。

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

以下是範例 JSON 檔案 `custom-events.json` 的範例內容。

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

您可以執行get-channel命令，確認整合是否正常運作，以及 CloudTrail 是否正確地從來源擷取事件。的輸出get-channel會顯示最近 CloudTrail接收到事件的時間戳記。

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(選用) 計算總和檢查碼值

您EventDataChecksum在PutAuditEvents要求中指定為值的總和檢查碼，可協助您驗證是否 CloudTrail 接收到符合總和檢查碼的事件；它有助於驗證事件的完整性。總和檢查碼值是您執行下列命令來計算的 base64-SHA256 演算法。

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

命令會傳回總和檢查碼。以下是範例。

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

總和檢查碼值會成為 PutAuditEvents 請求中的 EventDataChecksum 值。如果總和檢查碼與所提供事件的總和檢查碼不相符，則會 CloudTrail 拒絕該事件並顯示錯誤InvalidChecksum。

更新頻道 AWS CLI

若要更新通道的名稱或目的地事件資料存放區，請執行 update-channel 指令。--channel 參數是必要參數。您無法更新通道的來源。以下是範例。

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
```

```
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

刪除頻道以刪除與 AWS CLI

若要停止在外部擷取合作夥伴或其他活動事件 AWS，請執行delete-channel命令以刪除頻道。您要刪除的通道的 ARN 或通道 ID (ARN 字尾) 是必要項目。以下是範例。

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

整合合作夥伴的其他資訊

本節中的表格提供每個整合合作夥伴的來源名稱，並識別整合類型 (直接或解決方案)。

呼叫 `CreateChannel` API 時需要來源名稱一欄中的資訊。您會將來源名稱指定為 `Source` 參數的值。

合作夥伴名稱 (主控台)	來源名稱 (API)	整合類型
My custom integration	`Custom`	解決方案
Cloud Storage Security	`CloudStorageSecurityConsole`	解決方案
Clumio	`Clumio`	直接
CrowdStrike	`CrowdStrike`	解決方案
CyberArk	`CyberArk`	解決方案
GitHub	`GitHub`	解決方案
Kong Inc	`KongGatewayEnterprise`	解決方案
LaunchDarkly	`LaunchDarkly`	直接

合作夥伴名稱 (主控台)	來源名稱 (API)	整合類型
Netskope	NetskopeCloudExchange	解決方案
Nordcloud, an IBM Company	IBMMulticloud	直接
MontyCloud	MontyCloud	直接
Okta	OktaSystemLogEvents	解決方案
One Identity	OneLogin	解決方案
Shoreline.io	Shoreline	解決方案
Snyk.io	Snyk	直接
Wiz	WizAuditLogs	解決方案

檢視合作夥伴文件

您可以檢視合作夥伴的文件，進一步了解合作夥伴與 CloudTrail Lake 的整合。

若要檢視合作夥伴文件

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的整合。
3. 在 Integrations (整合) 頁面中，選擇 Available sources (可用來源)，然後針對您要檢視文件的合作夥伴選擇 Learn more (進一步了解)。

CloudTrail 湖集成事件架構

下表說明與 CloudTrail 事件記錄中的結構描述元素相符的必要和選擇性結構描述元素。的內容由您`eventData`的事件提供；其他欄位則由擷取 CloudTrail 後提供。

CloudTrail 事件記錄內容在中有更詳細的說明CloudTrail 記錄內容。

- 擷取 CloudTrail 後提供的欄位

- 您的事件提供的欄位

擷取 CloudTrail 後提供的欄位

欄位名稱	輸入類型	需求	描述
eventVersion	string	必要	事件版本。
eventCategory	string	必要	事件類別。對於非AWS 事件，值為ActivityAuditLog 。
eventType	string	必要	事件類型。對於非 AWS 事件，有效值為ActivityLog 。
eventID	string	必要	事件的唯一 ID。
eventTime	string	必要	事件時間戳記，採用 yyyy-MM-DDTHH:mm:ss 格式和國際標準時間 (UTC)。
awsRegion	string	必要	PutAuditEvents 打電話的 AWS 區域 地方。
recipientAccountId	string	必要	表示收到此事件的帳戶 ID。 CloudTrail 透過從事件裝載計算此欄位來填入此欄位。
附錄	-	選用	顯示事件處理延遲原因的相關資訊。如果現有事件中缺少資訊，則附錄區塊會包含

欄位名稱	輸入類型	需求	描述
			缺少的資訊，以及缺失的原因。
• reason	string	選用	事件或其部分內容遺失的原因。
• updatedFields	string	選用	附錄所更新的事件記錄欄位。只有當原因是 UPDATED_DATA 才提供此資訊。
• originalUID	string	選用	來自來源的原始事件 UID。只有當原因是 UPDATED_DATA 才提供此資訊。
• originalEventID	string	選用	原始事件 ID。只有當原因是 UPDATED_DATA 才提供此資訊。
中繼資料	-	必要	事件所使用通道的相關資訊。
• ingestionTime	string	必要	處理事件時的時間戳記，採用 yyyy-MM-DDTHH:mm:ss 格式和國際標準時間 (UTC)。
• channelARN	string	必要	事件所使用通道的 ARN。

客戶事件提供的欄位

欄位名稱	輸入類型	需求	描述
eventData	-	必要	PutAuditEvents 通話中傳送至 CloudTrail 的稽核資料。
• version	string	必要	來自來源的事件版本。 長度限制：長度上限為 256。
• userIdentity	-	必要	提出請求之使用者的相關資訊。
• • type	string	必要	使用者身分類型。 長度限制：長度上限為 128。
• • principalId	string	必要	事件執行者的唯一識別碼。 長度限制：長度上限為 1024。
• • 詳細資訊	JSON 物件	選用	身分識別的其他相關資訊。
• userAgent	string	選用	提出請求的代理程式。 長度限制：長度上限為 1024。
• eventSource	string	必要	這是合作夥伴事件來源，或記錄事件的自訂應用程式。

欄位名稱	輸入類型	需求	描述
			長度限制：長度上限為 1024。
• eventName	string	必要	請求的動作，來源服務或應用程式的 API 中的動作之一。 長度限制：長度上限為 1024。
• eventTime	string	必要	事件時間戳記，採用 `yyyy-MM-DDTHH:mm:ss` 格式和國際標準時間 (UTC)。
• UID	string	必要	識別請求的 UID 值。呼叫的服務或應用程式會產生此值。 長度限制：長度上限為 1024。
• requestParameters	JSON 物件	選用	請求時所傳送的參數 (如果有的話)。此欄位的大小上限為 100 KB，超過該限制的內容會被拒絕。
• responseElements	JSON 物件	選用	進行變更之動作 (建立、更新或刪除動作) 的回應元素。此欄位的大小上限為 100 KB，超過該限制的內容會被拒絕。

欄位名稱	輸入類型	需求	描述
• errorCode	string	選用	代表事件錯誤的字串。 長度限制：長度上限為 256。
• errorMessage	string	選用	錯誤的描述。 長度限制：長度上限為 256。
• sourceIPAddress	string	選用	提出請求的 IP 地址。接受 IPv4 和 IPv6 地址。
• recipientAccountId	string	必要	代表收到此事件的帳戶 ID。帳號 ID 必須與擁有該頻道的 AWS 帳號 ID 相同。
• additionalEventData	JSON 物件	選用	不屬於請求或回應之事件的額外資料。此欄位的大小上限為 28 KB，超過該限制的內容會被拒絕。

下列範例顯示符合 CloudTrail 事件記錄中結構描述元素的階層架構。

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
```

```
        "reason": String,
        "updatedFields": String,
        "originalUID": String,
        "originalEventID": String
    },
    "metadata" : {
        "ingestionTime": String,
        "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
             JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

檢視 CloudTrail 湖泊儀表板

您可以使用 CloudTrail Lake 儀表板來視覺化事件資料存放區中的事件。您可以在多種不同的儀表板類型中選取。可用於事件資料存放區的儀表板類型取決於該事件資料存放區的進階事件選取器組態。例

如，如果儀表板類型顯示有關 CloudTrail 管理事件的資訊，則只有當目前選取的事件資料存放區收集 CloudTrail 管理事件時，您才能選取儀表板。

每種儀表板類型均包含多個小工具，每個小工具代表一個 SQL 查詢。若要檢視某個小工具的查詢，請選擇在查詢編輯器中檢視並分析以開啟查詢編輯器。您不能修改由系統產生的用於填入小工具的查詢，但您可以在查詢編輯器中編輯並執行查詢，以便做進一步分析。

如需填入並更新儀表板，請選擇執行查詢。當您選擇 [執行查詢] 時， CloudTrail 會代表您執行系統產生的查詢。由於執行查詢會產生成本，所以會 CloudTrail 要求您確認與執行查詢相關的成本。您只需確認一次。如需有關 CloudTrail 定價的詳細資訊，請參閱CloudTrail 定價。

主題

限制

下列限制適用於目前版本。

- 目前的版本不支援自訂儀表板、小工具或查詢。
- 目前版本僅為收集 CloudTrail 事件 (資料事件、管理事件) 和 Insights 事件的事件資料存放區提供儀表板。
- 目前的版本不支援編輯由系統產生，用於填入儀表板的查詢。您可以在查詢編輯器索引標籤上檢視與編輯任何小工具的基礎查詢，但對查詢的任何變更都要以在儀表板外執行補充分析為目的。

必要條件

下列先決條件適用於 Lake 儀表板。

- 若要檢視和使用 Lake 儀表板，您必須至少建立一個 CloudTrail Lake 事件資料存放區。您可以使用主控台或 SDK 建立事件資料存放區。 AWS CLI如需有關使用主控台建立事件資料存放區的資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區。若要取得有關使用建立事件資料倉庫的資訊 AWS CLI，請參閱建立、更新和管理事件資料存放區 AWS CLI。

- 若要填入儀表板，請代表您 CloudTrail 執行查詢。第一次檢視「儀表板」頁面時， CloudTrail 會要求您確認與執行查詢相關的成本。選擇我同意以確認執行查詢的相關費用。

選擇一個儀表板

使用下列程序來選擇要檢視的事件資料存放區和儀表板類型。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇您想要視覺化呈現哪個事件資料存放區的資料。
4. 選擇您想要檢視的儀表板類型。儀表板清單根據所選事件資料存放區的進階事件選取器組態填入。

   下列是可能的儀表板類型。

   - 概觀控制面板-顯示最活躍的使用者 AWS 區域，以及 AWS 服務 按事件計數。您還可以檢視有關 `read` 和 `write` 管理事件活動、最常調節事件和常見錯誤的資訊。此儀表板適用於收集管理事件的事件資料存放區。
   - 管理事件儀表板 - 依使用者顯示主控台登入事件、存取遭拒事件、破壞性動作和常見錯誤。您還可以檢視有關 TLS 版本以及使用者的過期 TLS 呼叫的資訊。此儀表板適用於收集管理事件的事件資料存放區。
   - S3 資料事件儀表板 - 顯示 S3 帳戶活動、最常存取的 S3 物件、最常用的 S3 使用者和最常執行的 S3 動作。此儀表板適用於收集 Amazon S3 資料事件的事件資料存放區。
   - Insights 事件儀表板 - 依 Insights 類型顯示 Insights 事件的總體比例，依最常使用的使用者和服務的 Insights 類型顯示 Insights 事件的比例，以及顯示每天的 Insights 事件數量。此儀表板還包含一個小工具，可列出最多 30 天的 Insights 事件。它僅適用於收集 Insights 事件的事件資料存放區。

   > **Note**
   >
   > - 在來源事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能傳遞第一個 Insights 事件。如需詳細資訊，請參閱 了解 Insights 事件傳遞。
   > - Insights 事件儀表板僅顯示由所選事件資料存放區收集的 Insights 事件的相關資訊，這取決於來源事件資料存放區的組態。例如，如果您設定來源事件資料存放區啟用 `ApiCallRateInsight` 的 Insights 事件，而不啟用 `ApiErrorRateInsight` 的

Insights 事件，您將不會看到有關 `ApiErrorRateInsight` 的 Insights 事件的資訊。

5. 選擇按絕對範圍或相對範圍篩選儀表板資料。選擇絕對範圍以選取特定的日期和時間範圍。選擇相對範圍以選取預先定義的時間範圍或自訂範圍。依預設，儀表板會顯示過去 24 小時的事件資料。

> **Note**
>
> CloudTrail Lake 查詢會根據掃描的資料量產生費用。為協助您控制成本，您可以在較窄時間範圍內篩選。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

6. 選擇執行查詢，對儀表板的小工具執行查詢。

按日期或時間範圍篩選儀表板

依預設，儀表板會顯示過去 24 小時的資料。您可以按絕對範圍或相對範圍篩選儀表板。

選擇絕對範圍以選取特定的日期和時間範圍。

選擇相對範圍以選取預先定義的時間範圍或自訂範圍。

在選擇時間範圍後，選擇執行查詢以重新整理儀表板。

> **Note**
>
> CloudTrail Lake 查詢會根據掃描的資料量產生費用。為協助您控制成本，您可以在較窄時間範圍內篩選。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

檢視儀表板小工具的查詢

每個小工具都代表一個 SQL 查詢。若要檢視某個小工具的查詢，請選擇在查詢編輯器中檢視並分析以開啟查詢編輯器。使用查詢編輯器，您可以進一步細化儀表板外的查詢，並執行查詢以查看更新後查詢的結果。如需使用查詢的詳細資訊，請參閱 建立或編輯查詢。

> **Note**
>
> 您不能修改由系統產生的儀表板小工具查詢。在查詢編輯器索引標籤上對查詢的任何變更，都僅以在儀表板外執行進一步分析為目的。

CloudTrail 湖泊查詢

CloudTrail 湖泊中的查詢是使用 SQL 編寫的。您可以從頭開始以 SQL 撰寫查詢，或開啟已儲存或範例查詢並進行編輯，在 CloudTrail Lake Editor 索引標籤上建立查詢。您不能用變更覆寫包含的範例查詢，但可以將範例查詢另存為新查詢。如需允許的 SQL 查詢語言有關的詳細資訊，請參閱CloudTrail 湖泊 SQL 條件約束。

未限制查詢 (例如SELECT * FROM *edsID*) 會掃描事件資料存放區中的所有資料。為了協助控制成本，我們建議您對查詢新增開始和結束 eventTime 時間戳記來限制查詢。以下是在指定的事件資料存放區中搜尋所有事件的範例，其中的事件時間為 (>) 2023 年 1 月 5 日下午 1:51 之後，以及 (<) 2023 年 1 月 19 日下午 1:51 之前。由於事件資料存放區的最小保留期間為七天，因此開始和結束 eventTime 值之間的最小時間範圍也是七天。

```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

主題

- 查詢編輯器工具
- 在 CloudTrail 主控台中檢視範例查詢
- 建立或編輯查詢
- 執行查詢並儲存查詢結果
- 檢視查詢結果
- 下載已儲存的查詢結果
- 驗證已儲存查詢結果
- CloudTrail 使用 AWS CLI

查詢編輯器工具

查詢編輯器右上角的工具列提供命令，可協助撰寫 SQL 查詢並設置其格式。

下列清單說明工具列的命令。

- Undo (復原) – 還原在查詢編輯器中進行的最後一次內容變更。
- Redo (重做) – 重複在查詢編輯器中進行的最後一次內容變更。
- Format selected (所選格式) – 根據 SQL 格式和間距慣例排列查詢編輯器內容。
- 註解/取消選取部分的註解 - 若選取的查詢部分還沒有註解，則為其加上註解。如果選取部分已有註解，選擇此選項將移除註解。

在 CloudTrail 主控台中檢視範例查詢

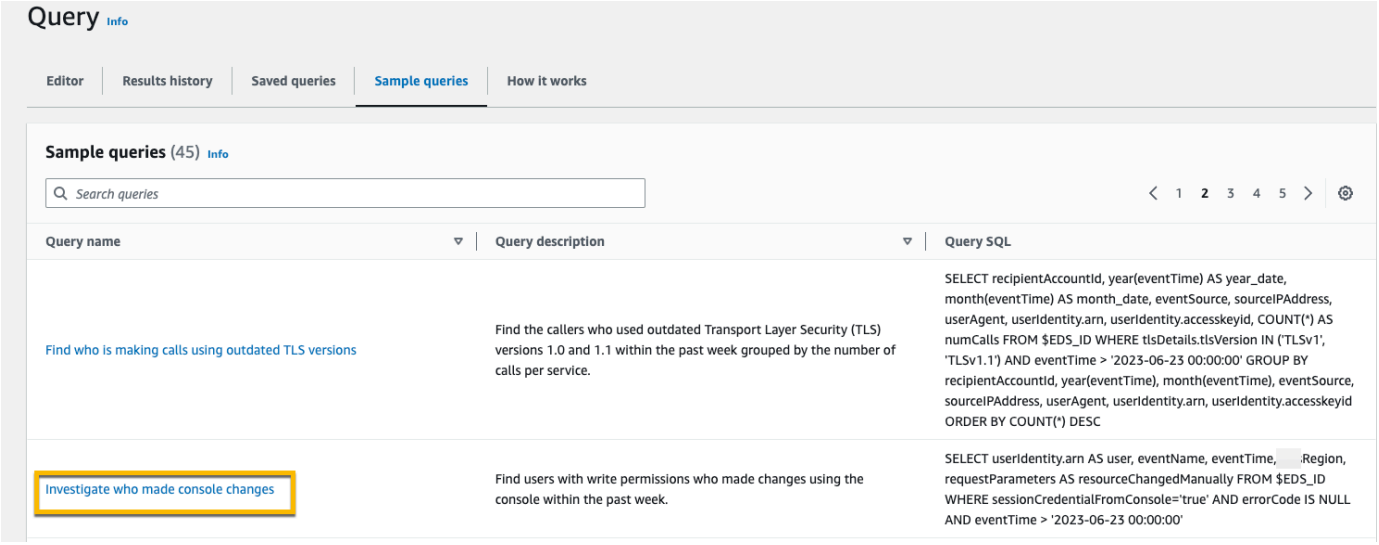
主 CloudTrail 控台提供許多範例查詢，可協助您開始撰寫自己的查詢。

CloudTrail 查詢會根據掃描的資料量產生費用。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

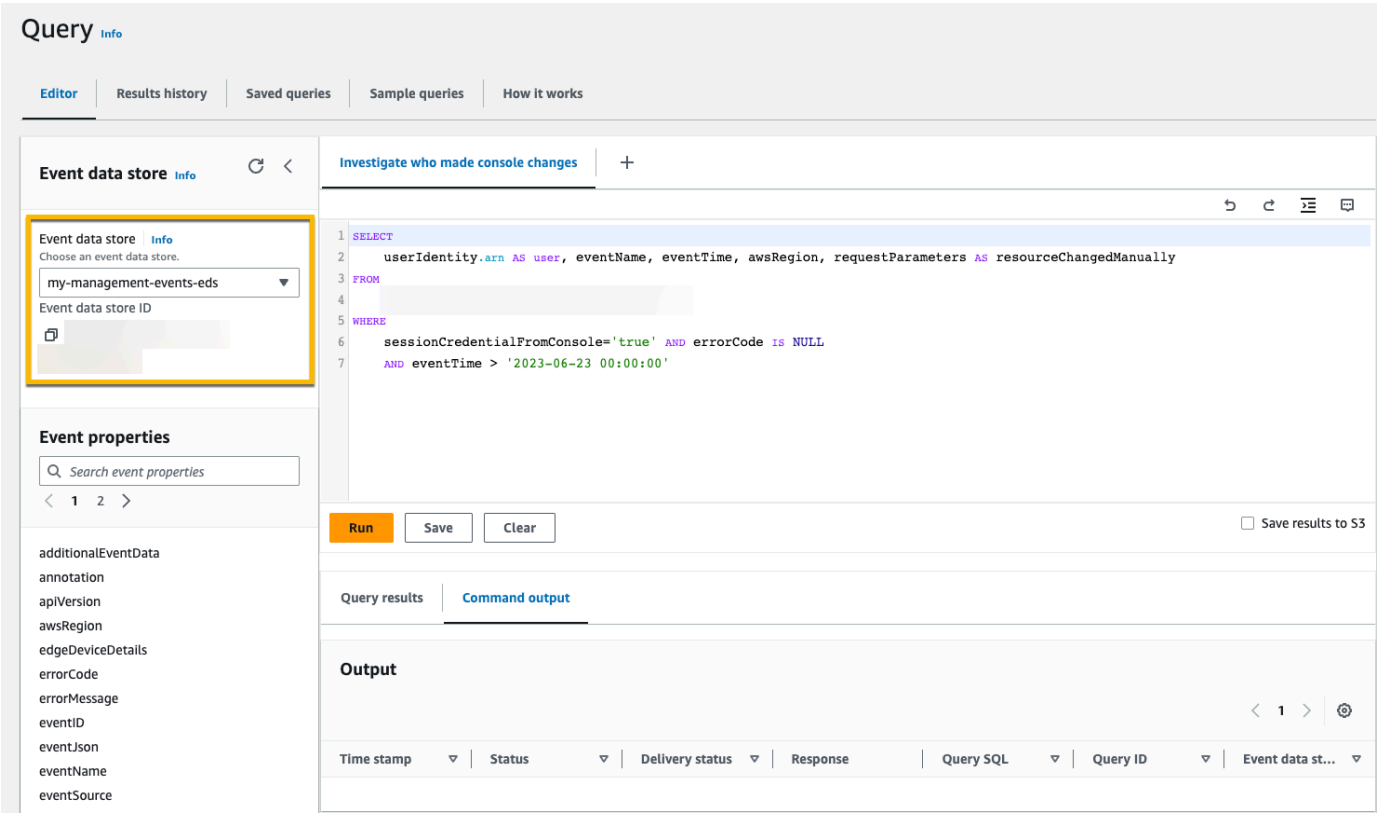
> **Note**
>
> 您也可以檢視 GitHub 社群建立的查詢。如需詳細資訊並檢視這些範例查詢，請參閱 GitHub 網站上的 CloudTrailLake 範例查詢。 AWS CloudTrail 尚未評估中的查詢 GitHub。

若要檢視與執行範例查詢

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在 Query (查詢) 頁面上，選擇 Sample queries (範例查詢) 索引標籤。
4. 在清單中選擇一個範例查詢，或者搜尋查詢以篩選清單。在此範例中，我們將透過選擇查詢名稱打開查詢調查誰變更了主控台。這會在 Editor (編輯器) 索引標籤中開啟查詢。

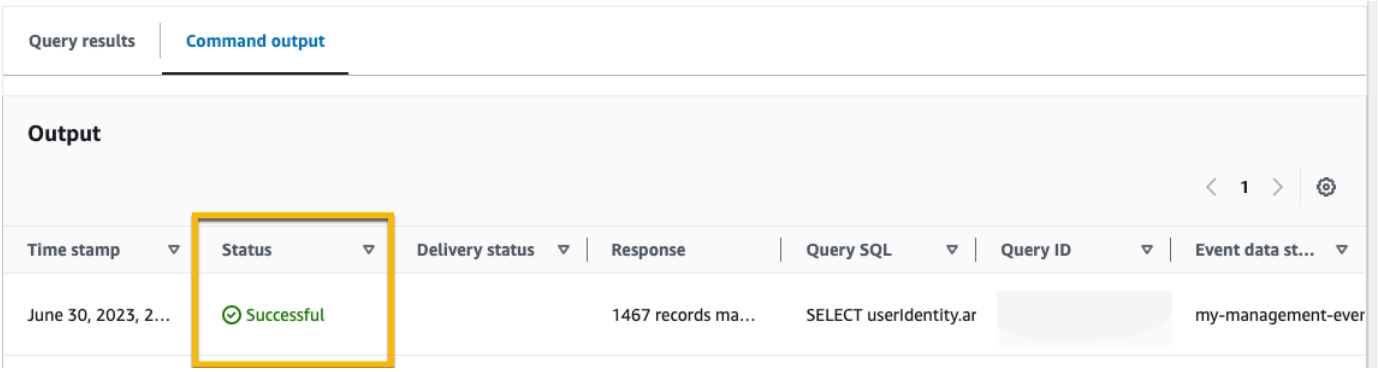


5. 在編輯器索引標籤上，選擇您想要為哪個事件資料存放區執行查詢。當您從清單中選擇事件資料倉庫時， CloudTrail 會自動將事件資料存放區 ID 填入查詢編輯器的FROM行中。

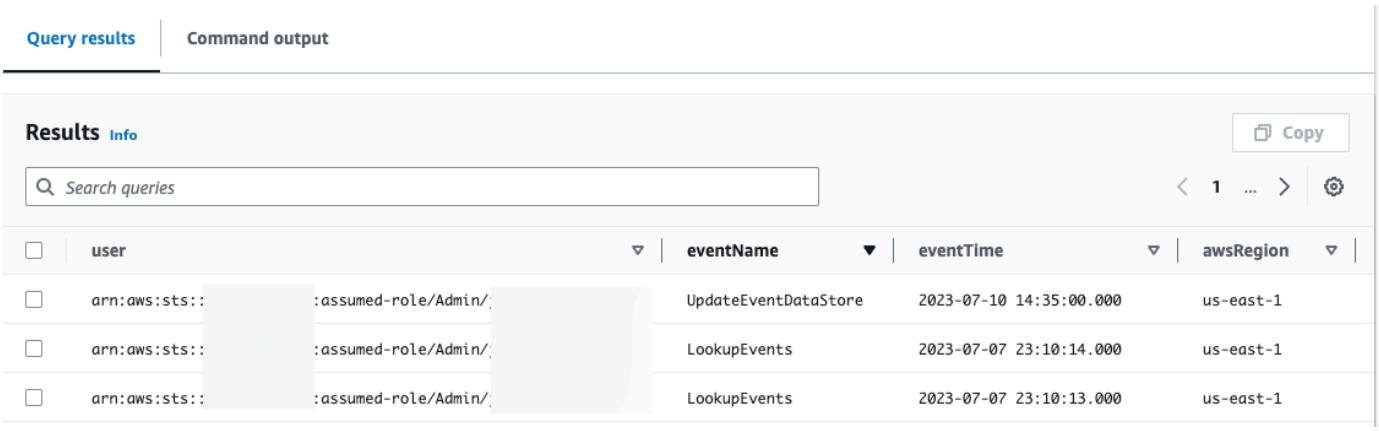


6. 選擇執行以執行查詢。

命令輸出索引標籤顯示您的查詢的相關中繼資料，例如查詢是否成功，相符的記錄數目，以及查詢的執行事件。



查詢結果索引標籤顯示所選事件資料存放區中與您的查詢相符的事件資料。



如需有關編輯查詢的詳細資訊，請參閱 建立或編輯查詢。如需有關執行查詢和儲存查詢結果的詳細資訊，請參閱 執行查詢並儲存查詢結果。

建立或編輯查詢

在這次逐步解說中，我們會打開其中一個範例查詢，進行編輯以查找名為 `Alice` 的特定使用者所做的動作，然後將其儲存為新查詢。您也可以在 Saved queries (已儲存的查詢) 索引標籤編輯已儲存的查詢 (如果有已儲存的查詢)。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在 Query (查詢) 頁面上，選擇 Sample queries (範例查詢) 索引標籤。

4. 選擇查詢名稱以打開範例查詢。這會在 Editor (編輯器) 索引標籤中開啟查詢。在此範例中，我們將選取名為調查使用者動作的查詢，然後編輯該查詢以查找名為 `Alice` 的特定使用者所做的動作。

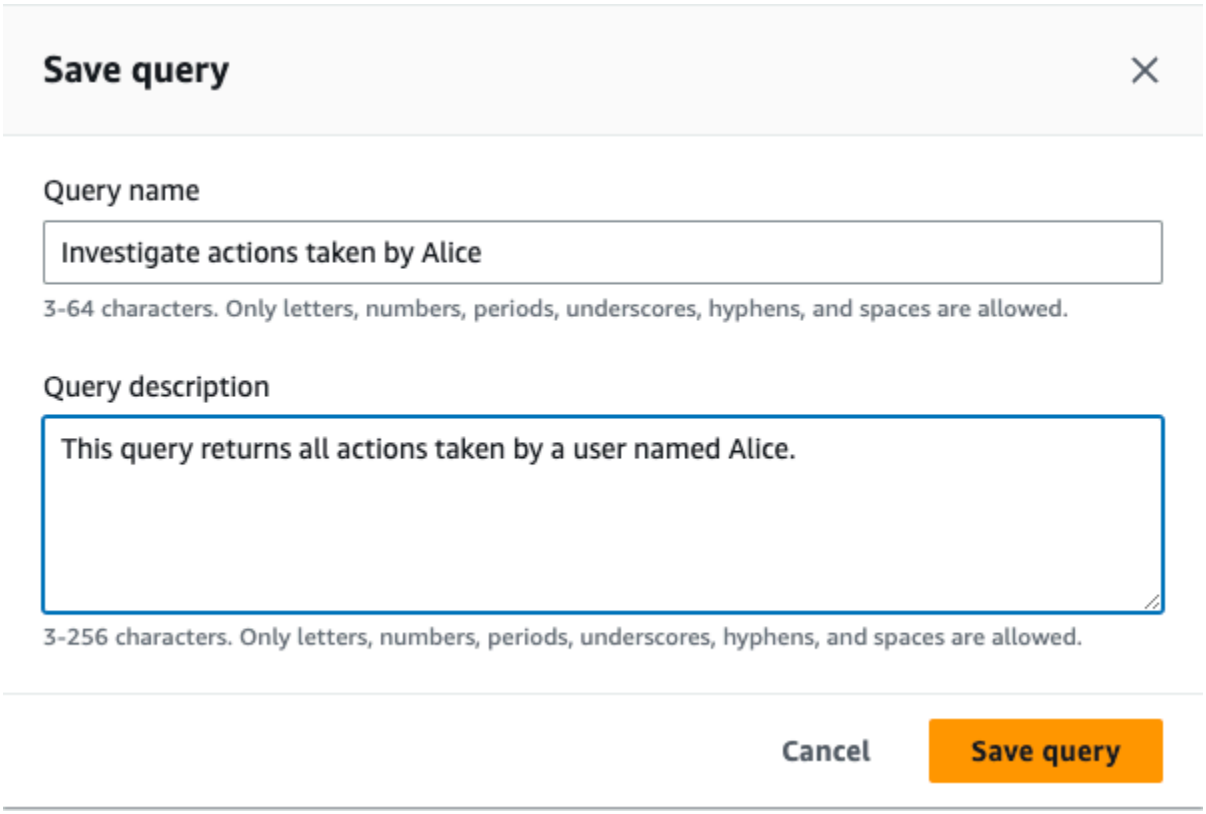
5. 在編輯器索引標籤中，編輯 `WHERE` 列以指定您想要調查的使用者，並視需要更新 `eventTime` 值。的值`FROM`是事件資料倉庫 ARN 的 ID 部分， CloudTrail 當您選擇事件資料倉庫時，會自動填入。

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. 您可以在儲存查詢之前執行查詢，以驗證查詢是否正常運作。若執行查詢，請從Event data store (事件資料存放區) 下拉式清單中選擇事件資料存放區，然後選擇 Run (執行)。檢視 Command output (命令輸出) 索引標籤的 Status (狀態) 欄，以驗證查詢是否成功執行。

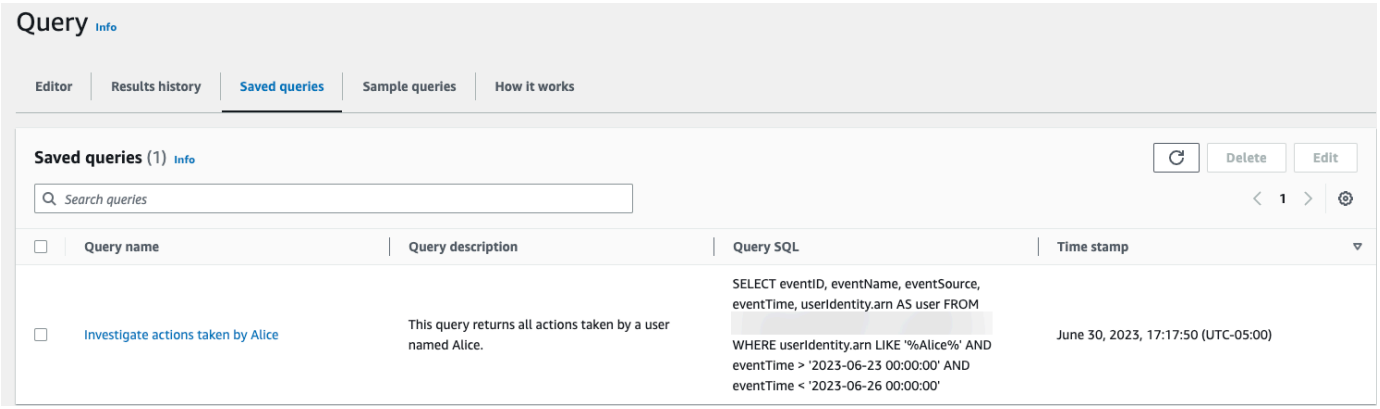
7. 如果您已更新範例查詢，請選擇儲存。

8. 在儲存查詢中，輸入查詢的名稱和描述。選擇 Save query (儲存查詢) 將變更另存為新查詢。若要放棄對查詢的變更，請選擇 Cancel (取消)，或關閉 Save query (儲存查詢) 視窗。



> **Note**
>
> 儲存的查詢會繫結至您的瀏覽器；如果您使用其他瀏覽器或其他裝置存取 CloudTrail 主控台，則無法使用儲存的查詢。

9. 開啟 Saved queries(已儲存的查詢) 索引標籤以查看表格中的新查詢。



執行查詢並儲存查詢結果

選擇或儲存查詢後，您就可以對事件資料存放區執行查詢。

執行查詢時，您可以選擇將查詢結果儲存到 Amazon S3 儲存貯體。在 CloudTrail Lake 中執行查詢時，會根據查詢掃描的資料量產生費用。將查詢結果儲存到 S3 儲存貯體不會產生額外的 CloudTrail Lake 費用，不過需支付 S3 儲存費用。如需 S3 定價的詳細資訊，請參閱 Amazon S3 定價。

儲存查詢結果時，查詢結果可能會在 S3 儲存貯體中檢視之前顯示在 CloudTrail 主控台中，因為查詢掃描完成後會 CloudTrail 傳送查詢結果。雖然大多數查詢會在幾分鐘內完成，但視事件資料存放區的大小而定，將查詢結果傳遞 CloudTrail 到 S3 儲存貯體可能需要相當長的時間。 CloudTrail 以壓縮的 gzip 格式將查詢結果傳送至 S3 儲存貯體。平均而言，查詢掃描完成後，每傳遞 1 GB 的資料到 S3 儲存貯體，可能會有 60 到 90 秒的延遲。

使用 CloudTrail 湖泊執行查詢的步驟

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在已儲存的查詢或範例查詢索引標籤上，選擇查詢名稱以選擇要執行的查詢。
4. 在 Editor (編輯器) 索引標籤，針對 Event data store (事件資料存放區)，從下拉式清單中選擇事件資料存放區。
5. (選擇性) 在 Editor (編輯器) 索引標籤，選擇 Save results to S3 (將結果儲存至 S3)，將查詢結果儲存至 S3 儲存貯體。當您選擇預設 S3 儲存貯體時， CloudTrail 會建立並套用所需的儲存貯體政策。如果您選擇預設 S3 儲存貯體，您的 IAM 政策需要包含`s3:PutEncryptionConfiguration`動作的權限，因為預設情況下會為儲存貯體啟用伺服器端加密。如需有關儲存查詢結果的詳細資訊，請參閱已儲存查詢結果的其他相關資訊。

   > **Note**
   >
   > 若要使用不同的儲存貯體，請指定儲存貯體名稱，或選擇 Browse S3 (瀏覽 S3) 以選擇儲存貯體。值區政策必須授 CloudTrail 予將查詢結果傳遞給值區的權限。如需手動編輯儲存貯體政策的資訊，請參閱「 CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策」。

6. 在 Editor (編輯器) 標籤上，選擇 Run (執行)。

   根據事件資料存放區的大小及其中包含的資料天數，查詢可能需要幾分鐘才能執行。所以 Command output (命令輸出) 索引標籤會顯示查詢的狀態，以及查詢是否已完成執行。查詢完成執行後，開啟 Query results (查詢結果) 索引標籤查看作用中查詢 (目前編輯器中顯示的查詢) 的結果表格。

> **Note**
>
> 執行時間超過一小時的查詢可能會逾時。您仍然可以取得在查詢逾時之前處理的部分結果。CloudTrail 不會將部分查詢結果傳遞至 S3 儲存貯體。若要避免逾時，您可以透過指定較短的時間範圍來調整查詢，以限制掃描的資料量。

已儲存查詢結果的其他相關資訊

儲存查詢結果後，您可以從 S3 儲存貯體下載已儲存的查詢結果。如需有關尋找和下載已儲存查詢結果的詳細資訊，請參閱下載已儲存的查詢結果。

您也可以驗證已儲存的查詢結果，以判斷查詢結果在 CloudTrail 傳送查詢結果之後是否已修改、刪除或未變更查詢結果。如需有關驗證已儲存查詢結果的詳細資訊，請參閱驗證已儲存查詢結果。

範例：將查詢結果儲存至 Amazon S3 儲存貯體

本逐步解說說明如何將查詢結果儲存至 S3 儲存貯體，然後下載這些查詢結果。

若要將查詢結果儲存至 Amazon S3 儲存貯體

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在範例查詢或已儲存的查詢索引標籤上，選擇查詢名稱以選擇要執行的查詢。在此範例中，我們將選擇名為調查使用者動作的範例查詢。
4. 在 Editor (編輯器) 索引標籤，針對 Event data store (事件資料存放區)，從下拉式清單中選擇事件資料存放區。當您從清單中選擇事件資料倉庫時， CloudTrail 會自動在該`From`行中填入事件資料倉庫 ID。
5. 在此範例查詢中，我們將編輯 `userIdentity.ARN` 值以指定名為 `Admin` 的使用者，然後我們將保留 `eventTime` 的預設值。執行查詢時，您將為掃描的資料量支付費用。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。

6. 選擇將結果儲存至 S3，以便將查詢結果儲存至 S3 儲存貯體。當您選擇預設 S3 儲存貯體時，CloudTrail 會建立並套用所需的儲存貯體政策。如果您選擇預設 S3 儲存貯體，您的 IAM 政策需要包含`s3:PutEncryptionConfiguration`動作的權限，因為預設情況下會為儲存貯體啟用伺服器端加密。在此範例中，我們使用預設的 S3 儲存貯體。

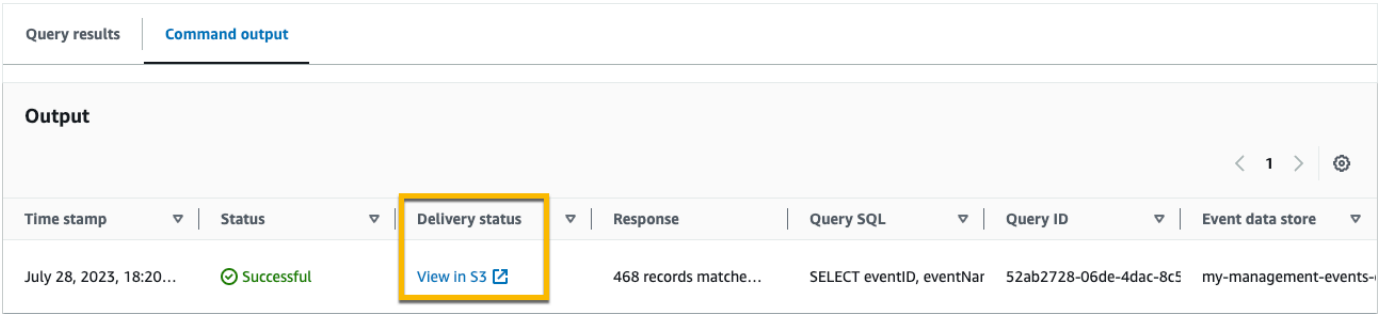
> **Note**
>
> 若要使用不同的儲存貯體，請指定儲存貯體名稱，或選擇 Browse S3 (瀏覽 S3) 以選擇儲存貯體。值區政策必須授 CloudTrail 予將查詢結果傳遞給值區的權限。如需手動編輯儲存貯體政策的資訊，請參閱「CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策」。

7. 選擇執行。根據事件資料存放區的大小及其中包含的資料天數，查詢可能需要幾分鐘才能執行。所以 Command output (命令輸出) 索引標籤會顯示查詢的狀態，以及查詢是否已完成執行。查詢完

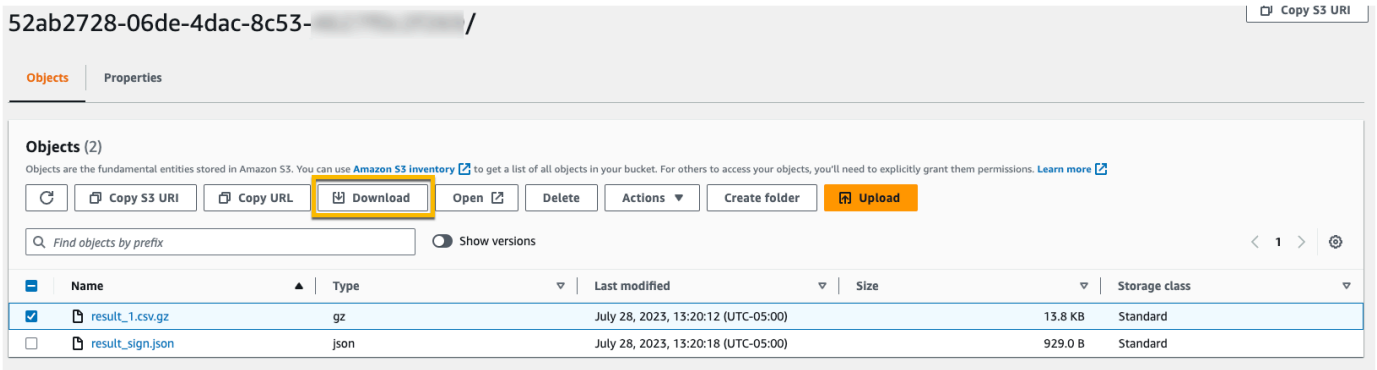
成執行後，開啟 Query results (查詢結果) 索引標籤查看作用中查詢 (目前編輯器中顯示的查詢) 的結果表格。

8. CloudTrail 完成將儲存的查詢結果交付到 S3 儲存貯體時，[交付狀態] 欄會提供 S3 儲存貯體的連結，該儲存貯體包含已儲存的查詢結果檔案，以及可用來驗證已儲存查詢結果的簽署檔案。選擇在 S3 中檢視，在 S3 儲存貯體中檢視查詢結果檔案和簽署檔案。

> **Note**
>
> 當您儲存查詢結果時，查詢結果可能會在 S3 儲存貯體中檢視之前顯示在 CloudTrail 主控台中，因 CloudTrail 為查詢掃描完成後會傳送查詢結果。雖然大多數查詢會在幾分鐘內完成，但視事件資料存放區的大小而定，將查詢結果傳遞 CloudTrail 到 S3 儲存貯體可能需要相當長的時間。 CloudTrail 以壓縮的 gzip 格式將查詢結果傳送至 S3 儲存貯體。平均而言，查詢掃描完成後，每傳遞 1 GB 的資料到 S3 儲存貯體，可能會有 60 到 90 秒的延遲。



9. 若要下載您的查詢結果，選擇查詢結果檔案 (在此範例中為 `result_1.csv.gz`)，然後選擇下載。



如需有關驗證已儲存查詢結果的資訊，請參閱 驗證已儲存查詢結果。

檢視查詢結果

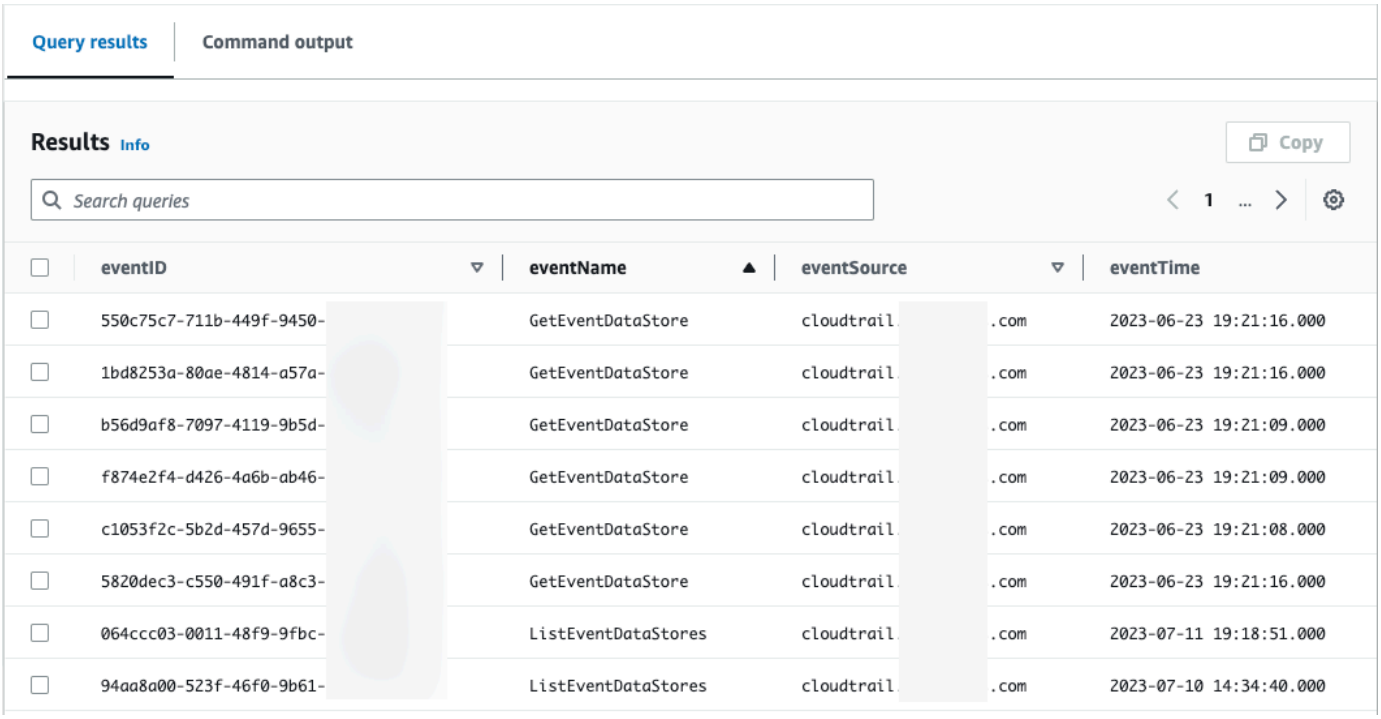
查詢完成後，您就可以查看其結果。查詢完成後，七天內可使用其查詢結果。您可以在 Query results (查詢結果) 索引標籤上查看作用中查詢的結果，也可以在 Lake 首頁的結果歷史記錄標籤上存取所有最近查詢的結果。

查詢結果可以從較早的查詢執行變更為較新的查詢結果，因為查詢期間的後續事件可以在查詢之間記錄。

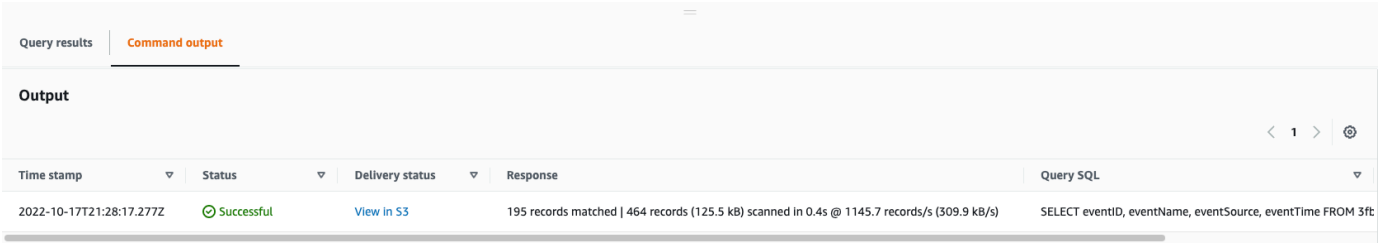
儲存查詢結果時，查詢結果可能會在 S3 儲存貯體中檢視之前顯示在 CloudTrail 主控台中，因為查詢掃描完成後會 CloudTrail 傳送查詢結果。雖然大多數查詢會在幾分鐘內完成，但視事件資料存放區的大小而定，將查詢結果傳遞 CloudTrail 到 S3 儲存貯體可能需要相當長的時間。 CloudTrail 以壓縮的 gzip 格式將查詢結果傳送至 S3 儲存貯體。 平均而言，查詢掃描完成後，每傳送到 S3 儲存貯體的 GB 資料可能會有 60 到 90 秒的延遲。如需有關尋找和下載已儲存查詢結果的詳細資訊，請參閱下載已儲存的查詢結果。

> **Note**
>
> 執行時間超過一小時的查詢可能會逾時。您仍然可以取得在查詢逾時之前處理的部分結果。CloudTrail 不會將部分查詢結果傳遞至 S3 儲存貯體。若要避免逾時，您可以透過指定較短的時間範圍來調整查詢，以限制掃描的資料量。

1. 在 Query results (查詢結果) 索引標籤上，每列代表與查詢相符的事件結果。在搜尋列中輸入全部或部分事件欄位值來篩選結果。若要複製事件，選擇您要複製的事件，然後選擇複製。



2. 在 Command output (命令輸出) 索引標籤上，檢視已執行的查詢有關的中繼資料，例如事件資料存放區 ID、執行時間、掃描的結果數以及查詢是否成功。如果您已將查詢結果儲存到 Amazon S3 儲存貯體，中繼資料也會包含已儲存查詢結果所在 S3 儲存貯體的連結。



下載已儲存的查詢結果

儲存查詢結果之後，您必須能夠找到包含查詢結果的檔案。 CloudTrail 將查詢結果傳遞到您在儲存查詢結果時指定的 Amazon S3 儲存貯體。

> **Note**
>
> 儲存查詢結果時，查詢結果可能會在 S3 儲存貯體中檢視之前顯示在主控台中，因為查詢掃描完成後會 CloudTrail 傳送查詢結果。雖然大多數查詢會在幾分鐘內完成，但視事件資料存放區的大小而定，將查詢結果傳遞 CloudTrail 到 S3 儲存貯體可能需要相當長的時間。 CloudTrail

以壓縮的 gzip 格式將查詢結果傳送至 S3 儲存貯體。平均而言，查詢掃描完成後，每傳遞 1 GB 的資料到 S3 儲存貯體，可能會有 60 到 90 秒的延遲。

主題

尋找 CloudTrail 湖泊儲存的查詢結果

CloudTrail 將查詢結果和簽署檔案發佈到 S3 儲存貯體。查詢結果檔案包含已儲存查詢的輸出，簽署檔案則提供查詢結果的簽章和雜湊值。您可以使用簽署檔案來驗證查詢結果。如需有關驗證查詢結果的詳細資訊，請參閱驗證已儲存查詢結果。

若要擷取查詢結果或簽署檔案，您可以使用 Amazon S3 主控台、Amazon S3 命令列界面 (CLI) 或 API。

使用 Amazon S3 主控台尋找查詢結果和簽署檔案

1. 開啟 Amazon S3 主控台。
2. 選擇您指定的儲存貯體。
3. 瀏覽物件階層，找出查詢結果和簽署檔案。查詢結果檔案的副檔名為 .csv.gz，而簽署檔案的副檔名為 .json。

您將瀏覽與下列範例類似的物件階層，但使用不同的儲存貯體名稱、帳戶 ID、日期和查詢 ID。

```
All Buckets
    Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

下載您的 CloudTrail Lake 儲存的查詢結果

儲存查詢結果時，會將兩種類型的檔案 CloudTrail 交付到 Amazon S3 儲存貯體。

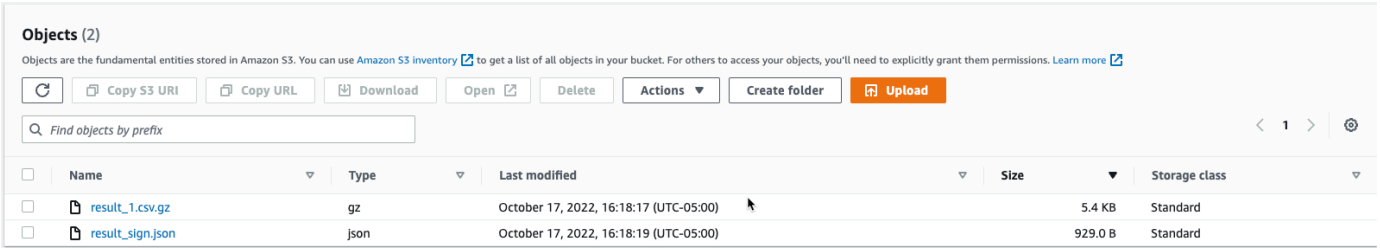
- 一個 JSON 格式的簽署檔案，可供您用於驗證查詢結果檔案。簽署檔案命名為 result_sign.json。如需簽署檔案的詳細資訊，請參閱 CloudTrail 簽署檔案結構。
- 一或多個 CSV 格式的查詢結果檔案，其中包含查詢的結果。傳送的查詢結果檔案數量取決於查詢結果的總大小。查詢結果檔案的檔案大小上限為 1 TB。每個查詢結果檔案都會命名為 result_*number*.csv.gz。例如，如果查詢結果的總大小為 2 TB，您將有兩個查詢結果檔案，result_1.csv.gz 和 result_2.csv.gz。

CloudTrail 查詢結果和簽署文件是 Amazon S3 對象。您可以使用 S3 主控台、 AWS Command Line Interface (CLI) 或 S3 API 擷取查詢結果和簽署檔案。

下列程序說明如何使用 Amazon S3 主控台下載查詢結果和簽署檔案。

使用 Amazon S3 主控台下載查詢結果或簽署檔案

1. 開啟 Amazon S3 主控台。
2. 選擇儲存貯體，然後選擇您要下載的檔案。



3. 選擇 Download (下載)，然後遵循提示來儲存檔案。

> **Note**
>
> 有些瀏覽器 (例如 Chrome) 會自動解壓縮查詢結果檔案。如果您的瀏覽器自動執行這項操作，則請跳到步驟 5。

4. 使用 7-Zip 這類產品來解壓縮查詢結果檔案。
5. 開啟查詢結果或簽署檔案。

驗證已儲存查詢結果

若要判斷查詢結果在 CloudTrail 傳遞查詢結果後是否已修改、刪除或未變更查詢結果，您可以使用 CloudTrail 查詢結果完整性驗證。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 查詢結果文件而不進行檢測。您可以使用命令列來驗證查詢結果檔案。

為什麼使用它？

驗證過的查詢結果檔案對於安全和鑑識調查十分重要。例如，驗證過的查詢結果檔案可讓您肯定地宣告查詢結果檔案本身並未變更。 CloudTrail 查詢結果檔案完整性驗證程序也會讓您知道查詢結果檔案是否已刪除或變更。

主題

驗證已儲存的查詢結果 AWS CLI

您可以使用 aws cloudtrail verify-query-results 命令驗證查詢結果檔案和簽署檔案的完整性。

必要條件

若要使用命令列驗證查詢結果完整性，必須符合下列條件：

- 您必須具有的線上連線 AWS。
- 您必須使用 AWS CLI 版本 2。
- 若要在本機驗證查詢結果檔案和簽署檔案，請套用下列條件：
  - 您必須將查詢結果檔案和簽署檔案放置在指定的檔案路徑。指定檔案路徑作為 --local-export-path 參數的值。
  - 您不得重新命名查詢結果檔案和簽署檔案。
- 若要在 S3 儲存貯體中驗證查詢結果檔案和簽署檔案，請套用下列條件：
  - 您不得重新命名查詢結果檔案和簽署檔案。
  - 您必須具有包含查詢結果檔案和簽署檔案之 Amazon S3 儲存貯體的讀取權限。
  - 指定的 S3 字首必須包含查詢結果檔案和簽署檔案。指定 S3 字首作為 --s3-prefix 參數的值。

verify-query-results

verify-query-results 命令透過比較每個查詢結果檔案的雜湊值和簽署檔案中的 `fileHashValue` 確認該雜湊值，然後驗證簽署檔案中的 `hashSignature`。

當確認查詢結果時，您可以使用 --s3-bucket 和 --s3-prefix 命令列選項來驗證儲存在 S3 儲存貯體中的查詢結果檔案和簽署檔案，或者您可以使用 --local-export-path 命令列選項對已下載查詢結果檔案和簽署檔案執行本機驗證。

> **Note**
>
> verify-query-results 命令限特定區域使用。您必須指定--region全域選項，以驗證特定的查詢結果 AWS 區域。

下列是 verify-query-results 命令選項。

--s3-bucket *<string>*

指定儲存查詢結果檔案和簽署檔案的 S3 儲存貯體名稱。您不能將此參數與 --local-export-path 搭配使用。

--s3-prefix *<string>*

指定包含查詢結果檔案和簽署檔案的 S3 資料夾的 S3 路徑 (例如，`s3/path/`)。您不能將此參數與 --local-export-path 搭配使用。如果檔案位於 S3 儲存貯體的根目錄中，則不需要提供此參數。

--local-export-path *<string>*

指定包含查詢結果檔案和簽署檔案的本機目錄 (例如，`/local/path/to/export/file/`)。您不能將此參數與 --s3-bucket 或 --s3-prefix 搭配使用。

範例

下列範例使用 --s3-bucket 和 --s3-prefix 命令列選項驗證查詢結果，以指定包含查詢結果檔案和簽署檔案的 S3 儲存貯體名稱和字首。

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

下列範例使用 --local-export-path 命令列選項驗證已下載查詢結果，以指定查詢結果檔案和簽署檔案的本機路徑。如需有關下載查詢結果檔案的詳細資訊，請參閱 下載您的 CloudTrail Lake 儲存的查詢結果。

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

驗證結果

下表說明查詢結果檔案和簽署檔案的可能驗證訊息。

檔案類型	驗證訊息	描述
Sign file	Successfully validated sign and query result files	簽署檔案簽章有效。可以檢查其參考的查詢結果檔案。
Query result file	ValidationError: "File *file_name* has inconsistent hash value with hash value recorded in sign file, hash value in sign file is *expected_hash* , but get *computed_hash*	驗證失敗，因為查詢結果檔案的雜湊值與簽署檔案中的 fileHashValue 不相符。
Sign file	ValidationError: Invalid signature in sign file	簽署檔案驗證失敗，因為簽章無效。

CloudTrail 簽署檔案結構

簽署檔案包含您儲存查詢結果時傳送至您 Amazon S3 儲存貯體的每個查詢結果檔案名稱、每個查詢結果檔案的雜湊值，以及檔案的數位簽章。數位簽章和雜湊是用於驗證查詢結果檔案和簽署檔案本身的完整性。

簽署檔案位置

簽署檔案會傳送到遵循此語法的 Amazon S3 儲存貯體位置。

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

範例簽署檔案內容

下列範例符號檔案包含 CloudTrail Lake 查詢結果的資訊。

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

簽署檔案欄位說明

以下是簽署檔案中每個欄位的說明：

`version`

簽署檔案的版本。

`region`

用於儲存查詢結果之 AWS 帳戶的「區域」。

`files.fileHashValue`

壓縮查詢結果檔案內容的十六進位編碼雜湊值。

`files.fileName`

查詢結果檔案的名稱。

`hashAlgorithm`

用於對查詢結果檔案進行雜湊的雜湊演算法。

`signatureAlgorithm`

用於簽署檔案的演算法。

`queryCompleteTime`

指出何時將查詢結果 CloudTrail 傳遞至 S3 儲存貯體。您可以使用此值來尋找公有金鑰。

`hashSignature`

檔案的雜湊簽章。

`publicKeyFingerprint`

用於簽署檔案之公有金鑰的十六進位編碼指紋。

CloudTrail 查詢結果檔案完整性驗證的自訂實作

由於 CloudTrail 使用業界標準、公開可用的加密演算法和雜湊函數，因此您可以建立自己的工具來驗證 CloudTrail 查詢結果檔案的完整性。將查詢結果儲存到 Amazon S3 儲存貯體時，會將簽署檔 CloudTrail 交付到 S3 儲存貯體。您可以實作自己的驗證解決方案，以驗證簽章和查詢結果檔案。如需簽署檔案的詳細資訊，請參閱 CloudTrail 簽署檔案結構。

本主題說明簽署檔案的簽署方式，並接著詳細說明您必須執行的步驟，以實作解決方案來驗證簽署檔案及其所參考的查詢結果檔案。

瞭解 CloudTrail 簽署檔案的簽署方式

CloudTrail 簽署檔案會使用 RSA 數位簽章簽署。針對每個簽署檔案， CloudTrail執行下列動作：

1. 建立雜湊清單，內含每個查詢結果檔案的雜湊值。

2. 取得區域唯一的私有金鑰。
3. 將字串和私有金鑰的 SHA-256 雜湊傳遞到 RSA 簽署演算法，以產生數位簽章。
4. 將簽章的位元組碼編碼為十六進位格式。
5. 將數位簽章放入簽署檔案中。

資料簽署字串內容

資料簽署字串是由每個查詢結果檔案的雜湊值 (以空格分隔) 所組成。簽署檔案會列出每個查詢結果檔案的 `fileHashValue`。

自訂驗證實作步驟

實作自訂驗證解決方案時，您需要先驗證簽署檔案，再驗證其所參考的查詢結果檔案。

驗證簽署檔案

若要驗證簽署檔案，您需要其簽章、其私有金鑰已用來簽署的公有金鑰，以及用來運算的資料簽署字串。

1. 取得簽署檔案。
2. 確認已從其原始位置擷取簽署檔案。
3. 取得簽署檔案的十六進位編碼簽章。
4. 取得其私有金鑰已用來簽署簽署檔案之公有金鑰的十六進位編碼指紋。
5. 擷取簽署檔案中 `queryCompleteTime` 對應時間範圍的公有金鑰。針對時間範圍，請選擇早於 `queryCompleteTime` 的 `StartTime` 和晚於 `queryCompleteTime` 的 `EndTime`。
6. 從所擷取的公有金鑰，選擇其指紋符合簽署檔案中 `publicKeyFingerprint` 值的公有金鑰。
7. 使用包含每個查詢結果檔案雜湊值 (以空格分隔) 的雜湊清單，重新建立用於驗證簽署檔案簽章的資料簽署字串。簽署檔案會列出每個查詢結果檔案的 `fileHashValue`。

   例如，如果簽署文件的 `files` 陣列包含以下三個查詢結果檔案，則雜湊清單為「aaa bbb ccc」。

```
“files": [

   {

        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"
```

```
    },
    {

         "fileHashValue" : “bbb”,

         "fileName" : "result_2.csv.gz"

    },
    {

         "fileHashValue" : “ccc”,

         "fileName" : "result_3.csv.gz"

    }
],
```

8. 傳遞字串、公有金鑰和簽章的 SHA-256 雜湊做為 RSA 簽章驗證演算法的參數，來驗證簽章。如果結果為 true，則簽署檔案有效。

驗證查詢結果檔案

如果簽署檔案有效，請驗證簽署檔案所參考的查詢結果檔案。若要驗證查詢結果檔案的完整性，請在其壓縮內容上運算 SHA-256 雜湊值，並將結果與簽署檔案中所記錄查詢結果檔案的 `fileHashValue` 進行比較。如果雜湊相符，則查詢結果檔案有效。

下列各節將詳細說明驗證程序。

A. 取得簽署檔案

第一步是取得簽署檔案和公有金鑰的指紋。

1. 針對您要驗證的查詢結果從 Amazon S3 儲存貯體取得簽署檔案。
2. 接下來，從簽署檔案中取得 `hashSignature` 值。
3. 在簽署檔案中，從 `publicKeyFingerprint` 欄位取得其私有金鑰已用來簽署檔案之公有金鑰的指紋。

B. 擷取用於驗證簽署檔案的公有金鑰

若要取得驗證簽署檔案的公開金鑰，您可以使用 AWS CLI 或 CloudTrail API。在這兩種情況下，您會為要驗證的簽署檔案指定時間範圍 (即開始時間和結束時間)。使用符號檔案中 `queryCompleteTime`

對應的時間範圍。您指定的時間範圍內可能會傳回一或多個公有金鑰。傳回的金鑰可能會有重疊的有效時間範圍。

> **Note**
>
> 由於每個區域 CloudTrail 使用不同的私鑰/公鑰對，因此每個簽署文件都使用其區域唯一的私鑰進行簽名。因此，當您驗證來自特定區域的簽署檔案時，您必須從同一個區域擷取其公有金鑰。

使用擷 AWS CLI 取公開金鑰

若要使用擷取簽署檔案的公開金鑰 AWS CLI，請使用`cloudtrail list-public-keys`指令。此命令的格式如下：

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

開始時間和結束時間參數是 UTC 時間戳記，而且是選用的。如果未指定，則會使用目前的時間，並傳回一或多個目前作用中的公有金鑰。

回應範例

回應會是代表所傳回之一或多個金鑰的 JSON 物件清單：

使用 CloudTrail API 擷取公開金鑰

若要使用 CloudTrail API 擷取簽署檔案的公開金鑰，請將開始時間和結束時間值傳遞至 `ListPublicKeys` API。`ListPublicKeys` API 會傳回其私有金鑰已在指定時間範圍內用來簽署檔案的公有金鑰。針對每個公有金鑰，API 也會傳回對應的指紋。

`ListPublicKeys`

本節說明 `ListPublicKeys` API 的請求參數和回應元素。

> **Note**
>
> `ListPublicKeys` 的二進位欄位編碼可能會有所變更。

請求參數

名稱	描述
StartTime	選擇性地指定時間範圍的開始時間範圍，以查詢 CloudTrail 簽署檔案的公開金鑰。如果 StartTime 未指定，則使用當前時間，並返回當前的公鑰。 類型: DateTime
EndTime	選擇性地指定時間範圍的結束時間範圍，以查詢 CloudTrail 簽署檔案的公開金鑰。如果 EndTime 未指定，則使用目前時間。 類型: DateTime

回應元素

PublicKeyList 是 PublicKey 物件陣列，其中包含：

名稱	描述
Value	PKCS #1 格式的 DER 編碼公有金鑰值。 類型：Blob
ValidityStartTime	公有金鑰的有效開始時間。 類型: DateTime
ValidityEndTime	公有金鑰的有效結束時間。 類型: DateTime
Fingerprint	公有金鑰的指紋。該指紋可用來識別驗證簽署檔案所需使用的公有金鑰。 類型：字串

C. 選擇要用於驗證的公有金鑰

從 list-public-keys 或 ListPublicKeys 所擷取的公有金鑰，選擇其指紋符合簽署檔案 publicKeyFingerprint 欄位中所記錄之指紋的公有金鑰。這是您將用來驗證簽署檔案的公有金鑰。

D. 重新建立資料簽署字串

現在您已擁有簽署檔案的簽章及相關聯的公有金鑰，您需要計算資料簽署字串。計算資料簽署字串之後，您將擁有驗證簽章所需的輸入。

資料簽署字串是由每個查詢結果檔案的雜湊值 (以空格分隔) 所組成。重新建立此字串之後，您可以驗證簽署檔案。

E. 驗證簽署檔案

將重新建立後的資料簽署字串、數位簽章和公有金鑰傳遞到 RSA 簽章驗證演算法。如果輸出為 true，則簽署檔案的簽章已經過驗證且簽署檔案有效。

F. 驗證查詢結果檔案

驗證簽署檔案之後，您可以驗證其所參考的查詢結果檔案。簽署檔案包含查詢結果檔案的 SHA-256 雜湊。如果其中一個查詢結果檔案在 CloudTrail 傳送之後被修改，SHA-256 雜湊將會變更，且簽署檔案的簽章將不符。

使用以下程序來驗證簽署檔案的 `files` 陣列中列出的查詢結果檔案。

1. 從簽署檔案中的 `files.fileHashValue` 欄位擷取檔案的原始雜湊。
2. 使用 `hashAlgorithm` 中指定的雜湊演算法，將查詢結果檔案的壓縮內容進行雜湊。
3. 將您為每個查詢結果檔案產生的雜湊值與簽署檔案中的 `files.fileHashValue` 進行比較。如果雜湊相符，則查詢結果檔案有效。

離線驗證簽章和查詢結果檔案

離線驗證簽署和查詢結果檔案時，您通常可以遵循先前章節中所述的程序。不過，您必須考慮以下有關公有金鑰的資訊。

公有金鑰

若要離線驗證，您必須先在線上取得在指定時間範圍內驗證查詢結果檔案所需的公有金鑰 (例如藉由呼叫 `ListPublicKeys`)，然後存放在離線位置。每當您想要在指定的初始時間範圍外驗證其他檔案時，都必須重複此步驟。

範例驗證程式碼片段

下列範例程式碼片段提供用於驗證 CloudTrail 符號和查詢結果檔案的基礎架構程式碼。此骨架程式碼線上/離線皆可使用；也就是說，您可以決定是否要線上連線到 AWS來實作它。建議的實作使用 Java Cryptography Extension (JCE) 和 Bouncy Castle 做為安全供應商。

此範例程式碼片段說明：

- 如何建立用來驗證簽署檔案簽章的資料簽署字串。
- 如何驗證簽署檔案的簽章。
- 如何計算查詢結果檔案的雜湊值，並將其與簽署檔案中列出的 `fileHashValue` 進行比較，以驗證查詢結果檔案的真實性。

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());
```

```
        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");

        for (int i = 0; i < jsonArray.length(); i++) {
            JSONObject file = jsonArray.getJSONObject(i);
            String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
file.getString("fileName"));

            // Load the export file from S3 (using Amazon S3 Client) or from your local
copy
            byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3ObjectKey);
            messageDigest.update(exportFileContent);
            byte[] exportFileHash = messageDigest.digest();
            messageDigest.reset();
            byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

            boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
            if (!signaturesMatch) {
                System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                        s3Bucket, fileS3ObjectKey,
                        Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
            } else {
                System.out.println(String.format("Export file: %s/%s hash match",
                        s3Bucket, fileS3ObjectKey));
            }

            hashList.add(file.getString("fileHashValue"));
        }
        String hashListString = hashList.stream().collect(Collectors.joining(" "));

        /*
            NOTE:
            To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
            of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
            returned from ListPublicKey API are DER encoded in PKCS#1 format:

            PublicKeyInfo ::= SEQUENCE {
```

```
                algorithm       AlgorithmIdentifier,
                PublicKey       BIT STRING
            }

            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
 getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
 AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
 rsaPublicKey);

        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

CloudTrail 使用 AWS CLI

您可以使用 AWS CLI 來執行和管理 L CloudTrail ake 查詢。使用時 AWS CLI，請記住您的命令會在為您的設定檔所 AWS 區域 設定的中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

CloudTrail 湖泊查詢的可用指令

在 CloudTrail Lake 中執行和管理查詢的指令包括：

- `start-query`以執行查詢。
- `describe-query`以傳回查詢的中繼資料。
- `get-query-results`以傳回指定查詢 ID 的查詢結果。
- `list-queries`以取得指定事件資料存放區的清單查詢。
- `cancel-query`以取消執行中的查詢。

若要取得 CloudTrail Lake 事件資料倉庫的可用指令清單，請參閱〈〉事件資料倉庫的可用指令。

如需 CloudTrail Lake 整合的可用命令清單，請參閱 CloudTrail 湖泊整合的可用命令。

啟動查詢 AWS CLI

下列範例 AWS CLI start-query命令會針對在查詢陳述式中指定為 ID 的事件資料存放區執行查詢，並將查詢結果傳送至指定的 S3 儲存貯體。`--query-statement` 參數提供用單引號括住的 SQL 查詢。選用參數包括 `--delivery-s3uri`，用於將查詢結果傳送到指定的 S3 儲存貯體。若要取得有關可在 CloudTrail Lake 中使用的查詢語言的更多資訊，請參閱〈〉CloudTrail 湖泊 SQL 條件約束。

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

回應為 `QueryId` 字串。若要取得查詢的狀態，請使用 start-query 傳回的 `QueryId` 值執行 describe-query。如果查詢成功，則可以執行 get-query-results 取得結果。

輸出

```
{
```

```
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> 執行時間超過一小時的查詢可能會逾時。您仍然可以取得在查詢逾時之前處理的部分結果。如果您使用選用--delivery-s3uri參數將查詢結果傳遞至 S3 儲存貯體，則儲存貯體政策必須授與將查詢結果交付給儲存貯體的 CloudTrail權限。如需手動編輯儲存貯體政策的資訊，請參閱「CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策」。

取得有關查詢的中繼資料 AWS CLI

下列範例 AWS CLI describe-query命令會取得有關查詢的中繼資料，包括以毫秒為單位的查詢執行時間、已掃描並符合的事件數、已掃描的位元組總數，以及查詢狀態。除非查詢仍在執行中，否則 BytesScanned 值與用於您帳戶查詢計費的位元組數相符。如果查詢結果被傳遞到 S3 儲存貯體，回應還會提供 S3 URI 和傳遞狀態。

您必須為 --query-id 或 --query-alias 參數指定一個值。指定 --query-alias 參數會傳回上一次為別名執行查詢的相關資訊。

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

以下是回應範例。

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

取得查詢結果 AWS CLI

下列範例 AWS CLI get-query-results 命令取得查詢的事件資料結果。您必須指定由 start-query 命令傳回的 --query-id。除非查詢仍在執行中，否則 BytesScanned 值與用於您帳戶查詢計費的位元組數相符。選用參數包括--max-query-results，藉以指定想要命令在單一頁面上傳回的最大結果數。如果結果多於您指定的 --max-query-results 值，請再次執行命令，新增傳回的 NextToken 值以取得下一頁的結果。

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

輸出

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

列出事件資料存放區上的所有查詢 AWS CLI

下列範例 AWS CLI list-queries 命令會傳回過去七天內指定事件資料存放區上的查詢和查詢狀態清單。您必須對於 --event-data-store 指定 ARN 或 ARN 值的 ID 尾碼。或者，若要縮短結果清單，您可以新增 --start-time 和 --end-time 參數以及 --query-status 值指定時間範圍 (格式為時間戳記)。QueryStatus 的有效值包括：QUEUED、RUNNING、FINISHED、FAILED 或 CANCELLED。

list-queries 也有選用的分頁參數。使用 --max-results 指定您想要命令在單一頁面上傳回的最大結果數。如果結果多於您指定的 --max-results 值，請再次執行命令，新增傳回的 NextToken 值以取得下一頁的結果。

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

輸出

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
    "NextToken": "20add42078135EXAMPLE"
}
```

取消執行中的查詢 AWS CLI

下列範例 AWS CLI cancel-query命令會取消狀態為的RUNNING查詢。您必須指定 --query-id 的值。你執行 cancel-query 時，即使 cancel-query 操作尚未完成，查詢狀態也可能會顯示為 CANCELLED。

> **Note**
>
> 取消的查詢可能會產生費用。取消查詢之前掃描的資料量仍會向您的帳戶收取費用。

以下是 CLI 的範例。

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

輸出

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail 湖泊 SQL 條件約束

CloudTrail 湖泊查詢是 SQL 字串。本節提供支援的函數、運算子和結構描述的相關資訊。

僅允許 SELECT 陳述式。任何查詢字串都無法變更或改變資料。

CloudTrail 湖支持所有有效的普雷斯托 SQL SELECT 語句，函數和運營商。如需支援之 SQL 函數和運算子的詳細資訊，請參閱 Presto 文件網站上的函數和運算子。

主 CloudTrail 控台提供許多範例查詢，可協助您開始撰寫自己的查詢。如需詳細資訊，請參閱 在 CloudTrail 主控台中檢視範例查詢。

主題

- 支援的函數、條件和聯結運算子
- 進階的多重資料表查詢支援

支援的函數、條件和聯結運算子

支援的函數

CloudTrail 湖支持所有普雷斯托功能。如需支援之函數的詳細資訊，請參閱 Presto 文件網站上的函數和運算子。

CloudTrail 湖不支持INTERVAL關鍵字。

支援的條件運算子

下列是支援的條件運算子。

```
AND
```

```
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

支援的聯結運算子

以下是支援的 JOIN 運算子。如需執行多重資料表查詢的詳細資訊，請參閱 進階的多重資料表查詢支援。

```
UNION
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

進階的多重資料表查詢支援

CloudTrail Lake 支援跨多個事件資料存放區的進階查詢語言。

- UNION|UNION ALL|EXCEPT|INTERSECT
- LEFT|RIGHT|INNER JOIN

若要執行查詢，請在 AWS CLI中使用 start-query 命令。以下是使用本節其中一個範例查詢的範例。

```
aws cloudtrail start-query
```

```
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

回應為 QueryId 字串。若要取得查詢的狀態，請使用 start-query 傳回的 QueryId 值執行 describe-query。如果查詢成功，則可以執行 get-query-results 取得結果。

UNION|UNION ALL|EXCEPT|INTERSECT

以下是使用 UNION 和 UNION ALL 在三個事件資料存放區 (EDS1、EDS2 和 EDS3) 依其事件 ID 和事件名稱尋找事件的查詢範例。會先從每個事件資料存放區中選取結果，然後將結果進行串連、依事件 ID 排序以及限制為十個事件。

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

LEFT|RIGHT|INNER JOIN

以下是一個範例查詢，其使用 LEFT JOIN 從名為 eds2 的事件資料存放區中尋找映射到 edsB 的所有事件，這些事件與主要 (左側) 事件資料存放區 edsA 中的事件相符。傳回的事件發生在 2020 年 1 月 1 日或之前，且僅會傳回事件名稱。

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

事件資料存放區的受支援 SQL 結構描述

下列各節提供每種事件資料存放區類型的受支援 SQL 結構描述。

主題

- 支援 CloudTrail 事件記錄欄位的結構描述

- CloudTrail 見解事件記錄欄位支援的結構描述
- 支援的 AWS Config 組態項目記錄欄位結構描述
- 支援的 AWS Audit Manager 證據記錄欄位架構
- 非AWS 事件欄位的支援結構描述

支援 CloudTrail 事件記錄欄位的結構描述

以下是 CloudTrail 管理和資料事件記錄欄位的有效 SQL 結構描述。如需 CloudTrail 事件記錄欄位的詳細資訊，請參閱CloudTrail 記錄內容。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
 "struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

 username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

 mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

 accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

 attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
                ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
    {
        "Name": "eventname",
        "Type": "string"
    },
```

```
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
        "Type": "string"
    },
    {
        "Name": "errorcode",
        "Type": "string"
    },
    {
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
```

```
    {
        "Name": "resources",
        "Type":
 "array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
```

```
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsonchecksum",
        "Type": "string"
    }
]
```

CloudTrail 見解事件記錄欄位支援的結構描述

下列是 Insights 事件記錄欄位的有效 SQL 結構描述。對於 Insights 事件，`eventcategory` 的值為 `Insight`，`eventtype` 的值為 `AwsCloudTrailInsight`。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
```

```
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
```

```
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type":
 "struct<baselineaverage:double,insightaverage:double,baselineduration:integer,

 insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
                insightaverage:double,baselinevalue:string,baselineaverage:double>>"
    }
]
```

支援的 AWS Config 組態項目記錄欄位結構描述

以下是組態項目記錄欄位的有效 SQL 結構描述。對於組態項目，eventcategory 的值為 ConfigurationItem，eventtype 的值為 AwsConfigurationItem。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
```

```
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

支援的 AWS Audit Manager 證據記錄欄位架構

以下是 Audit Manager 證據記錄欄位的有效 SQL 結構描述。對於 Audit Manager 證據記錄欄位，`eventcategory` 的值為 `Evidence`，`eventtype` 的值為 `AwsAuditManagerEvidence`。如需有關使用 Audit Manager 彙總 CloudTrail Lake 中證據的詳細資訊，請參閱使用AWS Audit Manager 者指南中的[證據搜尋工具](#)。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
```

```
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

非AWS 事件欄位的支援結構描述

以下是非AWS 事件的有效 SQL 結構描述。對於非AWS 事件，的值`eventcategory`為`ActivityAuditLog`，且的值`eventtype`為`ActivityLog`。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
```

```
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

控制 CloudTrail 湖泊的使用者權限

AWS CloudTrail 與 AWS Identity and Access Management (IAM) 整合，協助您控制對 CloudTrail Lake 和其他 CloudTrail 需要的 AWS 資源的存取。您可以使用 IAM 控制哪些使用 AWS 者可以建立、設定或刪除 CloudTrail 事件資料存放區或通道、啟動和停止事件擷取，以及複製追蹤事件。如需進一步了解，請參閱的 Identity and Access Management AWS CloudTrail。

下列主題可協助您瞭解權限、原則和 CloudTrail 安全性：

- 授與CloudTrail 管理權限
- CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策
- 複製追蹤事件所需的許可
- 聯合的所需許可
- 根據標籤對事件資料存放區進行限制存取的範例政策：範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限
- AWS CloudTrail 資源型政策範例
- 指派委派管理員所需的許可
- CloudTrail Lake 事件資料存放區的預設 KMS 金鑰原則

管理 CloudTrail 湖泊成本

AWS CloudTrail Lake 事件資料存放區和查詢會產生費用。我們建議您使用可協助您管理 CloudTrail 成本的 AWS 服務 和工具，做為最佳作法。您也可以透過擷取所需資料的方式設定事件資料存放區，同時具有成本效益。如需 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

主題

事件資料存放區定價選項

建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。

下表說明可用的定價選項。下表顯示主控台中的定價選項，以及 API 的對應 `BillingMode` 值，並列出每個選項的預設和最長保留期。

定價選項 (主控台)	BillingMode (API)	描述
一年可延長保留定價	`EXTENDABLE_RETENTION_PRICING`	如果您預期每月擷取的事件資料少於 25 TB，並且需要長達 10 年的彈性保留期，則建議使用此選項。如果您的事件資料存放區收集 AWS Config 組態項目、Audit Manager 證據和 AWS 外部事件，也建議使用此選項。 前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，延長保留將按 pay-as-you-go價格提供。 此為預設選項。 預設保留期：366 天 最長保留期：3,653 天
七年保留定價	`FIXED_RETENTION_PRICING`	如果您預期每月擷取的事件資料超過 25 TB，並且需要長達 7 年的彈性保留期，則建議使用此選項。

定價選項 (主控台)	BillingMode (API)	描述
		保留已包含在擷取定價中，無須額外付費。 預設保留期：2,557 天 最長保留期：2,557 天

了解 CloudTrail 湖泊費

下表提供 CloudTrail Lake 事件資料儲存和查詢如何產生費用的相關資訊。如需 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

收費類型	如何產生費用
資料擷取 (未壓縮的資料)	對於 CloudTrail Lake，您需要根據擷取的未壓縮資料付費。事件資料存放區的定價選項將決定擷取事件的成本： • 一年可延長保留定價：根據事件類型提供擷取定價。 • 七年保留定價：根據擷取的資料量提供擷取定價。當每月擷取的資料量超過 25 TB 時，即可達到最大程度的節省。 複製追蹤事件 當您將追蹤事件複製到 CloudTrail Lake 時，會 CloudTrail 解壓縮以 gzip (壓縮) 格式儲存的記錄檔。然後 CloudTrail 將記錄檔中包含的事件複製到您的事件資料存放區。未壓縮資料的大小可能大於實際的 Amazon S3 儲存大小。若要取得未壓縮資料大小的一般估計值，請將 S3 儲存貯體中的日誌大小乘以 10。 **Note** CloudTrail 如果事件時間早於指定的保留期間，則不會複製事件。若要確定適當的保留期，請計算您要複製的最舊事件所經歷的天數，以及要將事件保留在事件資料存放區中的天數，並將兩者加總，如以下等式所示：

收費類型	如何產生費用
	保留期間 = *oldest-event-in-days* + *number-days-to-retain* 例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。
資料保留 (最佳化和壓縮的資料)	CloudTrail 湖將基於行的 JSON 格式的現有事件轉換為 Apache ORC 格式。ORC 是一種單欄式儲存格式，已針對快速擷取壓縮資料進行最佳化。 事件資料存放區的保留期決定了事件資料在事件資料存放區中保留的時間長度。 CloudTrail Lake 會檢查事件的事件時間是否在指定的保留期間內，以判斷是否要保留事件。例如，如果您指定 90 天的保留期，則 CloudTrail 會在事件時間超過 90 天時移除事件。 若為使用七年保留定價選項的事件資料存放區，則儲存已包含在擷取定價中，無須額外付費。 若為使用一年可延長保留定價選項的事件資料存放區，則前 366 天 (預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天之後，儲存會依照事件資料存放區中最佳化 pay-as-you-pricing 和壓縮的資料提供，且會依據其中的最佳化和壓縮資料收費。
在 CloudTrail Lake 中執行查詢 (最佳化和壓縮資料)	在 CloudTrail Lake 中執行查詢時，您需要根據掃描的最佳化和壓縮資料量付費。

有關如何降低成本的建議

本節提供有關如何在使用 CloudTrail Lake 時降低成本的建議。

根據事件資料存放區將收集的事件類型，以及您預期的每月擷取量，選擇定價選項

建立事件資料存放區時，請根據事件資料存放區將收集的事件類型，以及您預期的每月擷取，選擇定價選項。

如果您預期每月擷取的事件資料少於 25 TB，並且需要長達 10 年的彈性保留期，請選擇一年可延長保留定價選項。對於從外部收集 AWS Config 組態項目、Audit Manager 證據和事件的事件資料存放區，我們通常也會建議使用此選項 AWS。

如果您預期每月擷取的事件資料超過 25 TB，並且需要長達 7 年的彈性保留期，請選擇七年保留定價選項。

評估事件資料存放區隨時間推移的每月擷取

評估事件資料存放區的歷史每月擷取，以查看是否有更符合您需求的定價選項。

如果您現有的事件資料存放區使用七年保留定價選項，而且您每月擷取的資料少於 25 TB，請考慮更新事件資料存放區，以使用一年可延長保留定價。對於使用七年保留定價選項的事件資料存放區，您可以使用CloudTrail 主控台或 UpdateEventDataStoreAPI 作業變更定價選項。AWS CLI

如果您現有的事件資料存放區使用一年可延長保留定價選項，而且您每月擷取的資料超過 25 TB，請考慮七年保留定價選項是否更符合您的需求。若要使用新的定價選項，請在您的事件資料存放區上停止擷取，並使用七年保留定價選項建立新的事件資料存放區。

使用進階事件選取器篩選掉不感興趣的事件

為 CloudTrail 管理或資料事件設定事件資料存放區時，請使用進階事件選取器篩選出不感興趣的事件。

如果您要建立事件資料存放區來收集管理事件，可以篩選掉 AWS Key Management Service (AWS KMS) 或 Amazon Relational Database Service (Amazon RDS) 資料 API 事件。通常情況下`Encrypt`， AWS KMS 動作如`Decrypt`、和`GenerateDataKey`產生超過 99% 的事件。

如果您要建立事件資料存放區來收集資料事件，則可以使用進階事件選取器依 `eventName`、`resources.type`、`resources.ARN` 和 `readOnly` 欄位進行篩選。如需範例，請參閱範例：為 S3 資料事件建立事件資料存放區。

在複製追蹤事件時選擇較短的時間範圍

將追蹤事件複製到 CloudTrail Lake 時，請指定較窄的開始事件時間和結束事件時間，以減少擷取的資料量。

如果您要將追蹤事件複製到 CloudTrail Lake 以進行歷史分析，但不想擷取 future 事件，請取消選取擷取事件的選項，這樣您就不會因擷取任何其他事件而產生費用。

格式化查詢以使用開始和結束 **`eventTime`**

在 Lake 中執行查詢時，您需要依據掃描的資料量付費。您可以指定查詢的開始和結束 `eventTime`，藉此限制成本。

協助管理成本的工具

AWS 預算是的一項功能 AWS Billing and Cost Management，可讓您設定自訂預算，以便在成本或用量超過 (或預測超過) 您的預算金額時提醒您。

建立事件資料存放區時，建議使用「 AWS 預算」建立預算是最佳做法，可協助您追蹤 CloudTrail 支出。 CloudTrail 基於成本的預算有助於提高您的使用可能需要支付多少費 CloudTrail 用的認識。 當帳單達到您定義的閾值時，預算警示會通知您。收到預算提醒時，您可以在計費週期結束之前進行變更，以便管理您的成本。

建立預算後，您可以使用 AWS Cost Explorer 來查看 CloudTrail 成本如何影響整體帳 AWS 單。在 Co AWS st Explorer 中，新增 CloudTrail 至服務篩選器之後，您可以依區域和帳戶比較您目前 month-to-date (MTD) 支出的歷史 CloudTrail支出。此功能可協助您監控並偵測每月 CloudTrail支出中的非預期成本。Cost Explorer 中的其他功能可讓您比較 CloudTrail 特定資源層級的支出與每月支出，提供有關可能導致帳單成本增加或減少的資訊。

若要開始使用 AWS 預算，請開啟 AWS Billing and Cost Management，然後選擇左側導覽列中的 [預算]。建議您在建立預算以追蹤 CloudTrail 支出時，設定預算警示。如需如何使用 AWS 預算的詳細資訊，請參閱使用管理成本 AWS Budgets和AWS 預算的最佳做法。

為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置

您可以建立使用者定義的成本配置標籤，以追蹤 CloudTrail Lake 事件資料存放區的查詢和擷取成本。使用者定義的成本分配標籤是可以和事件資料存放區關聯的鍵值組。啟動成本分配標籤之後，AWS 會使用標籤來整理成本分配報表上的資源成本。

- 若要在主控台中建立標籤，請參閱「建立 CloudTrail 管理或資料事件的事件資料倉庫」程序中的步驟 9。
- 若要使用 CloudTrail API 建立標籤，請參閱 AWS CloudTrail API 參考資料AddTags中的CreateEventDataStore和。
- 若要使用建立標籤 AWS CLI，請參閱《AWS CLI 指令參考》中的create-event-data-store並加入標籤。

如需有關啟用標籤的詳細資訊，請參閱啟用使用者定義的成本分配標籤。

另請參閱

- AWS CloudTrail 定價
- 支援的 CloudWatch 指標

- 管理您的成本 AWS Budgets
- Cost Explorer 入門

支援的 CloudWatch 指標

CloudTrail 湖支持 Amazon CloudWatch 指標。 CloudWatch 是資 AWS 源的監視服務。您可以用 CloudWatch 來收集和追蹤指標、設定警示，以及自動回應 AWS 資源中的變更。

命`AWS/CloudTrail`名空間包含下列 CloudTrail Lake 的度量。

指標	描述	個單位
`HourlyDataIngested`	最近一小時內擷取至事件資料存放區的資料量。此指標每小時更新一次。 此指標適用於所有事件資料存放區類型。	位元組
`TotalDataRetained`	整個保留期間在事件資料存放區中保留的資料量。此指標會每晚更新。 此指標適用於所有事件資料存放區類型。	位元組
`TotalStorageBytes`	截至當天為止，事件資料存放區中壓縮的總位元組數。 此指標適用於所有事件資料存放區類型。	位元組
`TotalPaidStorageBytes`	對於使用一年可延長保留定價選項的事件資料存放區，此指標為壓縮的總位元組數，時間範圍為 366 天後，直到為事件資料存放區設定的最長保留期。	位元組

指標	描述	個單位
	若為使用一年可延長保留定價選項的事件資料存放區，則前 366 天 (事件資料存放區的預設保留期) 的儲存已包含在擷取定價中，無須額外付費。366 天后，存儲是 pay-as-you-go。如需定價的資訊，請參閱 AWS CloudTrail 定價。 此指標僅適用於使用一年可延長保留定價選項的事件資料存放區。	
HourlyEventsAnalyzed	事件資料存放區中「 CloudTrail 見解」分析的事件總數。此指標每小時更新一次。 此量度適用於啟用 CloudTrail 深入解析的 CloudTrail 事件資料存放區。	計數

如需 CloudWatch 測量結果的相關資訊，請參閱下列主題。

- 使用 Amazon CloudWatch 指標
- 使用 Amazon CloudWatch 警報

使用 CloudTrail 軌跡

追蹤可擷取 AWS 活動記錄，在 Amazon S3 儲存貯體中交付和存放這些事件，並可選擇交付到CloudWatch 日誌和 Amazon EventBridge。

您可以透 CloudTrail 過建立追蹤，免費將一份正在進行的管理事件副本傳遞到 S3 儲存貯體，但是 Amazon S3 儲存會產生費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

您可以為一個建立兩種類型的系統線 AWS 帳戶：多區域系統線和單一區域系統線。

多區域步道

當您建立多區域追蹤時，會將事件 CloudTrail 記錄在您正 AWS 區域 在使用的AWS 分割區中的所有事件，並將 CloudTrail 事件日誌檔案傳送到您指定的 S3 儲存貯體。如果 AWS 區域 在您建立多區域追蹤後新增，則會自動包含該新區域，並記錄該區域中的事件。由於您要擷取帳戶所有區域內的活動，因此建立多區域追蹤是建議的最佳實務。您使用 CloudTrail 主控台建立的所有路徑都是多區域。您可以使用將單一區域系統軌跡轉換為多區域系統線。 AWS CLI如需詳細資訊，請參閱 在主控台中建立追蹤 及 將套用至一個區域的追蹤轉換成套用至所有區域。

單一區域步道

當您建立單一區域追蹤時，只會 CloudTrail 記錄該區域中的事件。然後，它會將 CloudTrail 事件日誌檔傳送到您指定的 Amazon S3 儲存貯體。您只能使用 AWS CLI建立單一區域追蹤。如果您建立額外的單一追蹤，您可以讓這些追蹤將 CloudTrail 事件日誌檔傳遞至相同的 S3 儲存貯體或個別儲存貯體。當您使用 AWS CLI 或 CloudTrail API 建立追蹤時，這是預設選項。如需詳細資訊，請參閱 建立、更新和管理追蹤 AWS CLI。

> **Note**
>
> 對於這兩種類型的追蹤，您可以指定來自任何區域的 Amazon S3 儲存貯體。

如果您已在中建立組織 AWS Organizations，則可以建立組織追蹤記錄該組織中所有 AWS 帳戶的所有事件。組織追蹤可套用至所有「區 AWS 域」或目前的「區域」。組織追蹤必須透過管理帳戶或委派的管理員帳戶建立，且在獲指定套用到組織時，將會自動套用到組織中的所有成員帳戶。成員帳戶可以看到組織軌跡，但無法修改或刪除它。在預設情況下，成員帳戶無法存取 Amazon S3 儲存貯體中組織追蹤的日誌檔案。如需更多詳細資訊，請參閱 建立組織追蹤。

主題

為您的建立追蹤 AWS 帳戶

建立線索之後，您要啟用以日誌檔案形式，持續將事件交付到您指定的 Amazon S3 儲存貯體。建立線索的好處相當多，包括如下：

- 超出 90 天事件的記錄。
- 透過將日誌事件傳送至 Amazon CloudWatch Logs，自動監控和警示指定事件的選項。
- 使用 Amazon Athena 查詢日誌和分析 AWS 服務活動的選項。

從 2019 年 4 月 12 日開始，您只能在他們記錄事件的 AWS 區域中檢視追蹤。如果您建立記錄所有 AWS 區域中事件的追蹤，該追蹤會顯示在您正在使用之 AWS 分割區中所有區域的主控台中。如果您建立只在單一 區域中記錄事件的追蹤，您可以僅在該 區域進行查看和管理。如果您使用 AWS CloudTrail 主控台建立追蹤，則建立多區域追蹤是預設選項，這是建議的最佳作法。若要建立單一區域追蹤，您必須使用 AWS CLI。

如果您使用 AWS Organizations，您可以建立追蹤，以記錄組織中所有 AWS 帳戶的事件。個別成員帳戶中將會建立名稱相同的線索，而個別線索的事件將交付到您指定的 Amazon S3 儲存貯體。

> **Note**
>
> 只有組織的管理帳戶或委派的管理員帳戶可以為該組織建立線索。為組織建立追蹤會自動啟用與組織之間 CloudTrail 的整合。如需更多詳細資訊，請參閱 建立組織追蹤。

主題

使用主控台建立和更新線索

您可以使用 CloudTrail 主控台建立、更新或刪除追蹤。使用主控台建立的追蹤為多區域追蹤。若要建立僅記錄一個事件的追蹤 AWS 區域，請使用 AWS CLI.

每個區域最多可以建立五個追蹤。建立追蹤後， CloudTrail會自動開始將帳戶中的 API 呼叫和相關事件記錄到您指定的 Amazon S3 儲存貯體。若要停止記錄，您可以關閉或刪除線索的記錄。

使用主 CloudTrail 控台建立或更新追蹤可提供下列優點。

- 如果這是您第一次建立追蹤，使用 CloudTrail 主控台可讓您檢視可用的功能和選項。
- 如果您要設定記錄資料事件的追蹤，使用 CloudTrail 主控台可讓您檢視可用的資料類型。如需有關記錄資料事件的詳細資訊，請參閱 記錄資料事件。

如需在中為組織建立軌跡的特定資訊 AWS Organizations，請參閱建立組織追蹤。

主題

建立追蹤

最佳實務是建立套用至所有 AWS 區域的追蹤。這是您在 CloudTrail主控台中建立追蹤時的預設設定。當追蹤套用至所有區域時，會將您正在使用之AWS 分割區中所有區域的日誌檔 CloudTrail 傳遞至您指定的 S3 儲存貯體。建立追蹤之後， AWS CloudTrail 會自動開始記錄您指定的事件。

> **Note**
>
> 建立追蹤之後，您可以設定其他，以 AWS 服務 進一步分析 CloudTrail 記錄檔中收集的事件資料並採取行動。如需詳細資訊，請參閱 AWS 與 CloudTrail 日誌的服務整合。

主題

在主控台中建立追蹤

使用下列程序建立追蹤，以記錄您正在使用的 AWS 磁碟分割中的所有 AWS 區域 事件。這是建議的最佳實務。若要記錄單一區域內的事件 (不建議)，請使用 AWS CLI。

使用建立 CloudTrail 系統線 AWS Management Console

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 服務首頁、「追蹤」頁面或「儀表板」頁面的「追蹤」區段中，選擇「建立軌跡」。
3. 在 Create Trail (建立追蹤) 頁面的 Trail name (追蹤名稱) 中，輸入追蹤的名稱。如需詳細資訊，請參閱 命名要求。
4. 如果這是組 AWS Organizations 織追蹤，您可以為組織中的所有帳戶啟用追蹤。若要查看此選項，您必須使用管理或委派的管理員帳戶中的使用者或角色登入到主控台。若要成功建立組織追蹤，請確保該使用者或角色具備足夠許可。如需詳細資訊，請參閱 建立組織追蹤。
5. 針對 Storage location (儲存位置)，選擇 Create a new S3 bucket (建立新 S3 儲存貯體)，以建立儲存貯體。建立值區時， CloudTrail會建立並套用所需的值區政策。如果您選擇建立新的 S3 儲存貯體，您的 IAM 政策需要包含`s3:PutEncryptionConfiguration`動作的權限，因為預設情況下會為儲存貯體啟用伺服器端加密。

   > **Note**
   >
   > 如果您選擇使用現有的 S3 儲存貯體，請在追蹤日誌儲存貯體名稱中指定一個儲存貯體，或選擇瀏覽以便在您自己的帳戶中選擇一個儲存貯體。如果想要在其他帳戶中使用儲存貯體，您需要指定儲存貯體名稱。值區政策必須授 CloudTrail 予寫入權限。如需手動編輯儲存貯體政策的資訊，請參閱「Amazon S3 存儲桶政策 CloudTrail」。

   為了更輕鬆地找到您的日誌，請在現有存儲桶中創建一個新文件夾（也稱為前綴）以存儲 CloudTrail 日誌。在字首中輸入字首。

6. 針對 Log file SSE-KMS encryption (日誌檔案 SSE-KMS 加密)，如果您想要使用 SSE-KMS 而非 SSE-S3 來加密日誌檔案，請選擇 Enabled (啟用)。預設為啟用。如果您未啟用 SSE-KMS 加密，則會使用 SSE-S3 加密來加密您的日誌。如需 SSE-KMS 加密的詳細資訊，請參閱使用伺服器端加密搭配 AWS Key Management Service (SS E-KMS)。如需 SSE-S3 加密的詳細資訊，請參閱搭配使用伺服器端加密與 Amazon S3 受管加密金鑰 (SSE-S3)。

   如果您啟用 SSE-KMS 加密，請選擇 [新增] 或 [現有]。 AWS KMS key在AWS KMS 別名中，以格式指定別名`alias/MyAliasName`。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

   > **Note**
   >
   > 您也可以從另一個帳戶輸入金鑰的 ARN。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。金鑰原則必須允許 CloudTrail 使用金鑰來加密記錄檔，並允許您指定的使用者以未加密的形式讀取記錄檔。如需手動編輯金鑰政策的資訊，請參閱「設定 AWS KMS 金鑰原則 CloudTrail」。

7. 在其他設定下，設定下列項目。

   a. 針對 Log file validation (日誌檔案驗證)，選擇 Enabled (啟用) 將日誌摘要交付到您的 S3 儲存貯體。您可以使用摘要檔來驗證記錄檔在 CloudTrail 傳送記錄檔之後是否未變更。如需詳細資訊，請參閱 驗證 CloudTrail 記錄檔完整性。

   b. 對於 SNS 通知傳遞，請選擇 [啟用]，以便在每次將記錄傳送至儲存貯體時收到通知。CloudTrail 將多個事件儲存在記錄檔中。SNS 通知是針對每個日誌檔案所傳送，而不是每個事件。如需詳細資訊，請參閱 設定 Amazon SNS 通知 CloudTrail。

      如果您啟用 SNS 通知，針對建立新 SNS 主題，選擇 New (新的) 以建立主題，或選擇 Existing (現有) 以使用現有的主題。如果您要建立套用至所有區域的追蹤，則會將所有區域中日誌檔案傳遞的 SNS 通知都交付至您建立的單一 SNS 主題。

      如果您選擇「新增」，請為您 CloudTrail 指定新主題的名稱，或者您也可以輸入名稱。如果選擇 Existing (現有),請從下拉式清單中選擇 SNS 主題。您也可以輸入來自另一個區域，或具有適當許可之帳戶的主題 ARN。如需詳細資訊，請參閱 Amazon SNS 主題政策 CloudTrail。

      如果您建立主題，則必須訂閱該主題，以便在日誌檔案交付時收到通知。您可以從 Amazon SNS 主控台進行訂閱。基於通知頻率，建議您設定訂閱以利用 Amazon SQS 佇列，透過編寫

程式的方式處理通知。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

8. 選擇性地選擇「記錄檔中已啟用」，設定 CloudTrail 將 CloudWatch 記錄檔傳送至CloudWatch 記錄檔。如需詳細資訊，請參閱 將事件傳送至 CloudWatch 記錄檔。

   a. 如果您啟用與 CloudWatch 記錄整合，請選擇 [新增] 以建立新的記錄群組，或選擇 [現有] 使用現有的記錄群組。如果選擇 [新增]，請為您 CloudTrail 指定新記錄群組的名稱，或者輸入名稱。

   b. 如果選擇 Existing (現有)，請從下拉式清單中選擇日誌群組。

   c. 選擇 [新增]，為許可建立新的 IAM 角色，以便將記錄傳送至 CloudWatch 記錄。選擇 Existing (現有) 從下拉式功能表中選擇現有的 IAM 角色。新角色或現有角色的政策陳述式會在您展開政策文件時顯示。如需有關此角色的詳細資訊，請參閱 使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件。

   > **Note**
   >
   > - 設定追蹤時，您可以選擇由其他帳戶所屬的 S3 儲存貯體和 SNS 主題。不過，如果您想 CloudTrail 要將事件傳遞至 CloudWatch 記錄檔記錄群組，則必須選擇目前帳戶中存在的記錄群組。
   > - 只有管理帳戶可以使用主控台為組織追蹤設定 CloudWatch 記錄檔群組。委派的系統管理員可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 作業來設定 CloudWatch 記錄檔記錄群組。

9. 對於 標籤 (Tags)，請將一個或多個自訂標籤 (鍵/值對) 新增至追蹤。標籤可協助您識別 CloudTrail 追蹤和包含 CloudTrail 日誌檔的 Amazon S3 儲存貯體。然後，您可以將資源群組用於資 CloudTrail 源。如需詳細資訊，請參閱 AWS Resource Groups及 標籤。

10. 在選擇日誌事件頁面上，選擇您要記錄的事件類型。對於 Management events (管理事件)，請執行下列動作。

    a. 針對 API 活動，選擇您是否希望追蹤記錄讀取事件、寫入事件，或兩者。如需詳細資訊，請參閱 管理事件。

    b. 選擇「排除 AWS KMS 事件」，將 AWS Key Management Service (AWS KMS) 事件從追蹤中篩選出來。預設設定是包含所有 AWS KMS 事件。

只有在追蹤記錄中記錄管理 AWS KMS 事件時，才能使用記錄或排除事件的選項。如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

AWS KMS 動作，例如`Encrypt`、`Decrypt`、`GenerateDataKey`通常會產生大量 (超過 99%) 的事件。這些動作現在會記錄為 Read (讀取) 事件。低容量的相關 AWS KMS 動作，例如`DisableDelete`、和 `ScheduleKey` (通常佔 AWS KMS 事件磁碟區的 0.5% 以下) 會記錄為「寫入」事件。

若要排除、和等大量事件 `Encrypt` `Decrypt`、`GenerateDataKey`，但仍記錄相關事件 (例如`Disable`、`Delete`和`ScheduleKey`)，請選擇記錄 Write 管理事件，然後清除 [排除 AWS KMS 事件] 的核取方塊。

c. 選擇排除 Amazon RDS Data API 事件從追蹤中篩選 Amazon Relational Database Service Data API 事件。預設設定是包含所有 Amazon RDS Data API 事件。如需 Amazon RDS Data API 事件的詳細資訊，請參閱《Amazon RDS 使用者指南 (Aurora)》中的使用 AWS CloudTrail記錄資料 API 呼叫。

11. 若要記錄資料事件，請選擇資料事件。記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

12.

> **Important**
>
> 依預設，透過使用進階事件選取器執行步驟 12-16，可設定資料事件。進階事件選取器可讓您設定更多資料事件類型，並對追蹤擷取的資料事件提供精細控制。如果您選擇使用基本事件選取器，請完成 使用基本事件選取器執行資料事件設定 中的步驟，然後返回至此程序的步驟 17。

針對資料事件類型，選擇您想要記錄資料事件的資源類型。如需有關可用資料事件類型的詳細資訊，請參閱 資料事件。

> **Note**
>
> 若要記錄由 Lake Formation 成所建立之 AWS Glue 表格的資料事件，請選擇 Lake Formation。

13. 選擇記錄選取器範本。 CloudTrail 包括記錄資源類型的所有資料事件的預先定義範本。若要建立自訂記錄選取器範本，請選擇 Custom (自訂)。

> **Note**
>
> 為 S3 儲存貯體選擇預先定義的範本，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何 IAM 身分執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的值區上執行也一樣。
>
> 如果追蹤僅套用至一個區域，選取預先定義的記錄所有 S3 儲存貯體的範本可針對下列儲存貯體啟用記錄資料事件：與您追蹤相同之區域中的所有儲存貯體，以及您稍後在該區域中建立的任何儲存貯體。它不會記錄帳戶中其他區域中 Amazon S3 儲存貯體的 AWS 資料事件。
>
> 如果您要為所有區域建立追蹤，請為 Lambda 函數選擇預先定義的範本，為 AWS 帳戶中目前的所有函數啟用資料事件記錄，以及在完成追蹤建立後可能在任何區域建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，此選項會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。
>
> 記錄所有功能的資料事件也可讓您記錄 AWS 帳戶中任何 IAM 身分所執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的函數上執行。

14. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。
15. 在進階事件選取器，請為您想要記錄資料事件的特定資源建立表達式。如果您使用預先定義的日誌範本，則可略過此步驟。

    a. 從下列欄位選取。

    - **readOnly**-readOnly 可以設定為等於true或的值false。唯讀資料事件是不會變更資源狀態的事件，例如 Get* 或 Describe* 事件. 寫入事件新增、變更或刪除資源、屬性或成品，例如 Put*、Delete* 或 Write* 事件。若要同時記錄 read 和 write 事件，請勿新增 readOnly 選擇器。
    - **eventName**-eventName可以使用任何運算子。您可以使用它來包含或排除記錄到的任何資料事件 CloudTrailPutBucket，例如PutItem、或GetSnapshotBlock。
    - **resources.ARN**-您可以將任何運算子搭配使用resources.ARN，但是如果您使用 equals 或不等於，則值必須完全符合您在範本中指定為值之類型之有效資源的 ARN。resources.type

下表顯示每種 resources.type 的有效 ARN 格式。

> **Note**
>
> 您無法使用resources.ARN欄位來篩選沒有 ARN 的資源類型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*

resources.type	resources.ARN
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*

resources.type	resources.ARN
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*

resources.type	resources.ARN
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*

resources.type	resources.ARN
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*

resources.type	resources.ARN
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*

resources.type	resources.ARN
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必須採用下列其中一種格式： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*

resources.type	resources.ARN
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必須採用下列其中一種格式： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	resources.ARN
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您指定 AWS::DynamoDB::Table 作為 resources.type，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在eventName欄位上新增篩選器。

[2] 若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 StartsWith 運算子，並僅包含儲存貯體 ARN 作為相符值。末尾斜線是有意保留，請勿排除。

[3] 若要在 S3 存取點中的所有物件上記錄事件，建議您僅使用存取點 ARN、不要包含物件路徑，並使用 StartsWith 或 NotStartsWith 運算子。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的動作、資源及條件金鑰。

b. 針對每個欄位，選擇 + 條件，視需要新增任意數目的條件，所有條件最多可指定 500 個值。例如，若要從追蹤記錄的資料事件中排除兩個 S3 儲存貯體的資料事件，您可以將欄位設定為 Resources.arn，將運算子設定為「不開始於」，然後貼上 S3 儲存貯體 ARN，或瀏覽您不想記錄事件的 S3 儲存貯體。

若要新增第二個 S3 儲存貯體，請選擇 + 條件，然後重複上述指令，在 ARN 中粘貼或瀏覽不同的儲存貯體。

> **Note**
>
> 追蹤上的所有選取器，您最多可以有 500 個值。這包括一個選擇器的多個值的陣列，如 eventName。如果所有選擇器都有單個值，則最多可以有 500 個條件新增至選擇器。
> 如果您的帳戶中有超過 15,000 個 Lambda 函數，則無法在建立追蹤時在 CloudTrail 主控台中檢視或選取所有函數。您仍然可以使用預先定義的選取器範本記錄所有函數，即使其未全部顯示。如果您要記錄特定函數之資料事件，則可以在得知該函數

的 ARN 後手動加以新增。您也可以在主控台中完成追蹤的建立，然後使用 AWS CLI 和put-event-selectors命令為特定 Lambda 函數設定資料事件記錄。如需詳細資訊，請參閱 管理軌跡 AWS CLI。

c. 選擇 + 欄位以根據需要新增其他欄位。為避免發生錯誤，請勿為欄位設定衝突或重複的值。例如，不要在一個選擇器中指定 ARN 等於一個值，然後指定 ARN 不等於另一個選取器中的相同值。

16. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。重複步驟 12 到此步驟，以設定資料事件類型的進階事件選取器。
17. 如果您希望追蹤記錄見解事件，請選擇「 CloudTrail深入解析」事件。

    在 Event type (事件類型) 中，選取 Insights 事件。您必須記錄寫入管理事件，以便記錄 API 呼叫率的 Insights 事件。您必須記錄讀取或寫入管理事件，以便記錄 API 錯誤率的 Insights 事件。

    CloudTrail Insights 會分析異常活動的管理事件，並在偵測到異常時記錄事件。依預設，追蹤不會記錄 Insights 事件。如需 Insights 事件的詳細資訊，請參閱記錄 Insights 事件。記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

    見解事件會傳遞到名為相同 S3 儲存貯體/CloudTrail-Insight的不同資料夾，該資料夾名稱為在追蹤詳細資料頁面的儲存位置區域中指定。 CloudTrail會為您建立新字首。例如，如果您目前的目的地 S3 儲存貯體名為 S3bucketName/AWSLogs/CloudTrail/，則具有新前綴的 S3 儲存貯體名稱會被命名為 S3bucketName/AWSLogs/CloudTrail-Insight/。
18. 當您完成選擇要記錄的事件類型時，請選擇 Next (下一頁)。
19. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇區段中的 Edit (編輯)，以變更該區段中顯示的追蹤設定。當您準備好建立追蹤時，請選擇 Create trail (建立追蹤)。
20. 新的追蹤會出現在 Trails (追蹤) 頁面上。大約 5 分鐘後，會 CloudTrail 發佈記錄檔，其中顯示您帳戶中發出的 AWS API 呼叫。您可以在所指定之 S3 儲存貯體中看到日誌檔案。如果您已啟用 Insights 事件記錄，且偵測到異常活動，則傳遞第一個 Insights 事件最多可能需 CloudTrail 要 36 小時的時間。

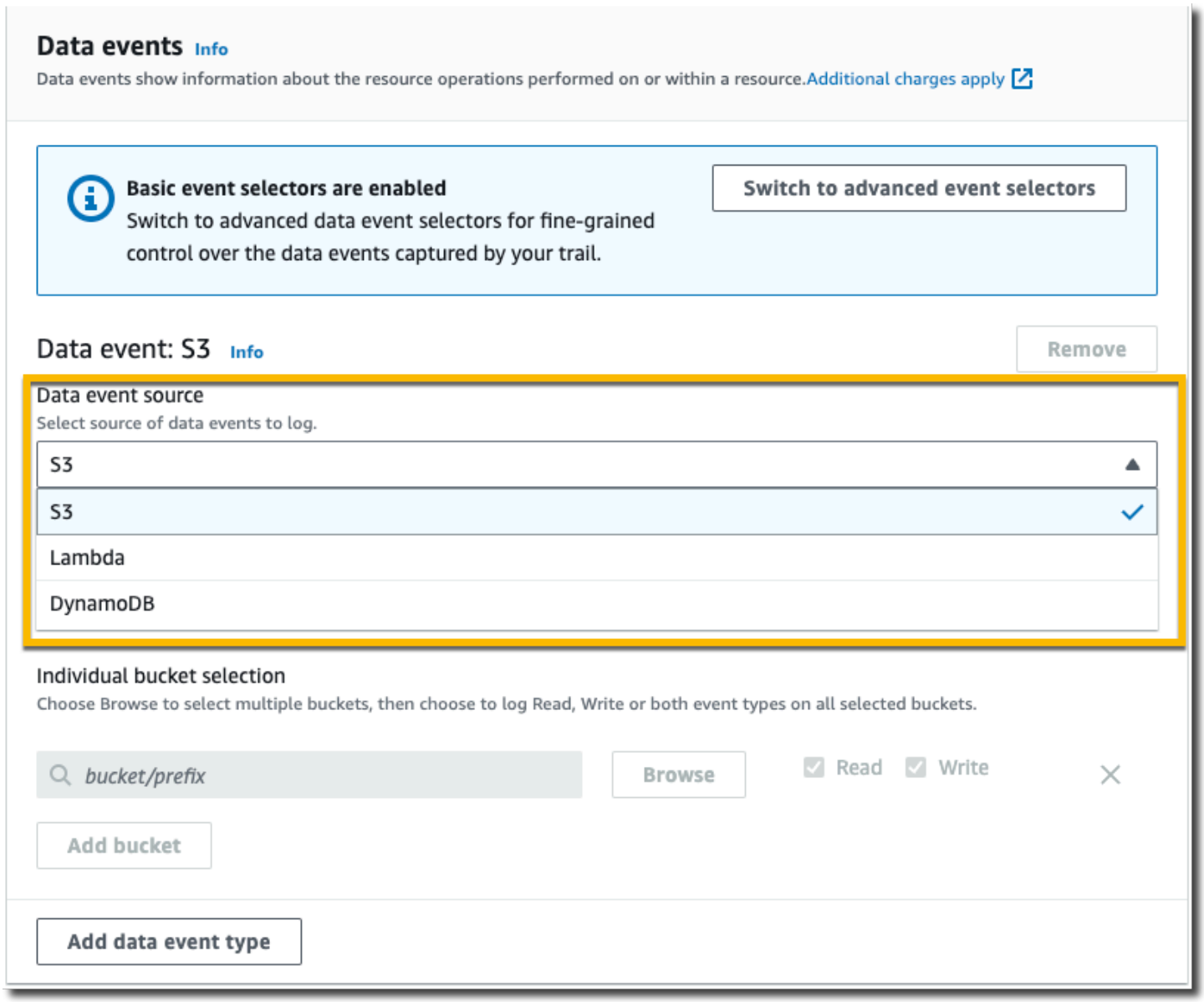
> **Note**
>
> CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內提供記錄檔。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。

如果您錯誤設定追蹤 (例如，無法連線 S3 儲存貯體)， CloudTrail 將嘗試將日誌檔重新傳送到 S3 儲存貯體 30 天，而且這些 attempted-to-deliver 事件將收取標準費用。CloudTrail 若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

使用基本事件選取器執行資料事件設定

您可以使用進階事件選取器來設定所有資料事件類型。進階事件選取器可讓您建立精細的選取器，以僅記錄感興趣的事件。

如果您使用基本事件選取器來記錄資料事件，則只能記錄 Amazon S3 儲存貯體、 AWS Lambda 函數和 Amazon DynamoDB 表的資料事件。您無法使用基本事件選取器篩選`eventName`欄位。



使用以下程序，透過基本事件選取器執行資料事件設定。

若要使用基本事件選取器執行資料事件設定

1. 在事件中，選擇資料事件以記錄資料事件。記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。
2. 對於 Amazon S3 儲存貯體：

   a. 對於 Data source (資料來源)，請選擇 S3。

   b. 您可以選取記錄所有目前和未來的 S3 儲存貯體，也可以指定個別儲存貯體或函數。依預設，會記錄所有目前和未來 S3 儲存貯體的資料事件。

   > **Note**
   >
   > 保留預設的 [所有目前和 future 的 S3 儲存貯體] 選項，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何 IAM 身分執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的值區上執行也一樣。
   >
   > 如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，選擇 [所有目前和 future 的 S3 儲存貯體] 會啟用與追蹤相同區域中的所有儲存貯體的資料事件記錄，以及稍後在該區域中建立的任何儲存貯體的資料事件記錄。它不會記錄帳戶中其他區域中 Amazon S3 儲存貯體的 AWS 資料事件。

   c. 如果您保留預設值，所有目前和未來的 S3 儲存貯體，選擇記錄讀事件、寫事件，或兩者。

   d. 若要選擇個別儲存貯體，請清空所有目前和未來的 S3 儲存貯體的讀和寫核取方塊。在個別儲存貯體選擇中，瀏覽要記錄資料事件的儲存貯體。透過輸入您想要的儲存貯體前綴來查找特定的儲存貯體。您可以在此視窗中選取多個儲存貯體。選擇新增儲存貯體以記錄更多儲存貯體的資料事件。選擇記錄 Read (讀取) 事件 (例如 `GetObject`)、Write (寫) 事件 (例如 `PutObject`) 還是兩者。

      此設定的優先順序高於您針對個別儲存貯體所設定的個別設定。例如，如果您指定記錄所有 S3 儲存貯體之 Read (讀取) 事件，然後選擇新增要記錄資料事件的特定儲存貯體，則您新增的儲存貯體會直接選取 Read (讀取)。您無法清除選取項目。您只能設定 Write (寫入) 的選項。

      若要從記錄中移除儲存貯體，請選擇 X。
3. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。
4. 針對 Lambda 函數：

a. 針對資料事件來源中，選擇 Lambda。

b. 在 Lambda 函數中，選擇所有區域來記錄所有的 Lambda 函數，或者輸入函數作為 ARN以記錄特定函數的資料事件。

若要記錄 AWS 帳戶中所有 Lambda 函數的資料事件，請選取記錄所有目前和 future 的函數。此設定的優先順序高於您針對個別函數所設定的個別設定。皆會記錄所有函數，縱使未顯示全部的函數。

> **Note**
>
> 如果您要建立所有區域的追蹤，則此選取項目可針對下列函數啟用記錄資料事件：目前在您 AWS 帳戶中的所有函數，以及在您完成建立追蹤之後可能在任何區域中建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，此選項會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。
> 記錄所有功能的資料事件也可讓您記錄 AWS 帳戶中任何 IAM 身分所執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的函數上執行。

c. 如果您選擇輸入函數作為 ARN，請輸入 Lambda 函數的 ARN。

> **Note**
>
> 如果您的帳戶中有超過 15,000 個 Lambda 函數，則無法在建立追蹤時在 CloudTrail 主控台中檢視或選取所有函數。您仍然可以選取記錄所有函數的選項，縱使其未全部顯示。如果您要記錄特定函數之資料事件，則可以在得知該函數的 ARN 後手動加以新增。您也可以在主控台中完成追蹤的建立，然後使用 AWS CLI 和put-event-selectors命令為特定 Lambda 函數設定資料事件記錄。如需詳細資訊，請參閱 管理軌跡 AWS CLI。

5. 針對 DynamoDB 資料表：

a. 針對資料事件來源中，選擇 DynamoDB。

b. 在 DynamoDB 資料表選取中，選擇 Browse (瀏覽) 以選取表格，或貼到您有權存取的 DynamoDB 資料表的 ARN 中。DynamoDB 資料表 ARN 採用以下格式：

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

若要新增其他資料表，請選擇 Add row (新增資料列)，然後瀏覽資料表或貼上您可以存取之資料表的 ARN。

6. 若要為您的追蹤設定 Insights 事件和其他設定，請返回本主題中的上述程序 ???。

後續步驟

在您建立追蹤之後，即可返回追蹤以進行變更：

- 如果您還沒有，您可以設定 CloudTrail 將記錄檔傳送至 CloudWatch 記錄檔。如需詳細資訊，請參閱 將事件傳送至 CloudWatch 記錄檔。
- 在 Amazon Athena 中建立資料表並用以執行查詢，以分析 AWS 服務活動。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的 CloudTrail 主控台中的為 CloudTrail 日誌建立表格。
- 將自訂標籤 (鍵/值對) 新增至追蹤。
- 若要建立另一個追蹤，請打開追蹤頁面，然後選擇建立追蹤。

更新追蹤

本節將描述如何變更追蹤設定。

若要更新單一區域追蹤以記錄您正在使用之AWS 分割區中的所有 AWS 區域 事件，或更新多區域追蹤以僅記錄單一區域中的事件，您必須使用. AWS CLI如需有關如何更新單一區域追蹤以記錄所有區域中事件的詳細資訊，請參閱 將套用至一個區域的追蹤轉換成套用至所有區域。如需有關如何更新多區域追蹤以記錄單一區域中事件的詳細資訊，請參閱 將多區域追蹤轉換成單一區域追蹤。

如果您已在 Amazon Security Lake 中啟用 CloudTrail 管理事件，則必須至少維護一個多區域的組織追蹤，並記錄`read`和`write`管理事件。您不能以不符合 Security Lake 要求的方式更新合格的追蹤。例如，透過將追蹤變更為單一區域，或關閉記錄 `read` 或 `write` 管理事件。

> **Note**
>
> CloudTrail 即使資源驗證失敗，也會更新成員帳號中的組織追蹤。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 存儲桶政策
> - 不正確的 Amazon SNS 主題政策
> - 無法傳遞至 CloudWatch 記錄檔記錄群組
> - 使用 KMS 金鑰加密權限不足

具有 CloudTrail 權限的成員帳戶可以在 CloudTrail 主控台上檢視追蹤的詳細資料頁面或執行 AWS CLI get-trail-status命令，來查看組織追蹤的任何驗證失敗。

使用更新系統線 AWS Management Console

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇追蹤，然後選擇追蹤名稱。
3. 在 General details (一般詳細資訊) 中，選擇 Edit (編輯) 變更下列設定。您無法變更追蹤的名稱。
   - 將追蹤套用至我的組織-變更此追蹤是否為 AWS Organizations 組織追蹤。

     Note

     只有組織的管理帳戶可以將組織追蹤轉換為非組織追蹤，或將非組織追蹤轉換為組織追蹤。
   - 追蹤日誌位置 - 變更您要存放此追蹤的日誌之 S3 儲存貯體名稱或前綴。
   - 日誌檔案 SSE-KMS 加密 -使用 SSE-KMS 而非 SSE-S3 來啟用或停用加密日誌檔案。
   - 日誌檔案驗證 - 選擇啟用或停用日誌檔案完整性的驗證。
   - SNS 通知傳遞 - 選擇啟用或停用日誌檔案已交付到針對追蹤指定的儲存貯體的 Amazon Simple Notification Service (Amazon SNS) 通知。

   a. 若要將追蹤變更為 AWS Organizations 組織追蹤，您可以選擇啟用組織中所有帳戶的追蹤。如需詳細資訊，請參閱 建立組織追蹤。

   b. 若要變更儲存位置中指定的儲存貯體，請選擇建立新 S3 儲存貯體來建立儲存貯體。建立值區時， CloudTrail 會建立並套用所需的值區政策。如果您選擇建立新的 S3 儲存貯體，您的 IAM 政策需要包含`s3:PutEncryptionConfiguration`動作的權限，因為預設情況下會為儲存貯體啟用伺服器端加密。

      Note

      如果您選擇使用現有的 S3 儲存貯體，請在追蹤記錄儲存貯體名稱中指定一個儲存貯體，或選擇 Browse (瀏覽) 以選擇儲存貯體。值區政策必須授 CloudTrail 予

寫入權限。如需手動編輯儲存貯體政策的資訊，請參閱「Amazon S3 存儲桶政策 CloudTrail」。

為了更輕鬆地找到您的日誌，請在現有存儲桶中創建一個新文件夾（也稱為前綴）以存儲 CloudTrail 日誌。在字首中輸入字首。

c. 針對 Log file SSE-KMS encryption (日誌檔案 SSE-KMS 加密)，如果您想要使用 SSE-KMS 而非 SSE-S3 來加密日誌檔案，請選擇 Enabled (啟用)。預設為啟用。如果您未啟用 SSE-KMS 加密，則會使用 SSE-S3 加密來加密您的日誌。如需 SSE-KMS 加密的詳細資訊，請參閱使用伺服器端加密搭配 AWS Key Management Service (SS E-KMS)。如需 SSE-S3 加密的詳細資訊，請參閱搭配使用伺服器端加密與 Amazon S3 受管加密金鑰 (SSE-S3)。

如果您啟用 SSE-KMS 加密，請選擇 [新增] 或 [現有]。 AWS KMS key在AWS KMS 別名中，以格式指定別名`alias/MyAliasName`。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。 CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

> **Note**
>
> 您也可以從另一個帳戶輸入金鑰的 ARN。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。金鑰原則必須允許 CloudTrail 使用金鑰來加密記錄檔，並允許您指定的使用者以未加密的形式讀取記錄檔。如需手動編輯金鑰政策的資訊，請參閱「設定 AWS KMS 金鑰原則 CloudTrail」。

d. 針對 Log file validation (日誌檔案驗證)，選擇 Enabled (啟用) 將日誌摘要交付到您的 S3 儲存貯體。您可以使用摘要檔來驗證記錄檔在 CloudTrail 傳送記錄檔之後是否未變更。如需詳細資訊，請參閱 驗證 CloudTrail 記錄檔完整性。

e. 對於 SNS 通知傳遞，請選擇 [啟用]，以便在每次將記錄傳送至儲存貯體時收到通知。CloudTrail 在記錄檔中儲存多個事件。SNS 通知是針對每個日誌檔案所傳送，而不是每個事件。如需詳細資訊，請參閱 設定 Amazon SNS 通知 CloudTrail。

如果您啟用 SNS 通知，針對建立新 SNS 主題，選擇 New (新的) 以建立主題，或選擇 Existing (現有) 以使用現有的主題。如果您要建立套用至所有區域的追蹤，則會將所有區域中日誌檔案傳遞的 SNS 通知都交付至您建立的單一 SNS 主題。

如果您選擇「新增」，請為您 CloudTrail 指定新主題的名稱，或者您也可以輸入名稱。如果選擇 Existing (現有),請從下拉式清單中選擇 SNS 主題。您也可以輸入來自另一個區域，或具有適當許可之帳戶的主題 ARN。如需詳細資訊，請參閱 Amazon SNS 主題政策 CloudTrail。

如果您建立主題，則必須訂閱該主題，以便在日誌檔案交付時收到通知。您可以從 Amazon SNS 主控台進行訂閱。基於通知頻率，建議您設定訂閱以利用 Amazon SQS 佇列，透過編寫程式的方式處理通知。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

4. 在「CloudWatch 記錄檔」中，選擇 「編輯」以變更將記 CloudTrail 錄檔傳送至 CloudWatch 記錄檔的設定。在CloudWatch 記錄檔中選擇「啟用」以啟用傳送記錄檔。如需詳細資訊，請參閱 將事件傳送至 CloudWatch 記錄檔。

   a. 如果您啟用與 CloudWatch 記錄整合，請選擇 [新增] 以建立新的記錄群組，或選擇 [現有] 使用現有的記錄群組。如果選擇 [新增]，請為您 CloudTrail 指定新記錄群組的名稱，或者輸入名稱。

   b. 如果選擇 Existing (現有)，請從下拉式清單中選擇日誌群組。

   c. 選擇 [新增]，為許可建立新的 IAM 角色，以便將記錄傳送至 CloudWatch 記錄。選擇 Existing (現有) 從下拉式功能表中選擇現有的 IAM 角色。新角色或現有角色的政策陳述式會在您展開政策文件時顯示。如需有關此角色的詳細資訊，請參閱 使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件。

   > **Note**
   >
   > - 設定追蹤時，您可以選擇由其他帳戶所屬的 S3 儲存貯體和 SNS 主題。不過，如果您想 CloudTrail 要將事件傳遞至 CloudWatch 記錄檔記錄群組，則必須選擇目前帳戶中存在的記錄群組。
   > - 只有管理帳戶可以使用主控台為組織追蹤設定 CloudWatch 記錄檔群組。委派的系統管理員可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 作業來設定 CloudWatch 記錄檔群組。

5. 在 Tags (標籤)中，選擇 Edit (編輯)，以變更、新增或刪除追蹤上的標籤。將一個或多個自訂標籤 (鍵/值對) 新增至追蹤。標籤可協助您識別 CloudTrail 追蹤和包含 CloudTrail 日誌檔的 Amazon S3 儲存貯體。然後，您可以將資源群組用於資 CloudTrail 源。如需更多詳細資訊，請參閱 AWS Resource Groups 及 標籤。

6. 在 Management events (管理事件) 中，選擇 Edit (編輯) 可變更管理事件記錄設定。

a. 針對 API 活動，選擇您是否希望追蹤記錄讀取事件、寫入事件，或兩者。如需詳細資訊，請參閱 管理事件。

b. 選擇「排除 AWS KMS 事件」，將 AWS Key Management Service (AWS KMS) 事件從追蹤中篩選出來。預設設定是包含所有 AWS KMS 事件。

   只有在追蹤記錄中記錄管理 AWS KMS 事件時，才能使用記錄或排除事件的選項。如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

   AWS KMS 動作，例如`Encrypt`、`Decrypt`、`GenerateDataKey`通常會產生大量 (超過 99%) 的事件。這些動作現在會記錄為 Read (讀取) 事件。低容量的相關 AWS KMS 動作，例如`DisableDelete`、和 `ScheduleKey` (通常佔 AWS KMS 事件磁碟區的 0.5% 以下) 會記錄為「寫入」事件。

   若要排除大量事件，例如 `Encrypt`、`Decrypt` 和 `GenerateDataKey`，但仍記錄相關事件，例如 `Disable`、`Delete` 和 `ScheduleKey`，選擇記錄 Write (寫入) 管理事件，然後清除 Exclude AWS KMS 事件的核取方塊。

c. 選擇排除 Amazon RDS Data API 事件從追蹤中篩選 Amazon Relational Database Service Data API 事件。預設設定是包含所有 Amazon RDS Data API 事件。如需 Amazon RDS Data API 事件的詳細資訊，請參閱《Amazon RDS 使用者指南 (Aurora)》中的使用 AWS CloudTrail記錄資料 API 呼叫。

7.

> **Important**
>
> 透過使用進階事件選取器執行步驟 7-11，可設定資料事件。進階事件選取器可讓您設定更多資料事件類型，並對追蹤擷取的資料事件提供精細控制。如果您使用的是基本事件選取器，請參閱 使用基本事件選取器更新資料事件設定，然後返回至此程序的步驟 12。

在 Data events (資料事件) 中，選擇 Edit (編輯) 可變更資料事件記錄設定。根據預設，追蹤不會記錄資料事件。記錄資料事件需支付額外的費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

針對資料事件類型，選擇您想要記錄資料事件的資源類型。如需有關可用資料事件類型的詳細資訊，請參閱 資料事件。

> **Note**
>
> 若要為 Lake Formation 成建立的 AWS Glue 表格記錄資料事件，請選擇 Lake Formation。

8. 選擇記錄選取器範本。 CloudTrail 包括記錄資源類型的所有資料事件的預先定義範本。若要建立自訂記錄選取器範本，請選擇 Custom (自訂)。

> **Note**
>
> 為 S3 儲存貯體選擇預先定義的範本，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的值區上執行。
>
> 如果追蹤僅套用至一個區域，選取預先定義的記錄所有 S3 儲存貯體的範本可針對下列儲存貯體啟用記錄資料事件：與您追蹤相同之區域中的所有儲存貯體，以及您稍後在該區域中建立的任何儲存貯體。並不會記錄 AWS 帳戶中其他區域內 Amazon S3 儲存貯體的資料事件。
>
> 如果您要為所有區域建立追蹤，請為 Lambda 函數選擇預先定義的範本，為 AWS 帳戶中目前的所有函數啟用資料事件記錄，以及在完成追蹤建立後可能在任何區域建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，此選項會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。
>
> 記錄所有函數的資料事件也可讓您記錄 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於其他 AWS 帳戶的函數上執行也一樣。

9. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。

10. 在 Advanced event selectors (進階事件選取器) 中，為您要收集資料事件的特定資源建置表達式。如果您使用預先定義的日誌範本，則可略過此步驟。

    a. 從下列欄位選取。

    - **`readOnly`**-`readOnly` 可以設定為等於`true`或的值`false`。若要同時記錄 `read` 和 `write` 事件，請勿新增 `readOnly` 選擇器。

- **eventName**-eventName可以使用任何運算子。您可以使用它來包含或排除記錄到的任何資料事件 CloudTrail，例如PutBucket或GetSnapshotBlock。
- **resources.ARN**-您可以將任何運算子搭配使用resources.ARN，但是如果您使用 equals 或不等於，則值必須完全符合您在範本中指定為值之類型之有效資源的 ARN。resources.type

  下表顯示每種 resources.type 的有效 ARN 格式。

  > **Note**
  >
  > 您無法使用resources.ARN欄位來篩選沒有 ARN 的資源類型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	resources.ARN
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	ARN 必須採用下列其中一種格式： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必須採用下列其中一種格式： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您指定 AWS::DynamoDB::Table 作為 resources.type，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在eventName欄位上新增篩選器。

[2] 若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 StartsWith 運算子，並僅包含儲存貯體 ARN 作為相符值。末尾斜線是有意保留，請勿排除。

[3] 若要在 S3 存取點中的所有物件上記錄事件，建議您僅使用存取點 ARN、不要包含物件路徑，並使用 StartsWith 或 NotStartsWith 運算子。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的動作、資源及條件金鑰。

b. 針對每個欄位，選擇 + 條件，視需要新增任意數目的條件，所有條件最多可指定 500 個值。例如，若要從追蹤記錄的資料事件中排除兩個 S3 儲存貯體的資料事件，您可以將欄位設定為 Resources.arn，將運算子設定為「不開始於」，然後貼上 S3 儲存貯體 ARN，或瀏覽您不想記錄事件的 S3 儲存貯體。

若要新增第二個 S3 儲存貯體，請選擇 + 條件，然後重複上述指令，在 ARN 中粘貼或瀏覽不同的儲存貯體。

> **Note**
>
> 追蹤上的所有選取器，您最多可以有 500 個值。這包括一個選擇器的多個值的陣列，如 `eventName`。如果所有選擇器都有單個值，則最多可以有 500 個條件新增至選擇器。
>
> 如果您的帳戶中有超過 15,000 個 Lambda 函數，則無法在建立追蹤時在 CloudTrail 主控台中檢視或選取所有函數。您仍然可以使用預先定義的選取器範本記錄所有函數，即使其未全部顯示。如果您要記錄特定函數之資料事件，則可以在得知該函數的 ARN 後手動加以新增。您也可以在主控台中完成追蹤的建立，然後使用 AWS CLI 和put-event-selectors命令為特定 Lambda 函數設定資料事件記錄。如需詳細資訊，請參閱 管理軌跡 AWS CLI。

c. 選擇 + 欄位以根據需要新增其他欄位。為避免發生錯誤，請勿為欄位設定衝突或重複的值。例如，不要在一個選擇器中指定 ARN 等於一個值，然後指定 ARN 不等於另一個選取器中的相同值。

11. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。重複步驟 3 到此步驟，以設定資料事件類型的進階事件選取器。
12. 如果您希望追蹤記錄見解事件，請在「 CloudTrail 見解」事件中選擇 「編輯」。

    在 Event type (事件類型) 中，選取 Insights 事件。

    在 Insights events (Insights 事件) 中，選擇 API call rate (API 呼叫率) 或 API error rate (API 錯誤率) (或兩者)。您必須記錄寫入管理事件，以便記錄 API 呼叫率的 Insights 事件。您必須記錄讀取或寫入管理事件，以便記錄 API 錯誤率的 Insights 事件。

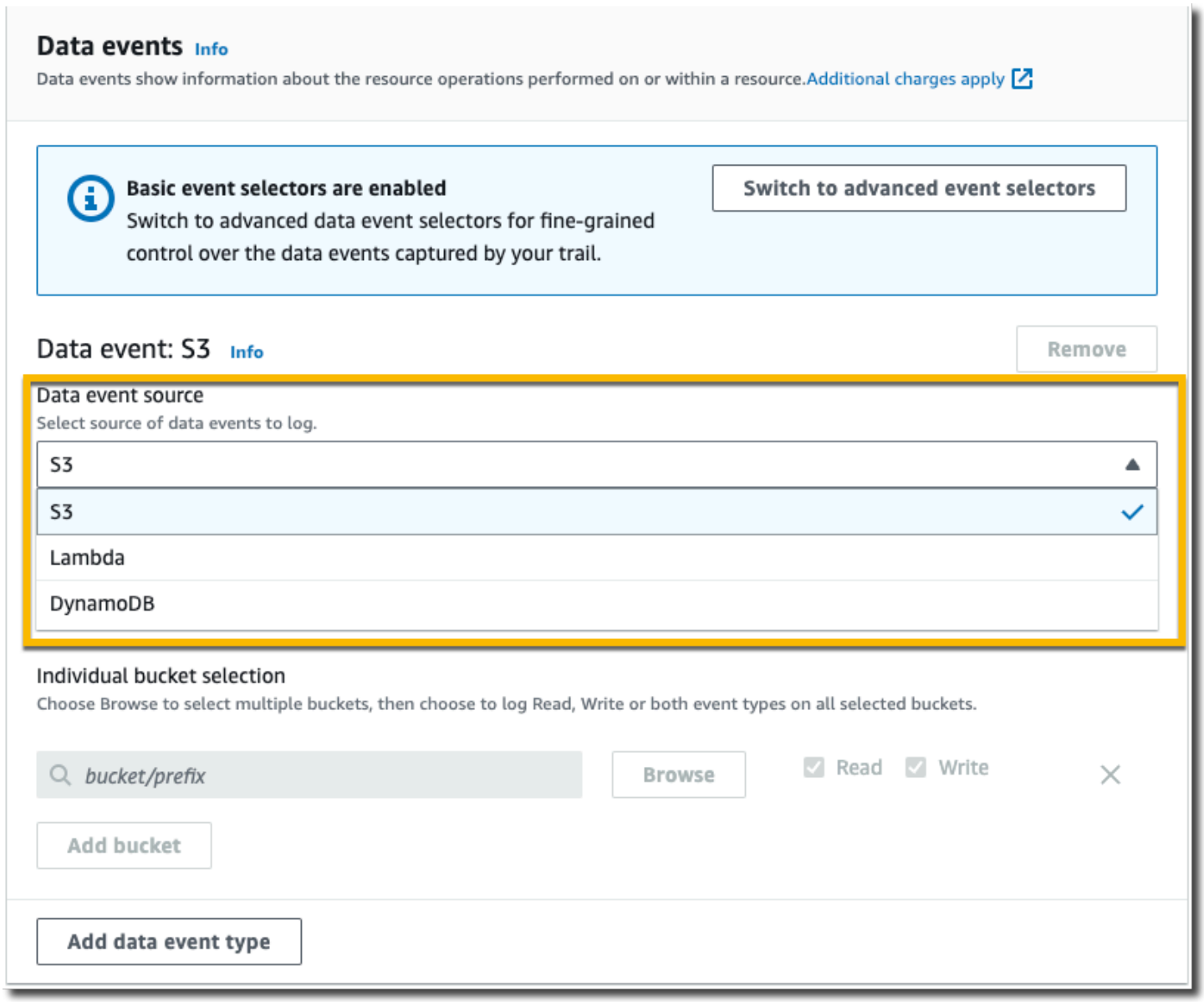
    CloudTrail Insights 會分析異常活動的管理事件，並在偵測到異常時記錄事件。依預設，追蹤不會記錄 Insights 事件。如需 Insights 事件的詳細資訊，請參閱記錄 Insights 事件。記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

    見解事件會傳遞到名為相同 S3 儲存貯體/`CloudTrail-Insight`的不同資料夾，該資料夾名稱為在追蹤詳細資料頁面的儲存位置區域中指定。 CloudTrail會為您建立新字首。例如，如果您目前的目的地 S3 儲存貯體名為 `S3bucketName/AWSLogs/CloudTrail/`，則具有新前綴的 S3 儲存貯體名稱會被命名為 `S3bucketName/AWSLogs/CloudTrail-Insight/`。
13. 完成變更追蹤的設定時，請選擇 Update trail (更新追蹤)。

使用基本事件選取器更新資料事件設定

您可以使用進階事件選取器來設定所有資料事件類型。進階事件選取器可讓您建立精細的選取器，以僅記錄感興趣的事件。

如果您使用基本事件選取器來記錄資料事件，則只能記錄 Amazon S3 儲存貯體、 AWS Lambda 函數和 Amazon DynamoDB 表的資料事件。您無法使用基本事件選取器篩選`eventName`欄位。



使用以下程序，透過基本事件選取器執行資料事件設定。

1. 在 Data events (資料事件) 中，選擇 Edit (編輯) 可變更資料事件記錄設定。使用基本事件選取器，您可以為 Amazon S3 儲存貯體、 AWS Lambda 函數、DynamoDBTables 或這些資源的組合指定記錄資料事件。進階事件選取器支援其他資料事件類型。根據預設，追蹤不會記錄資料事件。

記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 資料事件。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

對於 Amazon S3 儲存貯體：

a. 對於 Data source (資料來源)，請選擇 S3。

b. 您可以選取記錄所有目前和未來的 S3 儲存貯體，也可以指定個別儲存貯體或函數。依預設，會記錄所有目前和未來 S3 儲存貯體的資料事件。

> **Note**
>
> 保留預設的 [所有目前和 future 的 S3 儲存貯體] 選項，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於其他 AWS 帳戶的值區上執行的也一樣。
> 如果追蹤僅套用至一個區域，則選取 All current and future S3 buckets (所有目前和未來 S3 儲存貯體) 可針對下列儲存貯體啟用記錄資料事件：與您追蹤相同之區域中的所有儲存貯體，以及您稍後在該區域中建立的任何儲存貯體。它不會記錄帳戶中其他區域中 Amazon S3 儲存貯體的 AWS 資料事件。

c. 如果您保留預設值，所有目前和未來的 S3 儲存貯體，選擇記錄讀事件、寫事件，或兩者。

d. 若要選擇個別儲存貯體，請清空所有目前和未來的 S3 儲存貯體的讀和寫核取方塊。在個別儲存貯體選擇中，瀏覽要記錄資料事件的儲存貯體。若要尋找特定儲存貯體，請輸入所需儲存貯體的儲存貯體字首。您可以在此視窗中選取多個儲存貯體。選擇新增儲存貯體以記錄更多儲存貯體的資料事件。選擇記錄 Read (讀取) 事件 (例如 `GetObject`)、Write (寫) 事件 (例如 `PutObject`) 還是兩者。

   此設定的優先順序高於您針對個別儲存貯體所設定的個別設定。例如，如果您指定記錄所有 S3 儲存貯體之 Read (讀取) 事件，然後選擇新增要記錄資料事件的特定儲存貯體，則您新增的儲存貯體會直接選取 Read (讀取)。您無法清除選取項目。您只能設定 Write (寫入) 的選項。

   若要從記錄中移除儲存貯體，請選擇 X。

2. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。

3. 針對 Lambda 函數：

   a. 針對資料事件來源中，選擇 Lambda。

b. 在 Lambda 函數中，選擇所有區域來記錄所有的 Lambda 函數，或者輸入函數作為 ARN以記錄特定函數的資料事件。

若要記錄 AWS 帳戶中所有 Lambda 函數的資料事件，請選取記錄所有目前和 future 的函數。此設定的優先順序高於您針對個別函數所設定的個別設定。皆會記錄所有函數，縱使未顯示全部的函數。

> **Note**
>
> 如果您要為所有區域建立追蹤，此選項會啟用 AWS 帳戶中目前所有函數的資料事件記錄，以及在完成追蹤建立後可能在任何區域建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，此選項會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。記錄所有函數的資料事件也可讓您記錄 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於其他 AWS 帳戶的函數上執行也一樣。

c. 如果您選擇輸入函數作為 ARN，請輸入 Lambda 函數的 ARN。

> **Note**
>
> 如果您的帳戶中有超過 15,000 個 Lambda 函數，則無法在建立追蹤時在 CloudTrail 主控台中檢視或選取所有函數。您仍然可以選取記錄所有函數的選項，縱使其未全部顯示。如果您要記錄特定函數之資料事件，則可以在得知該函數的 ARN 後手動加以新增。您也可以在主控台中完成建立追蹤，然後使用 AWS CLI 和 put-event-selectors 命令為特定 Lambda 函數設定記錄資料事件。如需詳細資訊，請參閱 管理軌跡 AWS CLI。

4. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。
5. 針對 DynamoDB 資料表：

a. 針對資料事件來源中，選擇 DynamoDB。

b. 在 DynamoDB 資料表選取中，選擇 Browse (瀏覽) 以選取表格，或貼到您有權存取的 DynamoDB 資料表的 ARN 中。DynamoDB 資料表 ARN 採用以下格式：

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

若要新增其他資料表，請選擇 Add row (新增資料列)，然後瀏覽資料表或貼上您可以存取之資料表的 ARN。

6. 若要為您的追蹤設定 Insights 事件和其他設定，請返回本主題中的上述程序 更新追蹤。

刪除追蹤

您可以使用 CloudTrail 控制台刪除路徑。如果組織的管理帳戶或委派的管理員帳戶刪除了組織線索，則系統就會從組織的所有成員帳戶中移除線索。

如果您已在 Amazon Security Lake 中啟用 CloudTrail 管理事件，則必須至少維護一個多區域的組織追蹤，並記錄`read`和`write`管理事件。除非您關閉 Security Lake 中的 CloudTrail 管理事件，否則您只能刪除追蹤，如果它是您唯一符合此需求的追蹤。

使用 CloudTrail 主控台刪除追蹤

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 開啟主 CloudTrail 控台的 [追蹤] 頁面。
3. 選擇線索名稱。
4. 在線索詳細資訊頁面頂端，選擇 Delete (刪除)。
5. 出現提示要您確認刪除時，選擇 Delete (刪除) 以永久刪除線索。線索將會從線索清單中予以移除。將不會刪除已交付至 Amazon S3 儲存貯體的日誌檔案。

> **Note**
>
> 傳遞至 Amazon S3 儲存貯體的內容可能包含客戶內容。如需移除敏感資料的詳細資訊，請參閱 Amazon S3 使用者指南中的清空儲存貯體和刪除儲存貯體。

關閉記錄線索

當您建立線索時，會自動開啟記錄。您可以關閉記錄線索。

當您關閉記錄日誌時，現有的日誌仍然儲存在追蹤的 Amazon S3 儲存貯體中並繼續產生 S3 費用。

使用 CloudTrail 主控台關閉追蹤的記錄

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在左側導覽窗格中，選擇 Trails (線索)，然後選擇線索名稱。
3. 在線索詳細資訊頁面的上方，選擇 Stop logging (停止記錄) 關閉記錄線索。
4. 當系統提示您確認時，請選擇 [停止記錄]。 CloudTrail停止該追蹤的記錄活動。
5. 若要繼續記錄該線索，請選擇線索組態頁面上的 Start logging (開始記錄)。

建立、更新和管理追蹤 AWS CLI

您可以使 AWS CLI 用建立、更新和管理追蹤。使用時 AWS CLI，請記住您的命令會在為您的設定檔設定的 [AWS 區域] 中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

> **Note**
>
> 您需要命 AWS 令行工具來執行本主題中的 AWS Command Line Interface (AWS CLI) 命令。請確定您已 AWS CLI 安裝最新版本。如需詳細資訊，請參閱 AWS Command Line Interface 使用者指南。如需 CloudTrail 指令行中指 AWS CLI 令的說明，請鍵入`aws cloudtrail help`。

建立及管理追蹤的常用命令與狀態

在中建立和更新軌跡的一些較常用的指令 CloudTrail 包括：

- create-trail 可建立追蹤。
- update-trail 可變更現有追蹤的組態。
- add-tags 可新增一或多個標籤 (索引鍵/值組) 至現有追蹤。
- remove-tags 可從追蹤移除一或多個標籤。
- list-tags 可傳回與追蹤相關聯的標籤清單。
- put-event-selectors 可新增或修改追蹤的事件選取器。
- put-insight-selectors 以新增或修改現有追蹤的 Insights 事件選取器，以及啟用或停用 Insights 事件。

- start-logging 可開始使用追蹤記錄事件。
- stop-logging 可暫停使用追蹤記錄事件。
- delete-trail 可刪除追蹤。此命令不會刪除包含該追蹤日誌檔案的 Amazon S3 儲存貯體 (若有的話)。
- describe-trails返回有關 AWS 區域中軌跡的信息。
- get-trail 可傳回追蹤的設定資訊。
- get-trail-status 可傳回追蹤目前狀態的相關資訊。
- get-event-selectors 可傳回為追蹤設定的事件選取器相關資訊。
- get-insight-selectors 可傳回為追蹤設定的 Insights 事件選取器相關資訊。

建立及更新追蹤支援的命令：create-trail 與 update-trail

`create-trail` 和 `update-trail` 命令提供各種可用來建立及管理追蹤的功能，其中包括：

- 使用 `--is-multi-region-trail` 選項來建立跨區域接收日誌的追蹤，或是更新追蹤。在大多數情況下，您應該建立追蹤來記錄所有 AWS 區域中的事件。
- 創建一個跟踪，以接收帶有該--is-organization-trail選項的組織中所有 AWS 帳戶的日誌。
- 使用 `--no-is-multi-region-trail` 選項將多區域追蹤轉換成單一區域追蹤。
- 使用 `--kms-key-id` 選項來啟用或停用日誌檔案加密。此選項會指定您已建立的 AWS KMS 金鑰，以及您已附加可加密記錄 CloudTrail 的原則的金鑰。如需詳細資訊，請參閱 啟用和停用 CloudTrail 記錄檔加密 AWS CLI。
- 使用 `--enable-log-file-validation` 和 `--no-enable-log-file-validation` 選項來啟用或停用日誌檔案驗證。如需詳細資訊，請參閱 驗證 CloudTrail 記錄檔完整性。
- 指定 CloudWatch 記錄檔記錄群組和角色， CloudTrail 以便將事件傳遞至 CloudWatch 記錄檔記錄群組。如需詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。

廢除的命令：create-subscription 和 update-subscription

> **Important**
>
> `create-subscription` 和 `update-subscription` 命令先前可用來建立及更新追蹤，但已廢除。請勿使用這些命令，它們無法提供建立及管理追蹤的完整功能。
> 如果您設定為自動使用上述命令之一或兩者，建議您更新程式碼或指令碼，以使用 create-trail 等受支援的命令。

使用 create-trail

您可以執行 `create-trail` 命令來建立專為業務需求設定的追蹤。使用時 AWS CLI，請記住您的命令會在為您的設定檔設定的 [AWS 區域] 中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

建立套用至所有區域的追蹤

若要建立會套用至所有區域的追蹤，請使用 `--is-multi-region-trail` 選項。在預設情況下，`create-trail` 命令所建立的追蹤只會記錄該追蹤建立所在 AWS 區域中的事件。為了確保您記錄全域服務事件並擷取 AWS 帳戶中的所有管理事件活動，您應該建立追蹤以記錄所有 AWS 區域中的事件。

> **Note**
>
> 建立追蹤時，如果您指定的 Amazon S3 儲存貯體並非使用建立 CloudTrail，則需要附加適當的政策。請參閱Amazon S3 存儲桶政策 CloudTrail。

下列範例會建立名稱為 *my-trail* 的追蹤，以及索引鍵名稱為 *Group* 且具備 *Marketing* 值的標籤，藉此將所有區域的日誌交付至名為 *my-bucket* 的現有儲存貯體。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --tags-list [key=Group,value=Marketing]
```

若輸出中的 `IsMultiRegionTrail` 元素顯示 `true`，即可確定所有區域中皆有追蹤。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 使用 `start-logging` 命令來為追蹤啟動記錄功能。

啟動追蹤的記錄功能

`create-trail` 命令完成之後，請執行 `start-logging` 命令開始追蹤的記錄。

> **Note**
>
> 當您使用 CloudTrail 主控台建立追蹤時，會自動開啟記錄功能。

下列範例會為追蹤啟動記錄功能。

```
aws cloudtrail start-logging --name my-trail
```

此命令不會傳回輸出，但您可以使用 `get-trail-status` 命令來確認記錄功能已啟動。

```
aws cloudtrail get-trail-status --name my-trail
```

若輸出中的 `IsLogging` 元素顯示 `true`，即可確定追蹤正在進行記錄。

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

建立單一區域追蹤

下列命令會建立單一區域追蹤。指定的 Amazon S3 儲存貯體必須已經存在，並已套用適當的 CloudTrail 許可。如需詳細資訊，請參閱 Amazon S3 存儲桶政策 CloudTrail。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

如需詳細資訊，請參閱 命名要求。

下列為範例輸出。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

建立套用至所有區域且已啟用日誌檔案驗證的追蹤

若要在使用 create-trail 時啟用日誌檔案驗證，請使用 --enable-log-file-validation 選項。

如需日誌檔案驗證的相關資訊，請參閱驗證 CloudTrail 記錄檔完整性。

下列範例所建立的追蹤會將所有區域的日誌交付至指定儲存貯體。此命令會採用 --enable-log-file-validation 選項。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-region-trail --enable-log-file-validation
```

若輸出中的 LogFileValidationEnabled 元素顯示 true，即可確定日誌檔案驗證已啟用。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

使用 update-trail

> **Important**
>
> 截至 2021 年 11 月 22 日，AWS CloudTrail 改變了追蹤捕捉全球服務事件的方式。現在，由 Amazon 建立的事件 CloudFront AWS Identity and Access Management，並記錄 AWS STS 在其建立的區域，美國東部 (維吉尼亞北部) 區域 us-east-1。這使得這 CloudTrail 些服務如何與其他 AWS 全球服務一致。若要繼續接收美國東部 (維吉尼亞北部) 以外的全域服務事件，請務必將使用美國東部 (維吉尼亞北部) 以外全域服務事件的單一區域追蹤轉換為多區域追蹤。如需擷取全球服務事件的詳細資訊，請參閱本節下文的「啟用及停用全球服務事件記錄」。相反，CloudTrail 控制台中的事件歷史記錄和aws cloudtrail lookup-events命令將顯示這些事件發生的 AWS 區域 位置。

您可以使用 `update-trail` 命令來變更追蹤的組態設定。您也可以使用 add-tags 和 remove-tags 命令來新增及移除追蹤的標籤。您只能從建立系統線的「 AWS 區域」(其「居住區域」) 更新系統線。使用時 AWS CLI，請記住您的命令會在為您的設定檔設定的 [AWS 區域] 中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

如果您已在 Amazon Security Lake 中啟用 CloudTrail 管理事件，則必須至少維護一個多區域的組織追蹤，並記錄`read`和`write`管理事件。您不能以不符合 Security Lake 要求的方式更新合格的追蹤。例如，透過將追蹤變更為單一區域，或關閉記錄 `read` 或 `write` 管理事件。

> **Note**
>
> 如果您使用 AWS CLI 或其中一個 AWS SDK 修改追蹤，請確定追蹤的值區原則為 up-to-date。為了讓您的值區自動接收來自新的事件 AWS 區域，策略必須包含完整的服務名稱`cloudtrail.amazonaws.com`。如需詳細資訊，請參閱 Amazon S3 存儲桶政策 CloudTrail。

主題

將套用至一個區域的追蹤轉換成套用至所有區域

若要變更現有的追蹤，使該追蹤套用至所有區域，請使用 --is-multi-region-trail 選項。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

若輸出中的 IsMultiRegionTrail 元素顯示 true，即可確定追蹤現會套用至所有區域。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

將多區域追蹤轉換成單一區域追蹤

若要變更現有的多區域追蹤，使該追蹤只會套用至其建立所在的區域，請使用 --no-is-multi-region-trail 選項。

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

若輸出中的 IsMultiRegionTrail 元素顯示 false，即可確定追蹤現會套用至單一區域。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

啟用及停用全球服務事件記錄

若要變更追蹤以停止記錄全域服務事件，請使用 --no-include-global-service-events 選項。

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

若輸出中的 IncludeGlobalServiceEvents 元素顯示 false，即可確定追蹤不會再記錄全域服務事件。

```
{
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

若要變更追蹤以記錄全域服務事件，則可使用 --include-global-service-events 選項。

自 2021 年 11 月 22 日起，單一區域追蹤將不再接收全域服務事件，除非追蹤在這之前已出現於美國東部 (維吉尼亞北部) 區域 (us-east-1)。若要繼續擷取全域服務事件，請將追蹤組態更新為多區域追蹤。例如，此命令會將美國東部 (俄亥俄) (us-east-2) 中的單一區域追蹤更新為多區域追蹤。將 *myExistingSingleRegionTrailWithGSE* 取代為您的組態適當的追蹤名稱。

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

由於自 2021 年 11 月 22 日起，全域服務事件僅能在美國東部 (維吉尼亞北部) 提供，因此您也可以建立單一區域追蹤，訂閱美國東部 (維吉尼亞北部) 區域 (us-east-1) 的全域服務事件。下列命令會在 us-east-1 中建立單一區域追蹤，以接收 CloudFront、IAM 和事件： AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

啟用日誌檔案驗證

若要啟用追蹤的日誌檔案驗證，請使用 --enable-log-file-validation 選項。這會將摘要檔案交付到該追蹤的 Amazon S3 儲存貯體。

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

若輸出中的 LogFileValidationEnabled 元素顯示 true，即可確定日誌檔案驗證已啟用。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

停用日誌檔案驗證

若要停用追蹤的日誌檔案驗證，請使用 --no-enable-log-file-validation 選項。

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

若輸出中的 LogFileValidationEnabled 元素顯示 false，即可確定日誌檔案驗證已停用。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

若要使用驗證記錄檔 AWS CLI，請參閱驗證 CloudTrail 記錄檔完整性 AWS CLI。

管理軌跡 AWS CLI

AWS CLI 包括其他幾個可協助您管理路徑的指令。這些命令可用來將標籤新增至追蹤、取得追蹤狀態、啟動和停止追蹤的記錄功能，以及刪除追蹤。您必須從建立系統線的相同 AWS 區域 (其「主區域」) 執行這些指令。使用時 AWS CLI，請記住您的命令會在為您的設定檔設定的 [AWS 區域] 中執行。如果您想在不同區域中執行命令，則可變更設定檔的預設區域，或搭配 --region 參數使用命令。

主題

- 新增一或多個標籤至追蹤
- 列出一或多個追蹤的標籤

- 從追蹤移除一或多個標籤
- 擷取追蹤設定和追蹤狀態
- 設定 CloudTrail 深入解析事件選取器
- 設定事件選取器
- 設定進階事件選取器
- 停止及啟動追蹤的記錄功能
- 刪除追蹤

新增一或多個標籤至追蹤

若要將一或多個標籤新增至現有的追蹤，請執行 add-tags 命令。

下列範例會將名稱為 *Owner* (擁有者) 和值為 *Mary* 的標籤新增至美國東部 (俄亥俄) 區域 ARN 為 *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* 的追蹤。

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

若成功，此命令不會傳回任何內容。

列出一或多個追蹤的標籤

若要檢視與一或多個現有追蹤相關聯的標籤，請使用 list-tags 命令。

下列範例會列出 *Trail1* 和 *Trail2* 的標籤。

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

如果成功，此命令傳回的輸出會類似如下。

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "Name"
             },
```

```
            {
                "Value": "Ohio",
                "Key": "Location"
            }
        ]
    },
    {
        "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
        "TagsList": [
            {
                "Value": "Bob",
                "Key": "Name"
            }
        ]
    }
  ]
}
```

從追蹤移除一或多個標籤

若要從現有的追蹤移除一或多個標籤，請執行 remove-tags 命令。

下列範例為從美國東部 (俄亥俄) 區域中 ARN 為 *arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1* 的追蹤中移除名稱為 *Location* (位置) 和 *Name* (名稱) 的標籤。

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

若成功，此命令不會傳回任何內容。

擷取追蹤設定和追蹤狀態

執行命describe-trails令以擷取有關「 AWS 區域」中軌跡的資訊。下列範例會傳回美國東部 (俄亥俄) 區域中所設定追蹤的相關資訊。

```
aws cloudtrail describe-trails --region us-east-2
```

如果成功，您會看到類似如下的輸出。

```
{
  "trailList": [
```

```
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
    }
  ]
}
```

執行 `get-trail` 命令來擷取有關特定追蹤的設定資訊。下列範例會傳回名為 *my-trail* 的設定資訊。

```
aws cloudtrail get-trail - -name my-trail
```

如果成功，此命令傳回的輸出會類似如下。

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

若要擷取追蹤的狀態，請執行 `get-trail-status` 命令。您必須從建立該指令的「 AWS 區域」(「主區域」) 執行此指令，或者您必須透過新增--region參數來指定該「區域」。

> **Note**
>
> 如果追蹤檔是組織追蹤檔，而您是中組織中的成員帳戶 AWS Organizations，您必須提供該追蹤的完整 ARN，而不只是名稱。

```
aws cloudtrail get-trail-status --name my-trail
```

如果成功，您會看到類似如下的輸出。

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
```

```
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

如果發生 Amazon SNS 或 Amazon S3 錯誤，則除了上述 JSON 程式碼中所示的欄位外，狀態還會包含下列欄位：

- `LatestNotificationError` 包含主題訂閱失敗時由 Amazon SNS 發出的錯誤。
- `LatestDeliveryError`。 包含 Amazon S3 在無 CloudTrail 法將日誌檔交付至儲存貯體時發出的錯誤訊息。

設定 CloudTrail 深入解析事件選取器

執行 put-insight-selectors，並指定 `ApiCallRateInsight`、`ApiErrorRateInsight` (或兩者) 為 `InsightType` 屬性值，以啟用追蹤上的 Insights 事件。若要檢視追蹤的 Insights 選取器設定，請執行 `get-insight-selectors` 命令。您必須從建立軌跡的「 AWS 區域」(「主區域」) 執行此指令，或者您必須透過將--region參數加入至指令來指定「區域」。

> **Note**
>
> 若要記錄 `ApiCallRateInsight` 的 Insights 事件，追蹤必須記錄 `write` 管理事件。若要記錄 `ApiErrorRateInsight` 的 Insights 事件，追蹤必須記錄 `read` 或 `write` 管理事件。

記錄 Insights 事件的範例追蹤

下列範例會用put-insight-selectors來為名為 *`TrailName3`* 的追蹤建立 Insights 事件選取器。這會啟用 *`TrailName3`* 個追蹤的深入解析事件收集。Insights 事件選取器會記錄 `ApiErrorRateInsight` 和 `ApiCallRateInsight` Insights 事件類型。

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

此範例會傳回為追蹤設定的 Insights 事件選取器。

```
{
   "InsightSelectors":
```

```
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

範例：關閉收集 Insights 事件

下列範例會用put-insight-selectors來移除名為 *TrailName3* 之追蹤的 Insights 事件選取器。清除深入解析選取器的 JSON 字串會停用 *TrailName3* 個追蹤的深入解析事件收集。

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

此範例會傳回為追蹤設定的目前空白 Insights 事件選取器。

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

設定事件選取器

若要檢視追蹤的事件選取器設定，請執行 `get-event-selectors` 命令。您必須從建立該指令的「 AWS 區域」(「主區域」) 執行此指令，或者必須使用--region參數指定該「區域」。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 如果追蹤檔是組織追蹤檔，而您是中組織中的成員帳戶 AWS Organizations，您必須提供該追蹤的完整 ARN，而不只是名稱。

下列範例會傳回追蹤之事件選取器的預設設定。

```
{
```

```
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要建立事件選取器，請執行 `put-event-selectors` 命令。如果您希望在追蹤上記錄 Insights 事件，請確保事件選取器啟用記錄您想要設定追蹤的 Insights 類型。如需有關記錄 Insights 事件的詳細資訊，請參閱 記錄 Insights 事件。

當您的帳戶中發生事件時，請 CloudTrail 評估追蹤的組態。如果事件符合追蹤的任何事件選取器，則追蹤會處理並記錄該事件。一個追蹤最多可以設定 5 個事件選取器和 250 個資料資源。如需詳細資訊，請參閱記錄資料事件。

主題

- 使用特定事件選取器的範例追蹤
- 記錄所有管理和資料事件的範例追蹤
- 不記錄 AWS Key Management Service 事件的範例追蹤
- 記錄相關小量事件的範例追蹤 AWS Key Management Service
- 不會記錄 Amazon RDS Data API 事件的範例追蹤

使用特定事件選取器的範例追蹤

下列範例會為名為的追蹤建立事件選取器，*TrailName*以包含唯讀和唯寫管理事件、兩個 Amazon S3 儲存貯體/前置詞組合的資料事件，以及單一名為的函數的資料事件。 AWS Lambda *hello-world-python-function*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix","arn:aws:s3:::mybucket2/prefix2"]},{"Type": "AWS::Lambda::Function","Values":
 ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]}]}]'
```

此範例會傳回為追蹤設定的事件選取器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

記錄所有管理和資料事件的範例追蹤

下列範例會為名為 *TrailName2* 的追蹤建立事件選取器，其中包括帳戶中所有 Amazon S3 儲存貯體、函數和 Amazon DynamoDB 表的所有事件，包括唯讀和唯寫管理事件，以及所有 Amazon S3 儲存貯體、 AWS Lambda 函數和 Amazon DynamoDB 表格的所有資料事件。 AWS 由於此範例使用基本事件選取器，因此無法設定 S3 事件 AWS Outposts、以太坊節點上的 Amazon Managed Blockchain JSON-RPC 呼叫或其他進階事件選取器資源類型的記錄。您必須使用進階事件選取器來記錄這些資源的資料事件。如需詳細資訊，請參閱設定進階事件選取器。

> **Note**
>
> 如果追蹤僅套用至一個區域，就只會記錄該區域的事件，即使事件選取器參數指定所有 Amazon S3 儲存貯體和 Lambda 函數也一樣。事件選取器只會套用至建立追蹤的區域。

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

此範例會傳回為追蹤設定的事件選取器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

不記錄 AWS Key Management Service 事件的範例追蹤

下列範例會為名*TrailName*為包含唯讀和唯寫管理事件但排除 AWS Key Management Service (AWS KMS) 事件的追蹤建立事件選取器。由於 AWS KMS 事件會被視為管理事件，而且可能會有大量事件，因此如果您有多個追蹤可擷取管理事件的追蹤，這些事件可能會對 CloudTrail 帳單產生重大影響。此範例中的使用者已選擇從每個追蹤中排除 AWS KMS 事件，只有一個例外。若要排除事件來源，請將 ExcludeManagementEventSources 加入事件選取器，並在字串值中指定事件來源。

如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

若要再次開始記錄 AWS KMS 事件至追蹤，請傳遞空白陣列做為的值ExcludeManagementEventSources。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

此範例會傳回為追蹤設定的事件選取器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要再次開始記錄 AWS KMS 事件至追蹤，請傳遞一個空陣列做為的值ExcludeManagementEventSources，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

記錄相關小量事件的範例追蹤 AWS Key Management Service

下列範例會為名為包含唯寫管理事件和 AWS KMS 事*TrailName*件的追蹤建立事件選取器。由於 AWS KMS 事件會被視為管理事件，而且可能會有大量事件，因此如果您有多個追蹤可擷取管理事件的追蹤，這些事件可能會對 CloudTrail 帳單產生重大影響。此範例中的使用者已選擇包含「 AWS KMS 寫入」事件，這些事件將包括DisableScheduleKey、Delete和，但不再包含大量動作，例如EncryptDecrypt、和 GenerateDataKey (現在這些動作視為「讀取」事件)。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

此範例會傳回為追蹤設定的事件選取器。這會記錄唯寫管理事件，包括 AWS KMS 事件。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

不會記錄 Amazon RDS Data API 事件的範例追蹤

下列範例會為名為的追蹤建立事件選取器，*TrailName*以包含唯讀和唯寫管理事件，但排除 Amazon RDS Data API 事件。由於 Amazon RDS Data API 事件被視為管理事件，並且可能存在大量事件，因此如果您有多個追蹤可擷取管理事件的追蹤，這些事件可能會對您的 CloudTrail 帳單產生重大影響。此範例中的使用者已選擇從每個追蹤中排除 Amazon RDS Data API 事件，只有一個例外。若要排除事件來源，請將 ExcludeManagementEventSources 加入事件選取器，並在字串值 rdsdata.amazonaws.com 中指定事件 Amazon RDS Data API 來源。

如果您選擇不記錄管理事件，Amazon RDS Data API 事件不會記錄，而且您無法變更事件記錄設定。

若要開始將 Amazon RDS 資料 API 管理事件再次記錄到追蹤，請傳遞一個空陣列作為的值ExcludeManagementEventSources。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

此範例會傳回為追蹤設定的事件選取器。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要開始將 Amazon RDS 資料 API 管理事件再次記錄到追蹤，請傳遞一個空陣列作為的值`ExcludeManagementEventSources`，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

設定進階事件選取器

若要使用進階事件選取器來包含或排除資料事件，而非基本事件選取器，請在追蹤詳細資訊頁面上使用進階事件選取器。相較於基本事件選取器，進階事件選取器可讓您針對更多資源類型記錄資料事件。基本選取器可記錄 S3 物件活動， AWS Lambda 函數執行活動和 DynamoDB 資料表。

在進階事件選取器中，建立運算式以收集特定資源類型的資料事件，例如 S3 儲存貯體、 AWS Lambda 函數、DynamoDB 表、S3 物件 Lambda 存取點、EBS 快照上的 Amazon EBS 直接 API、S3 存取點、DynamoDB 串流、Lake Formation 建立的 AWS Glue 表格等。

如需進階事件選取器的詳細資訊，請參閱設定進階事件選取器。

若要檢視進階事件選取器的追蹤設定，請執行以下 `get-event-selectors` 命令。您必須從建立軌跡的「 AWS 區域」(「主區域」) 執行此指令，或者您必須透過新增--region參數來指定該「區域」。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 如果追蹤檔是組織追蹤，且您使用中組織中的成員帳戶登入 AWS Organizations，則您必須提供追蹤的完整 ARN，而不只是名稱。

下列範例會傳回追蹤之進階事件選取器的預設設定。依預設，不會針對追蹤設定進階事件選取器。

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要建立進階事件選取器，請執行 `put-event-selectors` 命令。當您的帳戶中發生資料事件時，請 CloudTrail 評估追蹤的組態。如果事件符合追蹤的任何進階事件選取器，則追蹤會處理並記錄該事件。您可以在追蹤上設定多達 500 個條件，包括為追蹤上所有進階事件選取器指定的所有值。如需詳細資訊，請參閱 記錄資料事件。

主題

- 使用特定進階事件選取器的範例追蹤
- 使用自訂進階事件選取器在 AWS Outposts 資料事件上記錄 Amazon S3 的範例追蹤
- 使用進階事件選取器排除 AWS Key Management Service 事件的範例追蹤
- 使用進階事件選取器排除 Amazon RDS 資料 API 管理事件的追蹤範例

使用特定進階事件選取器的範例追蹤

下列範例會為名*TrailName*為包含讀取和寫入管理事件的追蹤建立自訂進階事件選取器 (透過省略選`readOnly`取器)，以`PutObject`及所有 Amazon S3 儲存貯體/前置詞組合的`DeleteObject`資料事件 (名為的儲存貯體`sample_bucket_name`和名為函數的資料事件除外) 建立資料事件。 AWS Lambda `MyLambdaFunction`因為這些都是自訂進階事件選取器，所以每組選取器都有一個描述性的名稱。請注意，尾步斜線是 S3 儲存貯體 ARN 值的一部分。

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
```

```
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

範例傳回針對追蹤設定的進階事件選取器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
```

```
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

使用自訂進階事件選取器在 AWS Outposts 資料事件上記錄 Amazon S3 的範例追蹤

下列範例顯示如何設定追蹤，以便在前哨站的 AWS Outposts 物件上包含所有 Amazon S3 的所有資料事件。在此版本中，欄位 AWS Outposts 事件上 S3 支援的`resources.type`值為`AWS::S3Outposts::Object`。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
```

```
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

命令會傳回下列範例輸出。

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

使用進階事件選取器排除 AWS Key Management Service 事件的範例追蹤

下列範例會針對名*TrailName*為包含唯讀和唯寫管理事件的追蹤建立進階事件選取器 (藉由省略`readOnly`選取器)，但要排除 AWS Key Management Service (AWS KMS) 事件。由於 AWS KMS 事件會被視為管理事件，而且可能會有大量事件，因此如果您有多個追蹤可擷取管理事件的追蹤，這些事件可能會對 CloudTrail 帳單產生重大影響。

如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

若要再次開始將 AWS KMS 事件記錄到追蹤，請移除eventSource選取器，然後再次執行命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

範例傳回針對追蹤設定的進階事件選取器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要再次開始記錄排除的事件至追蹤，請從移除 eventSource 選取器，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
```

```
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

使用進階事件選取器排除 Amazon RDS 資料 API 管理事件的追蹤範例

下列範例會為名*TrailName*為包含唯讀和唯寫管理事件的追蹤建立進階事件選取器 (透過省略`readOnly`選取器)，但排除 Amazon RDS Data API 管理事件。若要排除 Amazon RDS 資料 API 管理事件，請在以下`eventSource`欄位的字串值中指定 Amazon RDS 資料 API 事件來源：`rdsdata.amazonaws.com`

如果您選擇不記錄管理事件，則不會記錄 Amazon RDS 資料 API 管理事件，而且您無法變更 Amazon RDS 資料 API 事件記錄設定。

若要重新開始將 Amazon RDS 資料 API 管理事件記錄到追蹤，請移除`eventSource`選取器，然後再次執行命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

範例傳回針對追蹤設定的進階事件選取器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
```

```
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要再次開始記錄排除的事件至追蹤，請從移除 eventSource 選取器，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

停止及啟動追蹤的記錄功能

以下命令啟動和停止 CloudTrail 記錄。

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> 您需要執行 stop-logging 命令，停止將事件交付至儲存貯體，才能刪除該儲存貯體。如果您不停止記錄，請 CloudTrail 嘗試在有限的時間內將記錄檔傳送至具有相同名稱的值區。
> 如果您停止記錄或刪除追蹤，就會停用該追蹤上的 CloudTrail 深入解析。

刪除追蹤

如果您已在 Amazon Security Lake 中啟用 CloudTrail 管理事件，則必須至少維護一個多區域的組織追蹤，並記錄`read`和`write`管理事件。除非您關閉 Security Lake 中的 CloudTrail 管理事件，否則您只能刪除追蹤，如果它是您唯一符合此需求的追蹤。

您可以使用下列命令來刪除追蹤。您只能刪除追蹤建立所在區域 (主區域) 中的追蹤。

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

當您刪除追蹤時，並不會刪除相關聯的 Amazon S3 儲存貯體或 Amazon SNS 主題。使用 AWS Management Console AWS CLI、或服務 API 分別刪除這些資源。

建立組織追蹤

如果您已在中建立組織 AWS Organizations，則可以建立追蹤來記錄該組織 AWS 帳戶 中所有人的所有事件。這有時稱為組織追蹤。

組織的管理帳戶可以指派委派的管理員來建立新的組織追蹤，或管理現有的組織追蹤。如需新增委派的管理員的詳細資訊，請參閱 新增 CloudTrail 委派管理員。

組織的管理帳戶可以編輯其帳戶中的現有追蹤，並將其套用到組織，使其成為組織追蹤。組織追蹤會記錄管理帳戶和組織中所有成員帳戶的事件。如需相關資訊 AWS Organizations，請參閱 Or ganizations 術語與概念。

> **Note**
>
> 您必須使用與組織相關聯的管理帳戶或委派的管理員帳戶進行登入，才能建立組織追蹤。您也必須擁有足夠的權限，讓管理或委派的管理員帳戶中的使用者或角色才能建立追蹤。如果沒有足夠的許可，您將不能選擇套用追蹤到組織。

使用主控台建立的所有組織追蹤都是多區域組織追蹤，可記錄組織 AWS 區域 中每個成員帳戶中已啟用的事件。若要記錄組織中所有 AWS 分割區中的事件，請在每個分割區中建立多區域組織追蹤。您可以使用建立單一區域或多區域組織追蹤。 AWS CLI如果您建立單一區域追蹤，則只會在追蹤記錄 AWS 區域 (也稱為「本地區」) 中記錄活動。

雖然大 AWS 區域 多數預設為啟用 AWS 帳戶，但您必須手動啟用某些區域 (也稱為選擇加入區域)。如需預設啟用哪些區域的相關資訊，請參閱《AWS Account Management 參考指南》中的啟用和停用區域之前的考量事項。如需 CloudTrail 支援的區域清單，請參閱CloudTrail 支援的地區。

當您建立組織軌跡時，系統會在屬於您組織的成員帳戶中建立一份具有您指定名稱之追蹤檔的複本。

- 如果組織追蹤是針對單一區域，且追蹤檔的本位目錄「區域」不是「選擇區域」，則會在每個成員帳戶的組織軌跡的本位目錄「區域」中建立追蹤副本。
- 如果組織追蹤檔是針對單一區域，且追蹤檔的本位目錄「區域」是「選擇區域」，則會在已啟用該「區域」的成員帳戶中，在組織軌跡的本位目錄「區域」中建立軌跡副本。
- 如果組織追蹤為「多區域」，且追蹤的主「區域」不是選擇加入「區域」，則會在每個成員帳戶 AWS 區域 中啟用的每個追蹤建立副本。當成員帳戶啟用選擇加入區域時，會在該區域啟動完成後，在該成員帳戶的新選擇中為該成員帳戶建立多區域追蹤的副本。
- 如果組織追蹤為「多區域」，且主「區域」是選擇加入「區域」，則除非成員帳戶選擇加入建立多區域追蹤的 AWS 區域 位置，否則不會將活動傳送至組織追蹤。例如，如果您建立多區域追蹤，並選擇「歐洲 (西班牙) 區域」作為軌跡的本位目錄區域，則只有為其帳戶啟用「歐洲 (西班牙) 區域」的成員帳戶才會將其帳戶作業傳送至組織追蹤檔。

> **Note**
>
> CloudTrail 即使資源驗證失敗，仍會在成員帳號中建立組織追蹤。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 存儲桶政策
> - 不正確的 Amazon SNS 主題政策
> - 無法傳遞至 CloudWatch 記錄檔記錄群組
> - 使用 KMS 金鑰加密權限不足
>
> 具有 CloudTrail 權限的成員帳戶可以在 CloudTrail 主控台上檢視追蹤的詳細資料頁面或執行 AWS CLI get-trail-status命令，來查看組織追蹤的任何驗證失敗。

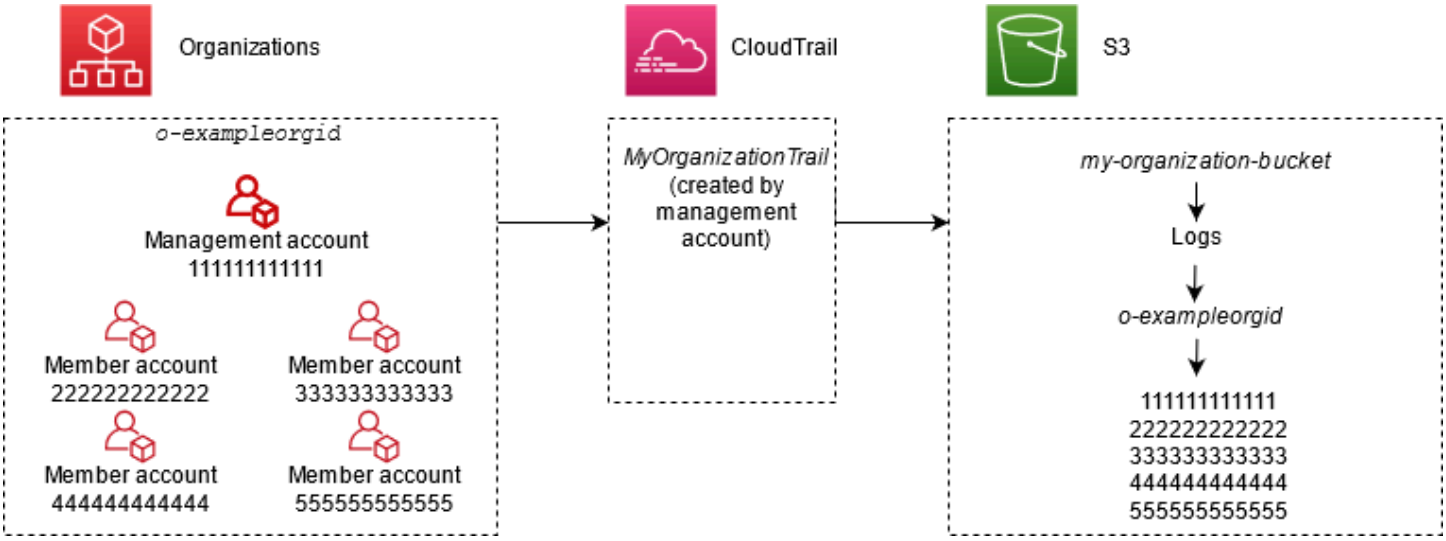
在成員帳戶中具有 CloudTrail 權限的使用者可以從其 AWS 帳戶登入 AWS CloudTrail 主控台或執行 AWS CLI 命令 (例如) 時查看組織追蹤`describe-trails`。不過，成員帳戶中的使用者沒有足夠的權限來刪除組織追蹤、開啟或關閉記錄、變更記錄的事件類型，或以任何方式變更組織追蹤。

當您在主控台中建立組織追蹤，或在 [組織] 中啟用 CloudTrail 為信任的服務時，這會建立服務連結角色，Organizations 便在組織的成員帳戶中執行記錄工作。此角色的名稱為 AWSServiceRoleForCloudTrail，並且是記錄組織事件所必需的角色。 CloudTrail 如果新增至組織，組織追蹤和服務連結角色會新增至該組織 AWS 帳戶，並在組織追蹤檔中自動啟動該帳戶的記錄。 AWS 帳戶 如果從組織中移除，則會從不再屬於組織一部分的組織中刪除組織追蹤和服務連結角色。 AWS

帳戶 AWS 帳戶 不過，在帳戶移除之前為受移除帳戶所建立的日誌檔案，會持續保留於專門儲存追蹤日誌檔案的 Amazon S3 儲存貯體中。

如果 AWS Organizations 組織的管理帳戶建立了組織軌跡，但隨後被移除為組織的管理帳戶，則使用其帳戶建立的任何組織軌跡都會變成非組織軌跡。

*############## 111111111111 ############MyOrganizationTrail####*該追蹤會將組織中所有帳戶的活動全部記錄在同一個 Amazon S3 儲存貯體。組織中的所有帳戶都可以*MyOrganizationTrail*在其追蹤清單中看到，但是成員帳戶無法移除或修改組織追蹤。只有管理帳戶或委派的管理員帳戶可以變更或刪除組織的追蹤。只有管理帳戶可以移除組織的成員帳戶。同樣地，依預設，只有管理帳戶可以存取追蹤*my-organization-bucket*的 Amazon S3 儲存貯體及其中包含的日誌。用於日誌檔案的高階儲存貯體中包含名為以組織 ID 命名的資料夾，以及以組織中每個帳戶的帳戶 ID 所命名的子資料夾。每個成員帳戶的事件都會記錄至對應到成員帳戶 ID 的資料夾。如果成員帳戶 4444444444 已從組織中移除，*MyOrganizationTrail*且服務連結的角色不再出現在 AWS 帳戶 44444444 中，而且組織追蹤檔不會記錄該帳戶的其他事件。不過，444444444444 資料夾仍會保留在 Amazon S3 儲存貯體中，以及該帳戶從組織移除之前建立的所有日誌。



在這個範例中，建立於管理帳戶中的追蹤 ARN 是 `aws:cloudtrail:us-east-2:111111111111:trail/`*MyOrganizationTrail*。這個 ARN 也是所有成員帳戶中所用追蹤的 ARN。

組織追蹤與一般追蹤在許多方面都很相似。您可以為組織建立多個追蹤，以及選擇要為所有區域或單一區域建立組織追蹤，以及您要透過組織追蹤記錄哪類事件，方式就像任何其他追蹤的使用方式。不過，還是有一些差異。例如，當您在主控台中建立追蹤並選擇是記錄 Amazon S3 儲存貯體或 AWS Lambda 函數的資料事件時， CloudTrail 主控台中列出的唯一資源就是管理帳戶的資源，但您可以為成員帳戶中的資源新增 ARN。這時會記錄特定成員帳戶資源的資料事件，而無需為這些資源手動設定跨

帳戶的存取權。如需記錄管理事件、Insights 事件和資料事件的詳細資訊記錄管理事件，請參閱記錄資料事件、和記錄 Insights 事件。

> **Note**
>
> 在主控台中，您可以建立多區域追蹤。這是建議的最佳做法；在您的所有區域中的記錄活動可 AWS 帳戶 協助您保持 AWS 環境更安全。若要建立單一區域追蹤，請使用 AWS CLI。

當您檢視中某個組織的事件歷史記錄中的事件時 AWS Organizations，您只能檢視您登入時 AWS 帳戶使用的事件。例如，如果您使用組織管理帳戶登入，則事件歷史記錄會顯示管理帳戶的最近 90 天管理事件。組織成員帳戶事件不會顯示在管理帳戶的事件歷史記錄中。若要檢視事件歷史記錄中的成員帳戶事件，請使用成員帳戶登入。

您可以設定其他 AWS 服務，以便進一步分析組織追蹤 CloudTrail 記錄中收集的事件資料，並採取行動，方式與執行任何其他追蹤的方式相同。例如，您可以使用 Amazon Athena 分析組織追蹤中的資料。如需詳細資訊，請參閱 AWS 與 CloudTrail 日誌的服務整合。

主題

從成員帳戶追蹤移至組織追蹤

如果您已針對個別成員帳戶設定追 CloudTrail 蹤，但想要移至組織追蹤以記錄所有帳戶中的事件，則您不想在建立組織追蹤之前刪除個別成員帳戶追蹤，以遺失事件。但是，當您有兩個追蹤時，由於額外的事件複本會傳送到組織追蹤，因此會產生更高的成本。

為了幫助管理成本，但又要避免在組織追蹤開始傳送日誌之前遺失事件，請考慮將您的個別成員帳戶追蹤和組織追蹤保留最多一天。如此可確保組織追蹤記錄所有事件，但您只會產生一天的重複事件成本。在第一天之後，即可停止登入 (或刪除) 任何個別成員帳戶追蹤。

準備建立組織追蹤

在建立組織的追蹤之前，請確保已正確設定您的組織管理帳戶或委派的管理員帳戶，以便建立追蹤。

- 您組織中的所有功能必須都預先啟用，您才能為其建立追蹤。如需詳細資訊，請參閱啟用組織中的所有功能。
- 管理帳戶必須具有 AWSServiceRoleForOrganizations 角色。此角色是由「組 Organizations」在您建立組織時自動建立的，並且是記錄組織事件的必要角色。 CloudTrail 如需詳細資訊，請參閱 Organizations 和服務連結角色。
- 在管理或委派的管理員帳戶中建立組織追蹤的使用者或角色，必須擁有可建立組織追蹤的足夠許可。您必須至少將 AWSCloudTrail_FullAccess 政策，或同等政策套用至該角色或使用者。您還必須擁有 IAM 和 Organizations 的足夠許可，才能建立服務連結角色，以及啟用受信任存取。如果您選擇使用 CloudTrail 主控台為組織追蹤建立新的 S3 儲存貯體， 您的保單還需要包括 `s3:PutEncryptionConfiguration` 動作是因為預設值區已啟用伺服器端加密。下列範例政策顯示最少的必要許可。

> **Note**
>
> 您不應該AWSCloudTrail_FullAccess在您的 AWS 帳戶. 相反地，由於所收集的資訊具有高度敏感性，因此您應該將其限制為 AWS 帳戶 系統管理員 CloudTrail。使用此角色的使用者能夠在自己的 AWS 帳戶中關閉或重新設定最敏感和重要的稽核功能。基於這個原因，您必須嚴密控制和監控對這類政策的存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

- 若要使用 AWS CLI 或 CloudTrail API 建立組織追蹤，您必須在組 Organizations CloudTrail 中啟用受信任的存取，並且必須使用允許組織追蹤記錄的政策手動建立 Amazon S3 儲存貯體。如需詳細資訊，請參閱 建立組織的追蹤 AWS Command Line Interface。
- 若要使用現有的 IAM 角色將組織追蹤的監控新增至 Amazon CloudWatch Logs，您必須手動修改 IAM 角色，以允許將成員帳戶的 CloudWatch CloudWatch 日誌傳遞到管理帳戶的日誌群組，如下列範例所示。

> **Note**
>
> 您必須使用存在於自己帳戶中的 IAM 角色和 CloudWatch 記錄日誌群組。您無法使用不同帳戶擁有的 IAM 角色或 CloudWatch 記錄日誌群組。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
```

```
        }
    ]
}
```

您可以在中了解有關 CloudTrail 和 Amazon CloudWatch 日誌的更多信息使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。此外，在決定啟用組織追蹤的體驗之前，請先考慮 CloudWatch 記錄限制和服務的定價考量。如需詳細資訊，請參閱CloudWatch 日誌限制和 Amazon CloudWatch 定價。

- 若要在組織追蹤，記錄成員帳戶中之特定資源的資料事件，請為這些資源準備 Amazon Resource Name (ARN) 清單。建立追蹤時，成員帳戶資源不會顯示在 CloudTrail 主控台中；您可以在支援資料事件收集的管理帳戶中瀏覽資源，例如 S3 儲存貯體。同樣地，建立或更新組織追蹤時，如果要在命令列中新增特定的成員資源，這時您將需要這些資源的 ARN。

> **Note**
>
> 記錄資料事件需支付額外的費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

在建立組織追蹤之前，您也應該考慮檢閱管理帳戶和成員帳戶中已有多少追蹤。 CloudTrail 限制可在每個區域中建立的軌跡數目。您在管理帳戶中建立組織追蹤的區域不能超過這個限制。不過，即使成員帳戶已達到區域內追蹤限制，成員帳戶中仍會建立該追蹤。任何區域中的第一個管理事件追蹤都是免費的，接著新增的任何追蹤將予以計費。若要降低組織追蹤的可能成本，請考慮刪除管理帳戶和成員帳戶中的任何不需要追蹤。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

組織追蹤中的安全最佳實務

我們建議的安全最佳實務是，將 `aws:SourceArn` 條件金鑰新增至您與組織追蹤搭配使用的資源政策 (例如 S3 儲存貯體、KMS 金鑰或 SNS 主題的政策)。`aws:SourceArn` 的值是組織追蹤 ARN (或多個 ARN，如果您為多個追蹤使用相同的資源，例如相同的 S3 儲存貯體，以存放多個追蹤的日誌)。這可確保資源 (例如 S3 儲存貯體) 僅接受與特定追蹤相關聯的資料。追蹤 ARN 必須使用管理帳戶的帳戶 ID。下列政策片段顯示有一個以上的追蹤正在使用資源的範例。

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

如需將條件金鑰新增至資源政策的詳細資訊，請參閱下列內容：

- Amazon S3 存儲桶政策 CloudTrail
- 設定 AWS KMS 金鑰原則 CloudTrail
- Amazon SNS 主題政策 CloudTrail

使用主控台建立組織追蹤

若要從 CloudTrail 主控台建立組織追蹤，您必須以具有足夠權限之管理或委派管理員帳戶中的使用者或角色身分登入主控台。如果您未使用管理或委派的系統管理員帳戶登入，當您從 CloudTrail主控台建立或編輯追蹤時，將不會看到將追蹤套用至組織的選項。

您可以採用多種方式來設定組織追蹤。例如，您可以為組織追蹤執行下列詳細設定：

- 依預設，當您在主控台中建立追蹤時，該追蹤會記錄您正在使用的 AWS 分割區中的所有 AWS 區域 。最佳做法是，我們強烈建議您在 AWS 帳戶. 若要為單一區域建立追蹤，請使用 AWS CLI。
- 指定是否將追蹤套用到您的組織。依預設，追蹤不會套用至組織。您必須選擇此選項，才能建立組織追蹤。
- 指定哪個 Amazon S3 儲存貯體會接收組織追蹤的日誌檔案。您可以選擇現有 Amazon S3 儲存貯體，或建立一個專門用於組織追蹤的儲存貯體。
- 對於管理和資料事件，指定您要記錄讀取、寫入，或二者。CloudTrail見解事件只會記錄在管理事件上。您可以指定為管理帳戶中的資源 (從主控台中的清單選擇) 記錄資料事件，而且若您有為每個要啟用資料事件記錄的資源指定個別 ARN，則您可以指定為成員帳戶中資源記錄事件。如需詳細資訊，請參閱 資料事件。

若要使用建立組織軌跡 AWS Management Console

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。

   您必須使用管理或委派的管理員帳戶中的 IAM 身分登入，並且具備足夠的許可才能建立組織追蹤。
2. 選擇 Trails (追蹤)，然後選擇 Create trail (建立追蹤)。
3. 在 Create Trail (建立追蹤) 頁面的 Trail name (追蹤名稱) 中，輸入追蹤的名稱。如需詳細資訊，請參閱 命名要求。
4. 選擇針對組織中的所有帳戶啟用。如果您使用管理或委派的管理員帳戶中的使用者或角色登入到主控台，這時您將只能看到這個選項。若要成功建立組織追蹤，請確保該使用者或角色具備足夠許可。

5. 針對 Storage location (儲存位置)，選擇 Create a new S3 bucket (建立新 S3 儲存貯體)，以建立儲存貯體。建立值區時， CloudTrail 會建立並套用所需的值區政策。

> **Note**
>
> 如果您選擇使用現有的 S3 儲存貯體，請在追蹤記錄儲存貯體名稱中指定一個儲存貯體，或選擇 Browse (瀏覽) 以選擇儲存貯體。您可以選擇屬於任何帳戶的值區，但值區政策必須授予寫入 CloudTrail權限。如需手動編輯儲存貯體政策的資訊，請參閱「Amazon S3 存儲桶政策 CloudTrail」。

為了更容易找到您的日誌，請在現有存儲桶中創建一個新文件夾（也稱為前綴）以存儲 CloudTrail 日誌。在字首中輸入字首。

6. 針對 Log file SSE-KMS encryption (日誌檔案 SSE-KMS 加密)，如果您想要使用 SSE-KMS 而非 SSE-S3 來加密日誌檔案，請選擇 Enabled (啟用)。預設為啟用。如果您未啟用 SSE-KMS 加密，則會使用 SSE-S3 加密來加密您的日誌。如需 SSE-KMS 加密的詳細資訊，請參閱搭配 AWS Key Management Service (SSE-KMS) 使用伺服器端加密。如需 SSE-S3 加密的詳細資訊，請參閱搭配使用伺服器端加密與 Amazon S3 受管加密金鑰 (SSE-S3)。

   如果您啟用 SSE-KMS 加密，請選擇 [新增] 或 [現有]。 AWS KMS key在AWS KMS 別名中，以格式指定別名`alias/`*`MyAliasName`*。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。

> **Note**
>
> 您也可以從另一個帳戶輸入金鑰的 ARN。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。金鑰原則必須允許 CloudTrail 使用金鑰來加密記錄檔，並允許您指定的使用者以未加密的形式讀取記錄檔。如需手動編輯金鑰政策的資訊，請參閱「設定 AWS KMS 金鑰原則 CloudTrail」。

7. 在其他設定下，設定下列項目。

   a. 針對 Log file validation (日誌檔案驗證)，選擇 Enabled (啟用) 將日誌摘要交付到您的 S3 儲存貯體。您可以使用摘要檔來驗證記錄檔在 CloudTrail 傳送記錄檔之後是否未變更。如需詳細資訊，請參閱 驗證 CloudTrail 記錄檔完整性。

   b. 對於 SNS 通知傳遞，請選擇 [啟用]，以便在每次將記錄傳送至儲存貯體時收到通知。CloudTrail 在記錄檔中儲存多個事件。SNS 通知是針對每個日誌檔案所傳送，而不是每個事件。如需詳細資訊，請參閱 設定 Amazon SNS 通知 CloudTrail。

如果您啟用 SNS 通知，針對建立新 SNS 主題，選擇 New (新的) 以建立主題，或選擇 Existing (現有) 以使用現有的主題。如果您要建立套用至所有區域的追蹤，則會將所有區域中日誌檔案傳遞的 SNS 通知都交付至您建立的單一 SNS 主題。

如果您選擇「新增」，請為您 CloudTrail 指定新主題的名稱，或者您也可以輸入名稱。如果選擇 Existing (現有),請從下拉式清單中選擇 SNS 主題。您也可以輸入來自另一個區域，或具有適當許可之帳戶的主題 ARN。如需詳細資訊，請參閱 Amazon SNS 主題政策 CloudTrail。

如果您建立主題，則必須訂閱該主題，以便在日誌檔案交付時收到通知。您可以從 Amazon SNS 主控台進行訂閱。基於通知頻率，建議您設定訂閱以利用 Amazon SQS 佇列，透過編寫程式的方式處理通知。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

8. 選擇性地選擇「記錄檔中已啟用」，設定 CloudTrail 將 CloudWatch 記錄檔傳送至CloudWatch 記錄檔。如需詳細資訊，請參閱 將事件傳送至 CloudWatch 記錄檔。

> **Note**
>
> 只有管理帳戶可以使用主控台為組織追蹤設定 CloudWatch 記錄檔群組。委派的系統管理員可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 作業來設定 CloudWatch 記錄檔群組。

   a. 如果您啟用與 CloudWatch 記錄整合，請選擇 [新增] 以建立新的記錄群組，或選擇 [現有] 使用現有的記錄群組。如果選擇 [新增]，請為您 CloudTrail 指定新記錄群組的名稱，或者輸入名稱。

   b. 如果選擇 Existing (現有)，請從下拉式清單中選擇日誌群組。

   c. 選擇 [新增]，為許可建立新的 IAM 角色，以便將記錄傳送至 CloudWatch 記錄。選擇 Existing (現有) 從下拉式功能表中選擇現有的 IAM 角色。新角色或現有角色的政策陳述式會在您展開政策文件時顯示。如需有關此角色的詳細資訊，請參閱 使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件。

> **Note**
>
> 設定追蹤時，您可以選擇由其他帳戶所屬的 S3 儲存貯體和 Amazon SNS 主題。不過，如果您想 CloudTrail 要將事件傳遞至 CloudWatch 記錄檔記錄群組，則必須選擇目前帳戶中存在的記錄群組。

9. 對於 標籤 (Tags)，請將一個或多個自訂標籤 (鍵/值對) 新增至追蹤。標籤可協助您識別 CloudTrail 追蹤和包含 CloudTrail 日誌檔的 Amazon S3 儲存貯體。然後，您可以將資源群組用於資 CloudTrail 源。如需詳細資訊，請參閱 AWS Resource Groups及 標籤。
10. 在選擇日誌事件頁面上，選擇您要記錄的事件類型。對於 Management events (管理事件)，請執行下列動作。

    a. 針對 API 活動，選擇您是否希望追蹤記錄讀取事件、寫入事件，或兩者。如需詳細資訊，請參閱 管理事件。

    b. 選擇「排除 AWS KMS 事件」，將 AWS Key Management Service (AWS KMS) 事件從追蹤中篩選出來。預設設定是包含所有 AWS KMS 事件。

       只有在追蹤記錄中記錄管理 AWS KMS 事件時，才能使用記錄或排除事件的選項。如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

       AWS KMS 動作，例如`Encrypt`、`Decrypt`、`GenerateDataKey`通常會產生大量 (超過 99%) 的事件。這些動作現在會記錄為 Read (讀取) 事件。低容量的相關 AWS KMS 動作，例如`DisableDelete`、和 `ScheduleKey` (通常佔 AWS KMS 事件磁碟區的 0.5% 以下) 會記錄為「寫入」事件。

       若要排除大量事件，例如 `Encrypt`、`Decrypt` 和 `GenerateDataKey`，但仍記錄相關事件，例如 `Disable`、`Delete` 和 `ScheduleKey`，選擇記錄 Write (寫入) 管理事件，然後清除 Exclude AWS KMS 事件的核取方塊。

    c. 選擇排除 Amazon RDS Data API 事件從追蹤中篩選 Amazon Relational Database Service Data API 事件。預設設定是包含所有 Amazon RDS Data API 事件。如需 Amazon RDS Data API 事件的詳細資訊，請參閱《Amazon RDS 使用者指南 (Aurora)》中的使用 AWS CloudTrail記錄資料 API 呼叫。
11. 若要記錄資料事件，請選擇資料事件。記錄資料事件需支付額外的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。
12.

> **Important**
>
> 依預設，透過使用進階事件選取器執行步驟 12-16，可設定資料事件。進階事件選取器可讓您設定更多資料事件類型，並對追蹤擷取的資料事件提供精細控制。如果您選擇使用基本事件選取器，請完成 使用基本事件選取器執行資料事件設定 中的步驟，然後返回至此程序的步驟 17。

針對資料事件類型，選擇您想要記錄資料事件的資源類型。如需有關可用資料事件類型的詳細資訊，請參閱 資料事件。

> **Note**
>
> 若要為 Lake Formation 成建立的 AWS Glue 表格記錄資料事件，請選擇 Lake Formation。

13. 選擇記錄選取器範本。 CloudTrail 包括記錄資源類型的所有資料事件的預先定義範本。若要建立自訂記錄選取器範本，請選擇 Custom (自訂)。

> **Note**
>
> 為 S3 儲存貯體選擇預先定義的範本，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何 IAM 身分執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的值區上執行。
> 如果追蹤僅套用至一個區域，選取預先定義的記錄所有 S3 儲存貯體的範本可針對下列儲存貯體啟用記錄資料事件：與您追蹤相同之區域中的所有儲存貯體，以及您稍後在該區域中建立的任何儲存貯體。並不會記錄 AWS 帳戶中其他區域內 Amazon S3 儲存貯體的資料事件。
> 如果您要為所有區域建立追蹤，請為 Lambda 函數選擇預先定義的範本，為 AWS 帳戶中目前的所有函數啟用資料事件記錄，以及在完成追蹤建立後可能在任何區域建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，此選項會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。
> 記錄所有功能的資料事件也可讓您記錄 AWS 帳戶中任何 IAM 身分執行的資料事件活動，即使該活動是在屬於其他 AWS 帳戶的函數上執行。

14. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。

15. 在進階事件選取器，請為您想要記錄資料事件的特定資源建立表達式。如果您使用預先定義的日誌範本，則可略過此步驟。

    a. 從下列欄位選取。

- **readOnly**-readOnly 可以設定為等於true或的值false。唯讀資料事件是不會變更資源狀態的事件，例如 Get* 或 Describe* 事件. 寫入事件新增、變更或刪除資源、屬性或成品，例如 Put*、Delete* 或 Write* 事件。若要同時記錄 read 和 write 事件，請勿新增 readOnly 選擇器。
- **eventName**-eventName可以使用任何運算子。您可以使用它來包含或排除記錄到的任何資料事件 CloudTrailPutBucket，例如PutItem、或GetSnapshotBlock。
- **resources.ARN**-您可以將任何運算子搭配使用resources.ARN，但是如果您使用 equals 或不等於，則值必須完全符合您在範本中指定為值之類型之有效資源的 ARN。resources.type

  下表顯示每種 resources.type 的有效 ARN 格式。

  > **Note**
  >
  > 您無法使用resources.ARN欄位來篩選沒有 ARN 的資源類型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*

resources.type	resources.ARN
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-aliases/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*

resources.type	resources.ARN
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*

resources.type	resources.ARN
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必須採用下列其中一種格式： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必須採用下列其中一種格式： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclie nt: *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您指定 AWS::DynamoDB::Table 作為 resources.type，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在eventName欄位上新增篩選器。

[2] 若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 StartsWith 運算子，並僅包含儲存貯體 ARN 作為相符值。末尾斜線是有意保留，請勿排除。

[3] 若要在 S3 存取點中的所有物件上記錄事件，建議您僅使用存取點 ARN、不要包含物件路徑，並使用 StartsWith 或 NotStartsWith 運算子。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的動作、資源及條件金鑰。

b. 針對每個欄位，選擇 + 條件，視需要新增任意數目的條件，所有條件最多可指定 500 個值。例如，若要從追蹤記錄的資料事件中排除兩個 S3 儲存貯體的資料事件，您可以將欄位設定為

Resources.arn，將運算子設定為「不開始於」，然後貼上 S3 儲存貯體 ARN，或瀏覽您不想記錄事件的 S3 儲存貯體。

若要新增第二個 S3 儲存貯體，請選擇 + 條件，然後重複上述指令，在 ARN 中粘貼或瀏覽不同的儲存貯體。

> **Note**
>
> 追蹤上的所有選取器，您最多可以有 500 個值。這包括一個選擇器的多個值的陣列，如 `eventName`。如果所有選擇器都有單個值，則最多可以有 500 個條件新增至選擇器。
> 如果您的帳戶中有超過 15,000 個 Lambda 函數，則無法在建立追蹤時在 CloudTrail 主控台中檢視或選取所有函數。您仍然可以使用預先定義的選取器範本記錄所有函數，即使其未全部顯示。如果您要記錄特定函數之資料事件，則可以在得知該函數的 ARN 後手動加以新增。您也可以在主控台中完成追蹤的建立，然後使用 AWS CLI 和put-event-selectors命令為特定 Lambda 函數設定資料事件記錄。如需詳細資訊，請參閱 管理軌跡 AWS CLI。

c. 選擇 + 欄位以根據需要新增其他欄位。為避免發生錯誤，請勿為欄位設定衝突或重複的值。例如，不要在一個選擇器中指定 ARN 等於一個值，然後指定 ARN 不等於另一個選取器中的相同值。

16. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。重複步驟 12 到此步驟，以設定資料事件類型的進階事件選取器。
17. 如果您希望追蹤記錄見解事件，請選擇「 CloudTrail深入解析」事件。

    在 Event type (事件類型) 中，選取 Insights 事件。在 Insights events (Insights 事件) 中，選擇 API call rate (API 呼叫率) 或 API error rate (API 錯誤率) (或兩者)。您必須記錄寫入管理事件，以便記錄 API 呼叫率的 Insights 事件。您必須記錄讀取或寫入管理事件，以便記錄 API 錯誤率的 Insights 事件。

    CloudTrail Insights 會分析異常活動的管理事件，並在偵測到異常時記錄事件。依預設，追蹤不會記錄 Insights 事件。如需 Insights 事件的詳細資訊，請參閱記錄 Insights 事件。記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

    見解事件會傳遞到名為相同 S3 儲存貯體/`CloudTrail-Insight`的不同資料夾，該資料夾名稱為在追蹤詳細資料頁面的儲存位置區域中指定。 CloudTrail會為您建立新字首。例如，如果您目前的目的地 S3 儲存貯體名為 `S3bucketName/AWSLogs/CloudTrail/`，則具有新前綴的 S3 儲存貯體名稱會被命名為 `S3bucketName/AWSLogs/CloudTrail-Insight/`。

18. 當您完成選擇要記錄的事件類型時，請選擇 Next (下一頁)。
19. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇區段中的 Edit (編輯)，以變更該區段中顯示的追蹤設定。當您準備好建立追蹤時，請選擇 Create trail (建立追蹤)。
20. 新的追蹤會出現在 Trails (追蹤) 頁面上。組織追蹤可能需要多達 24 小時的時間，才能完成在所有成員帳戶中於所有區域中的建立作業。Trails (追蹤) 頁面會顯示您帳戶中所有區域內的追蹤。大約 5 分鐘後，會 CloudTrail 發佈記錄檔，其中顯示在組織中進行的 AWS API 呼叫。您可以在所指定之 Amazon S3 儲存貯體中看到日誌檔案。

> **Note**
>
> 您無法重新命名已建立的追蹤。但是您可以改為刪除之，並建立新的追蹤。

後續步驟

在您建立追蹤之後，即可返回追蹤以進行變更：

- 透過編輯來變更追蹤的組態。如需詳細資訊，請參閱 更新追蹤。
- 如必要，設定 Amazon S3 儲存貯體，以允許成員帳戶中的特定使用者讀取組織的日誌檔案。如需詳細資訊，請參閱 在 AWS 帳戶之間共用 CloudTrail 記錄檔。
- 設定 CloudTrail 為將記錄檔傳送至 CloudWatch 記錄檔。如需詳細資訊，請參閱將事件傳送至 CloudWatch 記錄檔和中的 [CloudWatch 記錄] 項目準備建立組織追蹤。

  > **Note**
  >
  > 只有管理帳戶可以為組織追蹤設定 CloudWatch 記錄檔記錄群組。

- 在 Amazon Athena 中建立資料表並用以執行查詢，以分析 AWS 服務活動。如需詳細資訊，請參閱 Amazon Athena 使用者指南中的 CloudTrail 主控台中的為 CloudTrail 日誌建立表格。
- 將自訂標籤 (鍵/值對) 新增至追蹤。
- 若要建立另一個組織追蹤，請返回 Trails (追蹤) 頁面，然後選擇 Create trail (建立追蹤)。

> **Note**
>
> 設定追蹤時，您可以選擇由其他帳戶所屬的 Amazon S3 儲存貯體和 SNS 主題。不過，如果您想 CloudTrail 要將事件傳遞至 CloudWatch 記錄檔記錄群組，則必須選擇目前帳戶中存在的記錄群組。

建立組織的追蹤 AWS Command Line Interface

您可以使用 AWS CLI來建立組織追蹤。會 AWS CLI 定期更新其他功能和指令。為協助確保成功，在開始之前，請確定您已安裝或更新至最新 AWS CLI 版本。

> **Note**
>
> 本節中的範例是建立和更新組織追蹤的特定示範。如需使用管理系統線 AWS CLI 的範例，請參閱管理軌跡 AWS CLI和設定 CloudWatch 記錄監控 AWS CLI。使用建立或更新組織軌跡時 AWS CLI，您必須在管理帳戶或具有足夠權限的委派管理員帳戶中使用 AWS CLI 設定檔。如果您要將組織追蹤轉換為非組織追蹤，則必須使用該組織的管理帳戶。
> 您必須設定 Amazon S3 儲存貯體用於組織追蹤才有足夠的許可。

建立或更新 Amazon S3 儲存貯體以存放組織追蹤的日誌檔案

您必須指定 Amazon S3 儲存貯體以接收組織追蹤的日誌檔案。此值區必須具有允 CloudTrail 許將組織的記錄檔放入值區的政策。

以下是名為的 Amazon S3 儲存貯體的範例政策 *myOrganizationBucket*，該儲存貯體由組織的管理帳戶擁有。以組織的值取代*myOrganizationBucket*、*##*、*#### ID*、*####*和 *O ###* ID

此儲存貯體政策包含三個陳述式。

- 第一個語句 CloudTrail 允許在 Amazon S3 存儲桶調用 Amazon S3 `GetBucketAcl` 動作。
- 第二個陳述式允許記錄當追蹤從組織追蹤變更成僅限該帳戶使用的事件。
- 第三個陳述式允許組織追蹤記錄。

範例政策會納入 Amazon S3 儲存貯體政策的 `aws:SourceArn` 條件金鑰。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對特定追蹤或追蹤 CloudTrail 寫入 S3 儲存貯體。在組織追蹤中，`aws:SourceArn` 的值必須是管理帳戶所擁有且使用管理帳戶 ID 的追蹤 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

這個範例政策不允許成員帳戶中任何使用者存取為該組織建立的日誌檔案。在預設情況下，只有管理帳戶才能存取組織日誌檔案。如需有關如何允許成員帳戶中 IAM 使用者對於 Amazon S3 儲存貯體的讀取許可，請參閱 在 AWS 帳戶之間共用 CloudTrail 記錄檔。

啟用 CloudTrail 為信任的服務 AWS Organizations

您必須先啟用 Organizations 中的所有功能，才能建立組織追蹤。如需詳細資訊，請參閱啟用組織中的所有功能，或是使用管理帳戶中具備足夠許可之設定檔來執行以下命令：

```
aws organizations enable-all-features
```

啟用所有功能之後，您必須將「Organizations」設定 CloudTrail 為信任的服務。

若要建立 AWS Organizations 和之間的信任服務關係 CloudTrail，請開啟終端機或命令列，然後在管理帳戶中使用設定檔。依照下面範例示範的方式來執行 `aws organizations enable-aws-service-access` 命令。

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

使用 create-trail

建立套用到所有區域的組織追蹤

若要建立套用到所有區域的組織追蹤，請新增 `--is-organization-trail` 與 `--is-multi-region-trail` 選項。

> **Note**
>
> 當您使用建立組織追蹤時 AWS CLI，您必須使用管理帳戶中的 AWS CLI 設定檔或具有足夠權限的委派管理員帳戶。

以下範例會建立組織追蹤，將所有區域的日誌傳遞到名為 *my-bucket* 的現有儲存貯體：

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail --is-multi-region-trail
```

若要確認所有區域都有您的追蹤，輸出中的 `IsOrganizationTrail` 和 `IsMultiRegionTrail` 參數會同時設定為 `true`：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 執行 `start-logging` 命令來為追蹤啟動記錄功能。如需詳細資訊，請參閱 停止及啟動追蹤的記錄功能。

將組織追蹤建立成單一區域追蹤

下列命令會建立只記錄單一 (也稱為單 AWS 區域一區域追蹤) 中的事件的組織追蹤。記錄事件的 AWS 區域是在的組態設定檔中指定的區域 AWS CLI。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail
```

如需詳細資訊，請參閱 命名要求。

輸出範例：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

依預設，`create-trail` 命令會建立單一區域追蹤，而且該追蹤不會啟用日誌檔案驗證。

> **Note**
>
> 執行 `start-logging` 命令來為追蹤啟動記錄功能。

執行 update-trail 以更新組織追蹤

您可以執行 `update-trail` 命令來變更組織追蹤的組態設定，或是將單一 AWS 帳戶的現有追蹤套用到整個組織。請記住您只能從該追蹤建立所在區域執行 `update-trail` 命令。

> **Note**
>
> 如果您使用 AWS CLI 或其中一個 AWS SDK 更新追蹤，請確定追蹤的值區原則為 up-to-date。如需詳細資訊，請參閱 建立組織的追蹤 AWS Command Line Interface。
> 當您使用更新組織軌跡時 AWS CLI，您必須使用管理帳戶中的 AWS CLI 設定檔或具有足夠權限的委派管理員帳戶。如果您要將組織追蹤轉換為非組織追蹤，則必須使用該組織的管理帳戶，因為管理帳戶是所有組織資源的擁有者。

CloudTrail 即使資源驗證失敗，也會更新成員帳號中的組織追蹤。驗證失敗的範例包括：

- 不正確的 Amazon S3 存儲桶政策
- 不正確的 Amazon SNS 主題政策
- 無法傳遞至 CloudWatch 記錄檔記錄群組
- 使用 KMS 金鑰加密權限不足

具有 CloudTrail 權限的成員帳戶可以在 CloudTrail 主控台上檢視追蹤的詳細資料頁面或執行 AWS CLI get-trail-status命令，來查看組織追蹤的任何驗證失敗。

將現有追蹤套用到組織

若要變更現有追蹤，使其同時套用至組織 (而非單一 AWS 帳戶)，請新增`--is-organization-trail`選項，如下列範例所示。

> **Note**
> 使用管理帳戶將現有的非組織追蹤變更為組織追蹤。

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

若要確認追蹤現在會套用到組織，輸出中的 `IsOrganizationTrail` 元素會顯示 `true` 的值。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

在前述範例中，追蹤被設定成套用到所有區域 (`"IsMultiRegionTrail": true`)。只套用到單一區域的追蹤，將在輸出中顯示 `"IsMultiRegionTrail": false`。

將套用到一個區域的組織追蹤轉換成套用到所有區域

若要將現有的組織追蹤變更成可套用至所有區域，請新增 `--is-multi-region-trail` 選項，如下列範例中所示。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

若要確認追蹤現在會套用到所有區域，輸出中的 `IsMultiRegionTrail` 參數會顯示 `true` 的值。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

故障診斷

本節提供如何疑難排解組織追蹤問題的相關資訊。

主題

- CloudTrail 沒有傳遞事件
- CloudTrail 不會針對組織中的成員帳戶傳送 Amazon SNS 通知

CloudTrail 沒有傳遞事件

如果 CloudTrail 未將 CloudTrail 日誌檔案傳送到 Amazon S3 儲存貯體

檢查 S3 儲存貯體是否有問題。

- 從 CloudTrail 主控台，檢查軌跡的詳細資訊頁面。如果 S3 儲存貯體發生問題，詳細資料頁面會包含交付至 S3 儲存貯體失敗的警告。
- 從中 AWS CLI執行命get-trail-status令。如果發生故障，命令輸出會包含`LatestDeliveryError`欄位，該欄位會顯示嘗試將日誌檔傳送到指定儲存貯體時 CloudTrail 遇到的任何 Amazon S3 錯誤。只有在目的地 S3 儲存貯體發生問題時，才會發生此錯誤，對於逾時的請求不會發生。若要解決此問題，請修正值區政策， CloudTrail 以便寫入值區；或建立新值區，

然後呼叫update-trail以指定新值區。如需組織儲存貯體政策的相關資訊，請參閱建立或更新 Amazon S3 儲存貯體以用來存放組織追蹤的日誌檔。

如果 CloudTrail 未將記錄傳送至記 CloudWatch 錄檔

檢查 CloudWatch 記錄角色原則的設定是否有問題。

- 從 CloudTrail 主控台，檢查軌跡的詳細資訊頁面。如果 CloudWatch 記錄檔發生問題，詳細資料頁面會包含警告，指出 CloudWatch 記錄檔傳遞失敗。
- 從中 AWS CLI執行命get-trail-status令。如果發生失敗，命令輸出會包含LatestCloudWatchLogsDeliveryError欄位，該欄位會顯示嘗試將 CloudWatch 記錄傳送至記錄檔時 CloudTrail 遇到的任何記 CloudWatch 錄錯誤。若要解決此問題，請修正記 CloudWatch 錄檔角色原則。如需有關 CloudWatch 記錄檔角色原則的資訊，請參閱使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件。

如果您在組織追蹤記錄中看不到成員帳戶的活動

如果您在組織追蹤中看不到成員帳戶的活動，請檢查下列項目：

- 檢查主地區以了解路徑，看看它是否是選擇加入的區域

  雖然大 AWS 區域 多數預設為啟用 AWS 帳戶，但您必須手動啟用某些區域 (也稱為選擇加入區域)。如需預設啟用哪些區域的相關資訊，請參閱《AWS Account Management 參考指南》中的啟用和停用區域之前的考量事項。如需 CloudTrail 支援的區域清單，請參閱CloudTrail 支援的地區。

  如果組織追蹤為「多區域」，且主「區域」是選擇加入「區域」，則除非成員帳戶選擇加入建立多區域追蹤的 AWS 區域 位置，否則不會將活動傳送至組織追蹤。例如，如果您建立多區域追蹤，並選擇「歐洲 (西班牙) 區域」作為軌跡的本位目錄區域，則只有為其帳戶啟用「歐洲 (西班牙) 區域」的成員帳戶才會將其帳戶作業傳送至組織追蹤檔。若要解決此問題，請在組織中的每個成員帳戶中啟用選擇加入區域。如需有關啟用選擇加入區域的資訊，請參閱《AWS Account Management 參考指南》中的啟用或停用組織中的區域。
- 檢查組織以資源為基礎的策略是否與 CloudTrail 服務連結角色策略衝突

  CloudTrail 使用名為的服務連結角色AWSServiceRoleForCloudTrail來支援組織追蹤。此服務連結角色可 CloudTrail 對組織資源執行動作，例如organizations:DescribeOrganization。如果組織以資源為基礎的策略拒絕服務連結角色策略中允許的動作， CloudTrail 則即使服務連結角色策略中允許該動作也無法執行。若要解決此問題，請修正組織的以資源為基礎的原則，這樣它就不會拒絕服務連結角色原則中允許的動作。

CloudTrail 不會針對組織中的成員帳戶傳送 Amazon SNS 通知

具有 AWS Organizations 組織追蹤的成員帳戶未傳送 Amazon SNS 通知時，SNS 主題政策的組態可能發生問題。 CloudTrail 即使資源驗證失敗，也會在成員帳戶中建立組織追蹤，例如組織軌跡的 SNS 主題不包含所有成員帳號 ID。如果 SNS 主題原則不正確，就會發生授權失敗。

若要檢查追蹤的 SNS 主題原則是否有授權失敗：

- 從 CloudTrail 主控台，檢查軌跡的詳細資訊頁面。如果授權失敗，詳細資料頁面會包含警告，SNS `authorization failed`並指示要修正 SNS 主題原則。
- 從中 AWS CLI執行命get-trail-status令。如果授權失敗，命令輸出會包含值為的`LastNotificationError`欄位`AuthorizationError`。若要解決此問題，請修正 Amazon SNS 主題政策。如需 Amazon SNS 主題政策的相關資訊，請參閱Amazon SNS 主題政策 CloudTrail。

如需有關 SNS 主題及訂閱的詳細資訊，請參閱 Amazon 簡單通知服務開發人員指南中的 Amazon SNS 入門。

檢視追蹤的 CloudTrail 見解事件

在追蹤上啟用 CloudTrail 深入解析之後，您可以使用主 CloudTrail控台或 AWS CLI. 本節說明如何檢視、查詢和下載 Insights 事件的檔案。如需使用 `LookupEvents` API 擷取 CloudTrail 事件資訊的相關資訊，請參閱 AWS CloudTrail API 參考。如需 CloudTrail 深入解析的詳細資訊，請參閱本指南記錄 Insights 事件中的。

如需有關如何建立線索的詳細資訊，請參閱建立追蹤和取得及檢視您的 CloudTrail 記錄檔。

> **Note**
>
> 若要在 API 呼叫量上記錄 Insights 事件，追蹤必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，追蹤必須記錄 `read` 或 `write` 管理事件。

主題

- 在 CloudTrail 主控台中檢視追蹤的 CloudTrail 深入解析事件
- 檢視追蹤的 CloudTrail 見解事件 AWS CLI

在 CloudTrail 主控台中檢視追蹤的 CloudTrail 深入解析事件

在追蹤上啟用 CloudTrail Insights 事件後，當 CloudTrail 偵測到異常的 API 或錯誤率活動時，CloudTrail 會產生深入解析事件，並將其顯示在的儀表板和「見解」頁面上 AWS Management Console。您可以在控制台中查看 Insights 事件，並對異常的活動進行疑難排解。主控台中會顯示最近 90 天的 Insights 事件。您也可以使用 AWS CloudTrail 主控台下載見解事件。您可以使用 AWS SDK 或 AWS Command Line Interface以程式設計方式查詢事件。如需 CloudTrail 深入解析事件的詳細資訊，請參閱本指南記錄 Insights 事件中的。

> **Note**
>
> 若要在 API 呼叫量上記錄 Insights 事件，追蹤必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，追蹤必須記錄 `read` 或 `write` 管理事件。

記錄 Insights 事件之後，事件會顯示在 Insights (深入分析) 頁面 90 天。您無法從 Insights (深入分析) 頁面手動刪除事件。因為您必須先建立追蹤，才能啟用 CloudTrail Insights，因此只要您將事件存放在追蹤設定中設定的 S3 儲存貯體中，就可以檢視記錄到追蹤中的 Insights 事件。

監控追蹤日誌，並在 Amazon CloudWatch Logs 發生特定洞察事件活動時收到通知。如需詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。

檢視 Insights 事件

CloudTrail 必須在追蹤上啟用深入解析事件，才能在主控台中查看 Insights 事件。如果偵測到異常活動，最多需 CloudTrail 要 36 小時才能傳遞第一個「見解」事件。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/home/。
2. 在導覽窗格中，選擇 Dashboard (儀表板) 查看最近五個 Insights 事件，或選擇 Insights 查看過去 90 天內您帳戶記錄的所有 Insights 事件。

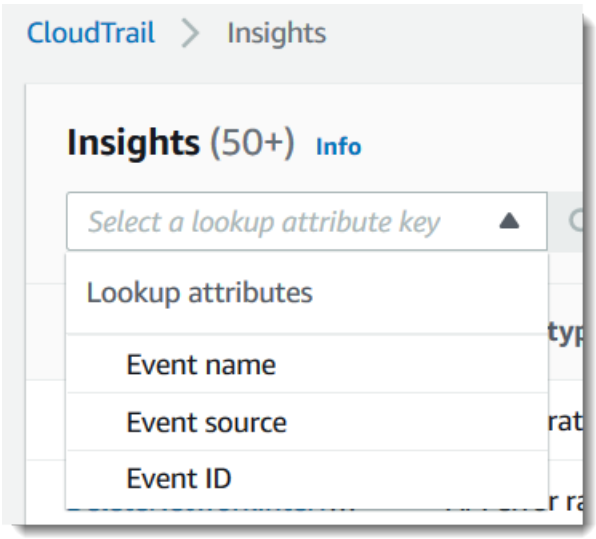
   在 Insights 頁面上，您可以依標準 (包括事件 API 來源、事件名稱和事件 ID) 來篩選 Insights 事件，並將顯示的事件限制在特定時間範圍內發生的事件。如需有關篩選 Insights 事件的詳細資訊，請參閱篩選 Insights 事件。

內容

- 檢視 Insights 事件的詳細資訊
- 縮放、平移和下載圖表
- 變更圖表時間範圍設定
- 下載 Insights 事件

篩選 Insights 事件

Insights (深入分析) 中事件的預設顯示會以反向時間順序顯示事件。最新的 Insights 事件 (按事件開始時間排序) 顯示在頂端。下列清單說明可用的屬性。您可以篩選前三個屬性：Event name (事件名稱)、Event source (事件來源) 及 Event ID (事件 ID)。



事件名稱

事件的名稱，通常是記錄異常活動層級的 AWS API。

洞見類型

CloudTrail 見解事件的類型，也就是 API 呼叫率或 API 錯誤率。API 呼叫率洞見類型會分析針對基準 API 呼叫量彙總的每分鐘唯寫管理 API 呼叫。API 錯誤率洞見類型會分析導致錯誤碼的管理 API 呼叫。如果 API 呼叫失敗，則顯示錯誤。

事件來源

提出要求的 AWS 服務，例如`iam.amazonaws.com`或`s3.amazonaws.com`。在您選擇 Event source (事件來源) 篩選條件之後，即可捲動事件來源清單。

事件 ID

Insights 事件的 ID。事件 ID不會顯示在 Insights 頁面資料表中，但它們是您可以用來篩選 Insights 事件的屬性。經分析而產生 Insights 事件之管理事件的事件 ID，與 Insights 事件的事件 ID 不同。

事件開始時間

Insights 事件的開始時間，計算方式為記錄異常活動的第一分鐘。此屬性顯示於 Insights 資料表，但您無法在主控台中篩選事件開始時間。

基準平均值

API 呼叫率或錯誤率活動的正常模式。基準平均值是在 Insights 事件開始前七天內計算。雖然基準持續時間 (CloudTrail分析 API 上正常活動的期間) 的值大約是 7 天，但是將基準持續時間 CloudTrail捨入為整數天，以便精確的基準持續時間可能會有所不同。

Insight 平均值

觸發 Insights 事件的 API 呼叫平均數，或呼叫 API 時傳回的特定錯誤的平均數。開始事件的「 CloudTrail 見解」平均值是觸發「見解」事件的發生率。通常情況下，這是異常活動的第一分鐘。結束事件的 Insights 平均值是異常活動持續時間 (開始 Insights 事件和結束 Insights 事件之間) 的發生率。

發生率變化

Baseline average (基準平均值) 和 Insight average (Insight 平均值) 之間的差異 (以百分比測量)。例如，如果 `AccessDenied` 錯誤發生率的基準平均值為 1.0，而 Insight 平均值為 3.0，則發生率變化為 300%。超過基準平均值的 Insight 平均值發生率變化會在數值旁顯示向上箭號。如果因為活動低於基準平均值而記錄 Insights 事件，Rate change (發生率變化) 會在百分比旁顯示向下箭頭。

如果在您所選擇的屬性或時間下沒有記錄的事件，則結果清單會是空的。除了時間範圍之外，您只能套用一個屬性篩選條件。如果您選擇不同的屬性篩選條件，則會保留您指定的時間範圍。

下列步驟說明如何依屬性進行篩選。

依屬性篩選

1. 若要依屬性篩選結果，請從下拉式功能表中選擇查詢屬性，然後在 Enter lookup value (輸入查詢值) 方塊中輸入或選擇值。
2. 若要移除屬性篩選條件，請選擇屬性篩選條件方塊右側的 X。

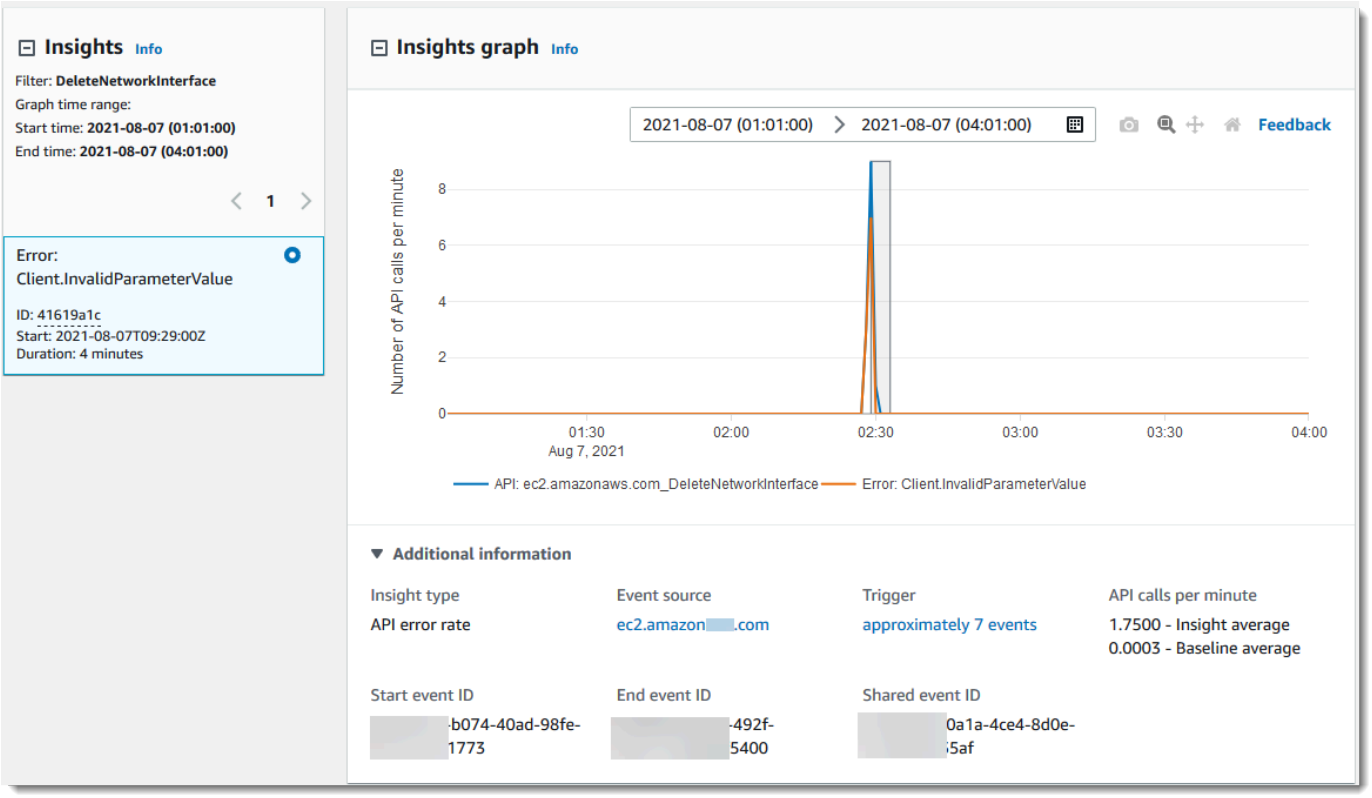
下列步驟說明如何依開始與結束日期及時間進行篩選。

依開始與結束日期及時間進行篩選

1. 若要縮小您要查看之事件的時間範圍，請選擇資料表頂部時間範圍列中的時間範圍。預設的時間範圍包括 30 分鐘、1 小時、3 小時或 12 小時。若要指定自訂時間範圍，請選擇 Custom (自訂)。
2. 選擇下列其中一個索引標籤。
   - 絕對 - 可讓您選擇特定時間。繼續進行下一個步驟。
   - 相對於所選事件 - 預設為已選取。可讓您選擇與 Insights 事件開始時間相關的時段。繼續步驟 4。
3. 若要設定 Absolute (絕對) 時間範圍，請執行下列動作。
   a. 在 Absolute (絕對) 索引標籤上，選擇時間範圍開始的日期。輸入所選日期的開始時間。若要手動輸入日期，請以 `yyyy/mm/dd` 格式輸入日期。開始和結束時間使用 24 小時制，且值必須是格式 `hh:mm:ss`。例如，若要指示下午 6:30 的開始時間，請輸入 **`18:30:00`**。
   b. 選擇行事曆上範圍的結束日期，或在行事曆下方指定結束日期與時間。選擇套用。
4. 若要設定 Relative to selected event (相對於所選事件) 時間範圍，請執行下列動作。
   a. 選擇與 Insights 事件開始時間相關的預設時段。可使用預設值 (分鐘、小時、天或週)。最大相對時段為 12 週。
   b. 如有需要，請在預設集下方的方塊中自訂預設值。選擇 Clear (清除)，視需要重設您的變更。設定您想要的相對時間後，選擇 Apply (套用)。
5. 在 To (至) 中，選擇日期，並指定您想要成為時間範圍結束的時間。選擇套用。
6. 若要移除時間範圍篩選條件，請選擇 Time range (時間範圍) 方塊右側的行事曆圖示，然後選擇 Remove (移除)。

檢視 Insights 事件的詳細資訊

1. 在結果清單中選擇 Insights 事件，以顯示其詳細資訊。Insights 事件的詳細資訊頁面會顯示異常活動時間表的圖表。



2. 將滑鼠停留在反白顯示的頻帶上，以顯示圖表中每個 Insights 事件的開始事件和持續期間。

下列資訊會顯示在圖表的 Additional information (其他資訊) 區域中：

- Insight type (Insight 類型)。這可以是 API 呼叫率或 API 錯誤率。
- 觸發條件。這是 CloudTrail 事件索引標籤的連結，其中會列出已分析以判斷發生異常活動的管理事件。
- 每分鐘 API 呼叫次數
  - Baseline average (基準平均值) - 記錄 Insights 事件的 API 的每分鐘典型發生率 (大約前 7 天內在您帳戶的特定區域中測量)。
  - Insights average (Insights 平均值) - 觸發 Insights 事件的此 API 的每分鐘發生率。開始事件的「CloudTrail 見解」平均值是指觸發見解事件之 API 上每分鐘的呼叫率或錯誤數。通常情況下，這是異常活動的第一分鐘。結束事件的 Insights 平均值是在異常活動持續期間 (開始 Insights 事件和結束 Insights 事件之間)，每分鐘 API 呼叫率或錯誤率。
- Event source (事件來源)。記錄異常 API 呼叫或錯誤數目的 AWS 服務端點。在上述影像中，來源為 `ec2.amazonaws.com`，這是 Amazon EC2 的服務端點。

- Event IDs (事件 ID)。
  - Start event ID (開始事件 ID) - 異常活動開始時記錄的 Insights 事件 ID。
  - End event ID (結束事件 ID) - 異常活動結束時記錄的 Insights 事件 ID。
  - 共用事件 ID-在見解事件中，共用事件 ID 是由 CloudTrail 見解產生的 GUID，可唯一識別洞察事件的開始和結束配對。Shared event ID (共用事件 ID) 在開始和結束 Insights 事件之間共用，有助於在這兩個事件之間建立關聯以唯一識別異常活動。

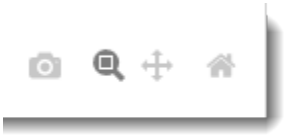
3. 選擇 Attributions (歸因) 索引標籤，可檢視有關使用者身分、使用者代理程式、API 呼叫率 Insights 事件，以及與異常和基準活動相關的錯誤代碼的資訊。Attributions (歸因) 索引標籤上的資料表中最多會顯示五個使用者身分、五個使用者代理程式和五個錯誤碼，按活動計數的平均值按從高到低的降序排列。如需有關 Attributions (歸因) 索引標籤的更多資訊，請參閱本指南中的 Attributions (歸因) 索引標籤 和 CloudTrail 見解`insightDetails`元素。
4. 在CloudTrail 事件索引標籤上，檢視 CloudTrail分析的相關事件，以判斷發生異常活動。依預設，Insights 事件名稱已套用篩選器，這也是相關 API 的名稱。CloudTrail 事件索引標籤會顯示 CloudTrail 與 Insights 事件的開始時間 (減去一分鐘) 和結束時間 (加上一分鐘) 之間發生的主旨 API 相關的管理事件。

   當您在圖形中選取其他 Insights 事件時，事件表格中顯示的CloudTrail 事件會變更。這些事件可協助您執行更深入的分析，以判斷 Insights 事件的可能原因，以及異常 API 活動的原因。

   若要顯示 Insights 事件持續時間期間所 CloudTrail 記錄的所有事件，而不僅是相關 API 的事件，請關閉篩選器。
5. 選擇 Insights event record (Insights 事件記錄) 索引標籤，以 JSON 格式檢視 Insights 開始和結束事件。
6. 選擇連結的 Event source (事件來源) 會返回由該事件來源篩選的 Insights 頁面。

縮放、平移和下載圖表

您可以使用右上角的工具列來縮放、平移和重設 Insights 事件詳細資訊頁面上的圖表軸。



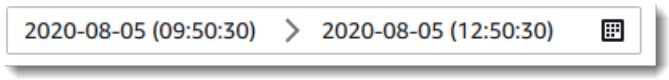
圖表工具列上的命令按鈕從左到右執行以下作業：

- Download plot as a PNG (下載散佈圖為 PNG) - 下載詳細資訊頁面上顯示的圖表影像，並將其儲存為 PNG 格式。

- Zoom (縮放) - 拖曳以在圖表上選取您要放大並更詳細地查看的區域。
- Pan (平移) - 移動圖表以查看相鄰的日期或時間。
- Reset axes (重置軸) - 將圖表軸變更回原始軸，清除縮放和平移設定。

變更圖表時間範圍設定

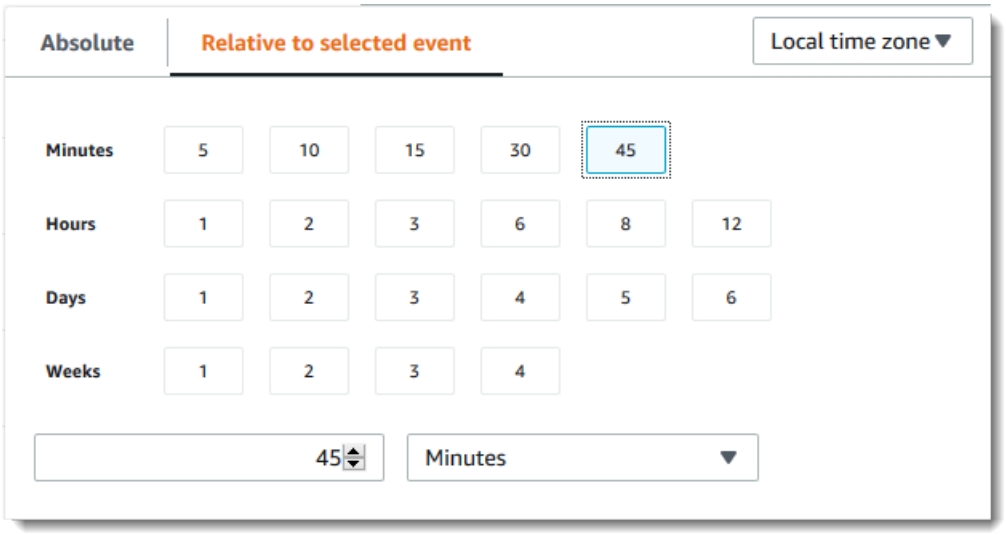
您可以變更時間範圍，也就是顯示在 x 軸 上的所選事件持續期間 - 透過選擇圖表右上角的設定來顯示在圖表中。



圖表中顯示的預設時間範圍，取決於所選 Insights 事件的持續時間。

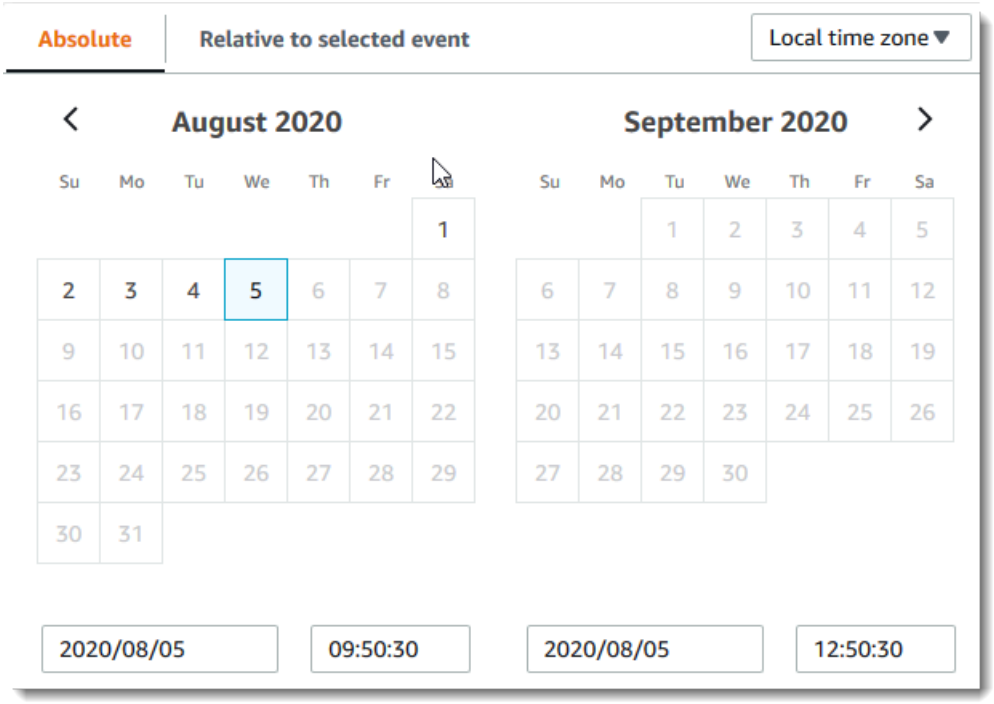
Insights 事件的持續時間	預設時間範圍
少於 4 小時	3h (3 小時)
4 至 12 小時	12h (12 小時)
12 至 24 小時	1d (一天)
24 至 72 小時	3d (三天)
超過 72 小時	1w (一週)

您可以選擇 5 分鐘、30 分鐘、1 小時、3 小時、12 小時的預設集，或自訂。下圖顯示相對於所選事件時段，您可以在自訂設定中選擇。相對時段是指所選 Insights 事件 (顯示在 Insights 事件詳細資訊頁面上) 開始和結束周圍的大約時段。



若要自訂選取的預設集，請在預設集下方的方塊中指定數字和時間單位。

若要指定確切的日期和時間範圍，請選擇 Absolute (絕對) 索引標籤。如果您設定了絕對日期和時間範圍，則需要開始和結束時間。如需設定時間的資訊，請參閱此主題中的 the section called “篩選 Insights 事件”。



下載 Insights 事件

您可以將已記錄的 Insights 事件歷史記錄以 CSV 或 JSON 檔案格式下載。善用篩選條件和時間範圍，減少下載的檔案大小。

> **Note**
>
> CloudTrail 事件歷程記錄檔案是包含可由個別使用者設定的資訊 (例如資源名稱) 的資料檔案。有些資料在用來讀取與分析資料 (CSV injection) 的程式中很可能會被解譯為命令。例如，當 CloudTrail 事件匯出為 CSV 並匯入試算表程式時，該程式可能會警告您有關安全性考量的問題。安全最佳實務是停用下載事件歷史記錄檔中的連結或巨集。

1. 指定您要下載之事件的篩選條件和時間範圍。例如，您可以指定事件名稱 `StartInstances`，並指定活動的時間範圍為最後三天。
2. 選擇 Download events (下載事件)，然後選擇 Download CSV (下載 CSV) 或 Download JSON (下載 JSON)。系統會提示您選擇儲存檔案的位置。

   > **Note**
   >
   > 您的下載可能需要一些時間才能完成。如需更快速的結果，請在您開始下載程序之前，使用更特定的篩選條件或較短的時間範圍來縮小結果範圍。

3. 下載完成後，請開啟檔案，以檢視您指定的事件。
4. 若要取消下載，請選擇 Cancel download (取消下載)。如果您在下載完成之前取消下載，本機電腦上的 CSV 或 JSON 檔案可能只包含部分事件。

檢視追蹤的 CloudTrail 見解事件 AWS CLI

您可以執行aws cloudtrail lookup-events命令，查詢過去 90 天的 CloudTrail 見解事件。此 `lookup-events` 命令提供以下選項：

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

若要取得有關使用的一般資訊 AWS Command Line Interface，請參閱《使AWS Command Line Interface 用指南》。

內容

必要條件

- 若要執行 AWS CLI 命令，您必須安裝 AWS CLI. 如需詳細資訊，請參閱開始使用 AWS CLI.
- 確保您的 AWS CLI 版本大於 1.6.6。若要驗證 CLI 版本，請在命令列上執行 aws --version。
- 若要設定 AWS CLI 工作階段的帳戶、區域和預設輸出格式，請使用aws configure指令。如需詳細資訊，請參閱設定 AWS 命令列界面。
- 若要在 API 呼叫量上記錄 Insights 事件，追蹤必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，追蹤必須記錄 `read` 或 `write` 管理事件。

> **Note**
>
> 這些命 CloudTrail AWS CLI 令是區分大小寫的。

取得命令列說明

若要查看 `lookup-events` 的命令列說明，請輸入下列命令：

```
aws cloudtrail lookup-events help
```

搜尋 Insights 事件

若要查看十個最新的 Insights 事件，請輸入下列命令：

```
aws cloudtrail lookup-events --event-category insight
```

傳回的事件看起來類似下列範例：

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.07",
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
```

```
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                    "average": 0.2
                  }
                ],
                "baseline": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
```

```
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      },
      {
          "eventVersion": "1.07",
          "eventTime": "2019-10-15T21:14:00Z",
          "awsRegion": "us-east-1",
          "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
          "eventType": "AwsCloudTrailInsight",
          "recipientAccountId": "123456789012",
          "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
          "insightDetails": {
          "state": "End",
          "eventSource": "autoscaling.amazonaws.com",
          "eventName": "CompleteLifecycleAction",
          "insightType": "ApiCallRateInsight",
          "insightContext": {
            "statistics": {
              "baseline": {
                "average": 0.0000882145
              },
              "insight": {
                "average": 0.6
              },
              "insightDuration": 5,
              "baselineDuration": 11336
            },
            "attributions": [
              {
                "attribute": "userIdentityArn",
                "insight": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.2
```

```
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
                  ],
                  "baseline": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "userAgent",
                  "insight": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
                    {
                      "value": "codedeploy.amazonaws.com",
                      "average": 0.0000882145
                    }
                  ]
                },
                {
                  "attribute": "errorCode",
                  "insight": [
                    {
                      "value": "null",
                      "average": 0.6
                    }
                  ],
                  "baseline": [
```

```
                    {
                      "value": "null",
                      "average": 0.0000882145
                    }
                  ]
                }
              ]
            }
          },
            "eventCategory": "Insight"
        }
    ]
}
```

如需輸出中查詢相關欄位的說明，請參閱本主題中的查詢輸出欄位。如需 Insights 事件中欄位的說明，請參閱 CloudTrail 記錄內容。

指定要傳回的 Insights 事件數目

若要指定要傳回的事件數目，請輸入下列命令。

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

如果未指定，*<integer>* 的預設值為 10。可能值為 1 到 50。下列範例會傳回一個結果。

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

依時間範圍查詢 Insights 事件

過去 90 天的 Insights 事件可用於查詢。若要指定時間範圍，請輸入下列命令。

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>* 指定 (UTC) 只會傳回在所指定時間或之後發生的 Insights 事件。如果指定的開始時間晚於指定的結束時間，則會傳回錯誤。

`--end-time` *<timestamp>* 指定 (UTC) 只會傳回在所指定時間或之前發生的 Insights 事件。如果指定的結束時間早於指定的開始時間，則會傳回錯誤。

預設的開始時間是過去 90 天內可使用資料的最早日期。預設的結束時間是在最接近目前時間所發生之事件的時間。

所有時間戳記均會以 UTC 顯示。

依屬性查詢 Insights 事件

若要依屬性進行篩選，請輸入下列命令。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

您只能為每個 lookup-events 命令指定一個屬性鍵/值對。以下是 `AttributeKey` 的有效 Insights 事件值。值名稱區分大小寫。

- `EventId`
- `EventName`
- `EventSource`

的最大長度`AttributeValue`為 2000 個字元。以下字符（'_'，"， "，,'\\n'）算作兩個字符，朝著 2000 個字符限制。

屬性查詢範例

下列範例命令會傳回 `EventName` 值為 `PutRule` 的 Insights 事件。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

下列範例命令會傳回 `EventId` 值為 `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002` 的 Insights 事件。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

下列範例命令會傳回 `EventSource` 值為 `iam.amazonaws.com` 的 Insights 事件。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

指定下一頁的結果

若要從 `lookup-events` 命令取得下一頁的結果，請輸入下列命令。

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

在此命令中，*<token>* 的值取自先前命令輸出的第一個欄位。

當您在命令中使用 --next-token 時，必須使用與先前命令相同的參數。例如，假設您執行下列命令。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

若要取得下一頁的結果，您的下一個命令會如下所示。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

從檔案取得 JSON 輸入

對 AWS CLI 於某些 AWS 服務，有兩個參數 --generate-cli-skeleton--cli-input-json，您可以使用它來生成 JSON 模板，您可以修改並用作--cli-input-json參數的輸入。本節說明如何搭配使用這些參數與 aws cloudtrail lookup-events。如需詳細資訊，請參閱AWS CLI 骨架和輸入檔案。

從檔案取得 JSON 輸入來查詢 Insights 事件

1. 將 lookup-events 輸出重新導向至檔案，以建立與 --generate-cli-skeleton 搭配使用的輸入範本，如下列範例所示。

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   產生的範本檔案 (在本例中為 LookupEvents .txt) 如下所示。

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
   ```

```
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. 視需要使用文字編輯器來修改 JSON。JSON 輸入只能包含所指定的值。

> **Important**
>
> 必須先從範本移除所有空白值或 null 值，才能使用它。

下列範例指定時間範圍以及要傳回的結果數目上限。

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. 若要使用編輯過的檔案做為輸入，請使用語法 `--cli-input-json file://<filename>`，如下列範例所示。

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> 您可以在與 `--cli-input-json` 相同的命令列上使用其他引數。

查詢輸出欄位

事件

根據所指定查詢屬性和時間範圍的查詢事件清單。事件清單是依時間排序，而且會先列出最新的事件。每個項目都包含查詢要求的相關資訊，並包含擷取之 CloudTrail 事件的字串表示法。

下列項目說明每個查詢事件中的欄位。

CloudTrailEvent

包含以物件呈現所傳回事件的 JSON 字串。如需所有傳回之元素的資訊，請參閱記錄內文內容。

EventId

字串，包含所傳回事件的 GUID。

EventName

字串，包含所傳回事件的名稱。

EventSource

提出要求的 AWS 服務。

EventTime

事件的日期和時間 (UNIX 時間格式)。

資源

所傳回之事件所參考的資源清單。每個資源項目都會指定資源類型和資源名稱。

ResourceName

字串，包含事件所參考資源的名稱。

ResourceType

字串，包含事件所參考資源的類型。無法判定資源類型時，會傳回 null。

使用者名稱

字串，包含所傳回事件之帳戶的使用者名稱。

NextToken

字串，可從先前的 `lookup-events` 命令取得下一頁的結果。若要使用字符，參數必須與原始命令中的參數相同。如果 `NextToken` 項目未出現在輸出中，則沒有可傳回的其他結果。

如需 CloudTrail 深入解析事件的詳細資訊，請參閱本指南記錄 Insights 事件中的。

將路徑活動複製到 CloudTrail湖

您可以將現有追蹤事件複製到 CloudTrail Lake 事件資料存放區，以建立記錄至追蹤的事件 point-in-time快照。複製追蹤事件不會干擾追蹤記錄事件的功能，也不會以任何方式修改追蹤。

您可以將追蹤事件複製到針 CloudTrail 對事件設定的現有事件資料存放區，也可以建立新的 CloudTrail 事件資料存放區並選擇「複製追蹤事件」選項做為事件資料存放區建立的一部分。如需有關將追蹤事件複製到現有事件資料存放區的詳細資訊，請參閱 使用 CloudTrail 主控台將追蹤事件複製到現有的事件資料存放區。如需有關建立新的事件資料存放區的詳細資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區。

將追蹤事件複製到 CloudTrail Lake 事件資料存放區，可讓您對複製的事件執行查詢。 CloudTrail 與事件歷史記錄或運LookupEvents行中的簡單鍵和值查詢相比，Lake 查詢提供了更深入且更可自定義的事件視圖。如需 CloudTrail 湖泊的更多資訊，請參閱〈〉工作, 由于, AWS CloudTrail 湖。

如果您要將追蹤事件複製到組織事件資料存放區，您必須使用組織的管理帳戶。您無法使用組織的委派管理員帳戶複製追蹤事件。

CloudTrail Lake 事件資料存放區會產生費用。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需有關 CloudTrail 定價和管理 Lake 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 湖泊成本.

將追蹤事件複製到 CloudTrail Lake 事件資料存放區時，會根據事件資料存放區擷取的未壓縮資料量產生費用。

當您將追蹤事件複製到 CloudTrail Lake 時，會 CloudTrail 解壓縮以 gzip (壓縮) 格式儲存的記錄檔，然後將記錄中包含的事件複製到您的事件資料存放區。未壓縮資料的大小可能大於實際的 S3 儲存大小。若要取得未壓縮資料大小的一般估計值，您可以將 S3 儲存貯體中的日誌大小乘以 10。

您可以縮小指定的複製事件的時間範圍，來降低該費用。如果您計劃只使用事件資料存放區來查詢複製的事件，可以關閉事件擷取以避免因未來事件而產生費用。如需詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 湖泊成本。

案例

下表描述一些複製追蹤事件的常見案例，以及您可以如何使用主控台應對每個案例。

案例	我可以如何在主控台中加以應對？
分析和查詢 CloudTrail 湖泊中的歷史跟踪事件，而無需攝入新事件	建立一個新的事件資料存放區，並且在建立事件資料存放區的過程中選擇複製追蹤事件選項。在建立事件資料存放區時，取消選取擷取事件 (程序中的步驟 15)，以確保事件資料存放區僅包含追蹤的歷史事件而不包含未來事件。

案例	我可以如何在主控台中加以應對？
使用 CloudTrail Lake 事件資料存放區取代您現有的追蹤	使用與建立追蹤時所使用的相同事件選取器來建立事件資料存放區，以確保事件資料存放區與您的追蹤有相同的覆蓋範圍。 若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請為複製的事件選擇早於事件資料存放區建立日期的日期範圍。 在建立您的事件資料存放區後，您可以關閉追蹤記錄，以避免產生額外費用。

主題

複製追蹤事件的考量

複製追蹤事件時，請考慮下列因素。

- 複製追蹤事件時， CloudTrail 會使用 S3 `GetObject`API 操作擷取來源 S3 儲存貯體中的追蹤事件。一些 S3 已封存儲存類別無法透過使用 `GetObject` 存取，例如 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Outposts 和 S3 Intelligent-Tiering Deep Archive 層。若要複製儲存在這些已封存儲存類別中的追蹤事件，您必須先使用 S3 `RestoreObject` 操作還原一個複本。如需有關還原已封存物件的詳細資訊，請參閱《Amazon S3 使用者指南》中的還原已封存的物件。
- 將追蹤事件複製到事件資料存放區時， CloudTrail 不論目的地事件資料存放區的事件類型、進階事件選取器或 AWS 區域的組態為何，都會複製所有追蹤事件。
- 將追蹤事件複製到現有的事件資料存放區前，請務必先為您的使用案例妥善設定事件資料存放區的定價選項和保留期。
  - 定價選項：定價選項決定擷取和儲存事件的成本。如需更多關於定價選項的資訊，請參閱 AWS CloudTrail 定價和 事件資料存放區定價選項。
  - 保留期：保留期決定事件資料在事件資料存放區中保留的時間長度。 CloudTrail 僅複製在事件資料存放區保留期`eventTime`內的追蹤事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *`oldest-`*

event-in-days+ *number-days-to-retain*)。例如，如果您要複製的最舊事件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。

- 如果您要複製追蹤事件到事件資料存放區以用於調查，而且不想擷取任何未來事件，您可以停止在事件資料存放區上的擷取。在建立事件資料存放區時，取消選取擷取事件選項 (程序中的步驟 15)，以確保事件資料存放區僅包含追蹤的歷史事件而不包含未來事件。
- 複製追蹤事件之前，請停用連接到來源 S3 儲存貯體的任何存取控制清單 (ACL)，並更新目的地事件資料存放區的 S3 儲存貯體政策。如需更新 S3 儲存貯體政策的詳細資訊，請參閱 複製追蹤事件的 Amazon S3 儲存貯體政策。如需停用 ACL 的詳細資訊，請參閱控制物件的擁有權並停用儲存貯體的 ACL。
- CloudTrail 只會從來源 S3 儲存貯體中的 Gzip 壓縮日誌檔複製追蹤事件。 CloudTrail 不會從未壓縮的記錄檔或使用 Gzip 以外的格式壓縮的記錄檔複製追蹤事件。
- 若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請為複製的事件選擇早於事件資料存放區建立日期的時間範圍。
- 根據預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前綴。如果您要複製其他前置詞中包含的 CloudTrail 事件，則必須在複製追蹤事件時選擇前置詞。
- 若要將追蹤事件複製到組織事件資料存放區，您必須使用組織的管理帳戶。您無法使用委派的管理員帳戶將追蹤事件複製到組織事件資料存放區。

複製追蹤事件所需的許可

複製追蹤事件之前，請確定您擁有 IAM 角色的所有必要許可。如果您選擇現有的 IAM 角色來複製追蹤事件，則只需更新 IAM 角色許可。如果您選擇建立新的 IAM 角色，請 CloudTrail 提供該角色的所有必要許可。

如果來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策允許 CloudTrail 解密儲存貯體中的資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，您必須更新每個金鑰的政策， CloudTrail 以允許解密儲存貯體中的資料。

主題

- 複製追蹤事件的 IAM 許可
- 複製追蹤事件的 Amazon S3 儲存貯體政策
- 用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策

複製追蹤事件的 IAM 許可

複製追蹤事件時，您可以選擇建立新的 IAM 角色，也可以使用現有的 IAM 角色。當您選擇新的 IAM 角色時，請 CloudTrail 建立具有所需許可的 IAM 角色，您不需要進一步採取任何動作。

如果您選擇現有角色，請確保 IAM 角色的政策允許 CloudTrail 從來源 S3 儲存貯體複製追蹤事件。此區段提供所需 IAM 角色許可和信任政策的範例。

下列範例提供許可政策，允許 CloudTrail 從來源 S3 儲存貯體複製追蹤事件。使用適合您組態的值取代*myBucketName*、*MyAccountI eventDataStored*、*##*、*###*和 ID。*MyAccountId* 是用於 CloudTrail 湖泊的 AWS 帳戶識別碼，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

使用用於加密來源 S3 儲存貯體的 KMS 金鑰的值來取代 *key-region*、*keyAccountID* 和 *keyID*。如果來源 S3 儲存貯體不使用 KMS 金鑰進行加密，則您可以省略 `AWSCloudTrailImportKeyAccess` 陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

下列範例提供 IAM 信任政策，該政策 CloudTrail 允許假設 IAM 角色從來源 S3 儲存貯體複製追蹤事件。將 *MyAccount ID*、*##*和 *eventDataStoreID* 取代為您的組態適當的值。*MyAccountId* 是用於 CloudTrail 湖泊的 AWS 帳戶識別碼，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

複製追蹤事件的 Amazon S3 儲存貯體政策

根據預設，所有 Amazon S3 儲存貯體和物件皆為私有。只有資源擁有者 (建立儲存貯體的 AWS 帳戶)，可存取儲存貯體及其包含的物件。資源擁有者可藉由編寫存取政策，將存取許可授予其他資源和使用者。

在複製追蹤事件之前，您必須更新 S3 儲存貯體政策，以 CloudTrail 允許從儲存貯體複製追蹤事件。

您可以將下列陳述式新增至 S3 儲存貯體政策，以授予這些權限。取*# roleArn* 並*myBucketName*使用適合您組態的適當值。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策

如果來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策提 CloudTrail 供從已啟用 SSE-KMS 加密的 S3 儲存貯體複製追蹤事件所需的`kms:GenerateDataKey`權限。`kms:Decrypt`如果您的來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策。更新 KMS 金鑰政策允許解密 CloudTrail 來源 S3 儲存貯體中的資料、執行驗證檢查以確保事件符合 CloudTrail標準，以及將事件複製到 CloudTrail Lake 事件資料存放區。

下列範例提供 KMS 金鑰政策，可讓您解密 CloudTrail 來源 S3 儲存貯體中的資料。*# roleArn#myBucketName##### eventDataStore ID ##################MyAccountId* 是用於 CloudTrail 湖泊的 AWS 帳戶識別碼，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

使用 CloudTrail 主控台將追蹤事件複製到現有的事件資料存放區

使用下列程序將追蹤事件複製到現有的事件資料存放區。如需有關如何建立新事件資料存放區的資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區。

> **Note**
>
> 將追蹤事件複製到現有的事件資料存放區前，請務必先為您的使用案例妥善設定事件資料存放區的定價選項和保留期。
>
> - 定價選項：定價選項決定擷取和儲存事件的成本。如需更多關於定價選項的資訊，請參閱 AWS CloudTrail 定價和 事件資料存放區定價選項。
> - 保留期：保留期決定事件資料在事件資料存放區中保留的時間長度。 CloudTrail 僅複製在事件資料存放區保留期eventTime內的追蹤事件。若要決定適當的保留期間，請採用您要複製的最舊事件的總和 (以天為單位)，以及要在事件資料存放區中保留事件的天數 (保留期間 = *oldest-event-in-days*+ *number-days-to-retain*)。例如，如果您要複製的最舊事

件為 45 天前的事件，並希望這些事件在事件資料存放區中再保留 45 天，則可以將保留期設為 90 天。

若要將追蹤事件複製到事件資料存放區

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 主控台左側導覽窗格中選擇 [追蹤]。
3. 在 Trails (追蹤) 頁面上，選擇相應的追蹤，然後選擇 Copy events to Lake (將事件複製到 Lake)。如果追蹤的來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確定 KMS 金鑰政策允許 CloudTrail 解密儲存貯體中的資料。如果來源 S3 儲存貯體使用多個 KMS 金鑰，您必須更新每個金鑰的政策，以允許 CloudTrail 解密儲存貯體中的資料。如需更新 KMS 金鑰政策的詳細資訊，請參閱 用於解密來源 S3 儲存貯體中資料的 KMS 金鑰政策。
4. (選擇性) 依預設， CloudTrail 只會複製 S3 儲存貯體`CloudTrail`前綴中包含的 CloudTrail 事件和前綴內的`CloudTrail`前綴，而不會檢查其他 AWS 服務的前置詞。如果您要複製其他前置詞中包含的 CloudTrail 事件，請選擇 [輸入 S3 URI]，然後選擇 [瀏覽 S3] 以瀏覽至首碼。

   S3 儲存貯體政策必須授予複製追蹤事件的 CloudTrail 存取權。如需更新 S3 儲存貯體政策的詳細資訊，請參閱 複製追蹤事件的 Amazon S3 儲存貯體政策。
5. 對於指定事件的時間範圍，請選擇複製事件的時間範圍。 CloudTrail 在嘗試複製追蹤事件之前，先檢查字首和記錄檔名稱，以確認名稱包含在所選開始日期與結束日期之間的日期。您可以選擇 Relative range (相對範圍) 或 Absolute range (絕對範圍)。若要避免來源追蹤和目的地事件資料存放區之間發生重複事件，請選擇早於事件資料存放區建立日期的時間範圍。

   > **Note**
   >
   > CloudTrail 僅複製在事件資料存放區保留期`eventTime`內的追蹤事件。例如，如果事件資料存放區的保留期為 90 天，則不 CloudTrail 會複製任何`eventTime`超過 90 天的追蹤事件。

   - 如果您選擇「相對範圍」，則可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。 CloudTrail 複製所選期間內記錄的事件。
   - 如果選擇「絕對範圍」，則可以選擇特定的開始日期和結束日期。 CloudTrail 複製所選開始日期和結束日期之間發生的事件。

6. 對於 Delivery location (交付地點)，從下拉式清單中選擇目的地事件資料存放區。
7. 對於 Permissions (許可)，從下列 IAM 角色選項中選擇。如果您選擇現有的 IAM 角色，請確認 IAM 角色政策提供必要的許可。如需更新 IAM 角色許可的詳細資訊，請參閱複製追蹤事件的 IAM 許可。
   - 選擇 Create a new role (recommended) (建立新角色 (建議使用)) 以建立新的 IAM 角色。對於 Enter IAM role name (輸入 IAM 角色名稱)，請輸入角色的名稱。 CloudTrail 會自動為這個新角色建立必要的權限。
   - 選擇「使用自訂 IAM 角色 ARN」以使用未列出的自訂 IAM 角色。對於 Enter IAM role ARN (輸入 IAM 角色 ARN)，輸入 IAM ARN。
   - 從下拉式清單中選擇現有的 IAM 角色。
8. 選擇 Copy events (複製事件)。
9. 系統會提示您確認複製。當您就緒確認時，請選擇 Copy trail events to Lake (將追蹤事件複製到 Lake)，接著選擇 Copy events (複製事件)。
10. 在 Copy details (複製詳細資訊) 頁面中，您可檢視複製狀態並檢閱任何失敗。追蹤事件複製完成時，如果沒有錯誤，則其 Copy status (複製狀態) 設定為 Completed (完成)；如果發生錯誤，則設定為 Failed (失敗)。

    > **Note**
    >
    > 事件複製詳細資訊頁面上顯示的詳細資訊不是即時的。實際的詳細資訊值 (例如 Prefixes copied (複製的字首)) 可能會高於頁面上顯示的值。 CloudTrail 在事件副本的過程中逐步更新詳細信息。

11. 如果 Copy status (複製狀態) 是 Failed (失敗)，修正 Copy failures (複製失敗) 中顯示的任何錯誤，接著選擇 Retry copy (重試複製)。當您重試副本時，會在發生失敗的位置 CloudTrail 繼續複製。

如需檢視追蹤事件複製之詳細資訊，請參閱 事件複製詳細資訊。

取得及檢視您的 CloudTrail 記錄檔

在您建立線索並設定其擷取您要的日誌檔案後，您必須要能夠找到日誌檔案，並解釋其中所包含的資訊。

CloudTrail 將日誌檔交付到您在建立追蹤時指定的 Amazon S3 儲存貯體。 CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內提供記錄檔。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。Insights 事件通常會在異常活動的 30 分鐘內送達您的儲存貯體。第一次啟用 Insights 事件之後，如果偵測到異常的活動，可能需等待 36 小時才能看到第一個 Insights 事件。

> **Note**
>
> 如果您錯誤設定追蹤 (例如，無法連線 S3 儲存貯體)， CloudTrail 將嘗試將日誌檔重新傳送到 S3 儲存貯體 30 天，而且這些 attempted-to-deliver 事件將收取標準費用。 CloudTrail 若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

主題

尋找您的 CloudTrail 記錄檔

CloudTrail 將日誌文件發佈到 gzip 存檔中的 S3 存儲桶。在 S3 儲存貯體中，日誌檔案都有包含下列元素的格式化名稱：

- 您在建立追蹤時指定的值區名稱 (可在 CloudTrail 主控台的「追蹤」頁面找到)
- 在您建立線索時指定的 (選用) 前綴
- 字串 "AWSLogs」
- 帳戶號碼
- 字串 "CloudTrail」
- 區域識別符，例如 us-west-1
- 發佈日誌檔案的年份，格式為 YYYY
- 發佈日誌檔案的月份，格式為 MM
- 發佈日誌檔案的日期，格式為 DD
- 在涵蓋的相同時段中，能自其他檔案區分該檔案的英數字串

下列範例顯示完整的日誌檔案物件名稱：

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> 對於組織追蹤，S3 儲存貯體中的日誌檔物件名稱會在路徑中包含組織單位 ID，如下所示：
>
> ```
> bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

若要擷取日誌檔案，您可以使用 Amazon S3 主控台、Amazon S3 命令列界面 (CLI) 或 API。

使用 Amazon S3 主控台找到日誌檔案

1. 開啟 Amazon S3 主控台。
2. 選擇您指定的儲存貯體。
3. 瀏覽物件階層，直到找到您要的日誌檔案。

   所有日誌檔案的副檔名都是 .gz。

您將瀏覽與下列範例類似的物件階層，但使用不同的儲存貯體名稱、帳戶 ID、區域和日期。

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

上述物件階層的日誌檔案如下所示：

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> 雖然很少見，但是您可能會收到包含一或多個重複事件的日誌檔案。在大多數情況下，重複的事件會有相同的 `eventID`。如需 `eventID` 欄位的相關資訊，請參閱 CloudTrail 記錄內容。

下載您的 CloudTrail 記錄檔

日誌檔案為 JSON 格式。如果您已安裝 JSON 檢視器附加功能，則可以直接在瀏覽器中檢視檔案。按兩下儲存貯體中的日誌檔案名稱，以開啟新的瀏覽器視窗或標籤。JSON 會以可讀取格式顯示。

CloudTrail 日誌文件是 Amazon S3 對象。您可以使用 Amazon S3 主控台、 AWS Command Line Interface (CLI) 或 Amazon S3 API 擷取日誌檔案。

如需詳細資訊，請參閱 Amazon S3 物件概觀 (位於 Amazon 簡單儲存服務使用者指南)。

下列程序說明如何使用 AWS Management Console下載日誌檔案。

下載和讀取日誌檔案

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 選擇儲存貯體，然後選擇您想要下載的日誌檔案。
3. 選擇 Download (下載) 或 Download as (下載為)，然後遵循提示來儲存檔案。這會以壓縮格式儲存檔案。

   > **Note**
   >
   > 有些瀏覽器 (例如 Chrome) 會自動解壓縮日誌檔案。如果您的瀏覽器自動執行這項操作，則請跳到步驟 5。

4. 使用 7-Zip 這類產品來解壓縮日誌檔案。
5. 在 Notepad++ 這類文字編輯器中開啟日誌檔案。

如需可出現在日誌檔案項目中之事件欄位的詳細資訊，請參閱「CloudTrail 記錄內容」。

AWS 與第三方專家合作進行記錄和分析，以提供使用 CloudTrail 輸出的解決方案。如需詳細資訊，請參閱AWS CloudTrail 合作夥伴。

> **Note**
>
> 您也可以使用「事件歷史記錄」功能來查詢過去 90 天期間之建立、更新和刪除 API 活動的事件。
> 如需更多詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。

設定 Amazon SNS 通知 CloudTrail

您可以在將新的日誌檔 CloudTrail 發佈到 Amazon S3 儲存貯體時收到通知。您可以使用 Amazon Simple Notification Service (Amazon SNS) 來管理通知。

通知為選用。如果需要通知，可 CloudTrail 以設定為在傳送新的日誌檔時將更新資訊傳送至 Amazon SNS 主題。若要收到這些通知，您可以使用 Amazon SNS 來訂閱主題。身為訂閱者，您會收到傳送到 Amazon Simple Queue Service (Amazon SQS) 佇列的更新，這可讓您透過編寫程式的方式處理這些通知。

主題

設定 CloudTrail 傳送通知

您可以設定線索來使用 Amazon SNS 主題。您可以使用主 CloudTrail 控台或 aws cloudtrail create-trailCLI 命令建立主題。 CloudTrail 為您建立 Amazon SNS 主題並附加適當的政策，以便 CloudTrail 擁有發佈到該主題的權限。

在您建立 SNS 主題名稱時，名稱必須符合下列要求：

- 長度介於 1 與 256 個字元之間
- 包含大小寫 ASCII 字母、數字、底線或連字號

當您為套用至所有區域的追蹤設定通知時，所有區域的通知會傳送至您指定的 Amazon SNS 主題。如果您有一或多個區域特定追蹤，則必須為每個區域建立單獨主題，並分別訂閱每個主題。

若要接收通知，請訂閱 Amazon SNS 主題或 CloudTrail 使用的主題。您可以使用 Amazon SNS 主控台或 Amazon SNS CLI 命令執行這項作業。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的訂閱 Amazon SNS 主題。

> **Note**
>
> CloudTrail 當日誌檔案寫入 Amazon S3 儲存貯體時傳送通知。作用中的帳戶可能會產生大量通知。如果您透過電子郵件或 SMS 進行訂閱，就會收到為數龐大的訊息。建議您使用 Amazon Simple Queue Service (Amazon SQS) 訂閱，可讓您透過編寫程式的方式處理通知。如需詳細資訊，請參閱 Amazon Simple Queue Service 開發人員指南中的訂閱 Amazon SNS 主題 (主控台) 的 Amazon SQS 佇列。

Amazon SNS 通知中含有具 `Message` 欄位的 JSON 物件。`Message` 欄位會列出日誌檔案的完整路徑，如下列範例所示：

```
{
    "s3Bucket": "your-bucket-name","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

如果將多個日誌檔案交付至您的 Amazon S3 儲存貯體，則通知可能會包含多個日誌，如下列範例所示：

```
{
    "s3Bucket": "your-bucket-name",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

如果您選擇透過電子郵件接收通知，則電子郵件內文會包含 `Message` 欄位的內容。如需 JSON 結構的相關資訊，請參閱 Amazon 簡單通知服務開發人員指南中的扇出至 Amazon SQS 佇列。只有`Message`欄位會顯示 CloudTrail 資訊。其他欄位包含 Amazon SNS 服務中的資訊。

如果您使用 CloudTrail API 建立追蹤，您可以指定要與`CreateTrail`或`UpdateTrail`作業一起傳 CloudTrail 送通知的現有 Amazon SNS 主題。您必須確定主題是否存在，而且它具有允許傳送通知 CloudTrail 給該主題的權限。請參閱Amazon SNS 主題政策 CloudTrail。

其他資源

如需 Amazon SNS 主題及訂閱方式的詳細資訊，請參閱 Amazon Simple Notification Service 開發人員指南。

管理線索的秘訣

- 從 2019 年 4 月 12 日開始，追蹤只能在其記錄事件的 AWS 區域 位置檢視。如果您創建了一個記錄事件的跟踪 AWS 區域，它將顯示在您正在工作的AWS 分區中的所有 AWS 區域 控制台中。如果您建立僅記錄單一事件的追蹤 AWS 區域，則只能在該記錄中檢視和管理它 AWS 區域。
- 若要編輯清單中的線索，請選擇線索名稱。
- 請至少設定一個套用至所有區域的追蹤，以便您從您正在使用的 AWS 分割區中的所有區域接收記錄檔。
- 若要記錄特定區域中的事件，並將日誌檔案傳遞至相同區域中的 S3 儲存貯體，您可以更新追蹤以套用至單一區域。如果您想要分開日誌檔案，這十分有用。例如，您可能希望用戶在特定區域中管理自己的日誌，或者您可能希望按地區分隔 CloudWatch 日誌警報。
- 若要在一個追蹤中記錄來自多個 AWS 帳戶的事件，請考慮在中建立組織， AWS Organizations 然後建立組織追蹤。
- 建立多個線索會產生額外的成本。如需定價的詳細資訊，請參閱 AWS CloudTrail 定價。

管理 CloudTrail 追蹤成本

最佳做法是，我們建議您使用可協助您管理 CloudTrail 成本的 AWS 服務和工具。您也可以透過擷取所需資料的方式設定和管理 CloudTrail 追蹤，同時保持符合成本效益。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

協助管理成本的工具

AWS 預算是的一項功能 AWS Billing and Cost Management，可讓您設定自訂預算，以便在成本或用量超過 (或預測超過) 您的預算金額時提醒您。

當您建立多個追蹤時，建議您使 CloudTrail 用「 AWS 預算」建立預算是最佳做法，可協助您追蹤 CloudTrail 支出。基於成本的預算有助於提高您的使用可能需要支付多少費 CloudTrail 用的認識。 當

帳單達到您定義的閾值時，預算警示會通知您。收到預算提醒時，您可以在計費週期結束之前進行變更，以便管理您的成本。

建立預算後，您可以使用 AWS Cost Explorer 來查看 CloudTrail 成本如何影響整體帳 AWS 單。在 Co AWS st Explorer 中，新增 CloudTrail 至服務篩選器之後，您可以依區域和帳戶比較您目前 month-to-date (MTD) 支出的歷史 CloudTrail支出。此功能可協助您監控和偵測每月 CloudTrail支出中的非預期成本。Cost Explorer 中的其他功能可讓您比較 CloudTrail 特定資源層級的支出與每月支出，提供有關可能導致帳單成本增加或減少的資訊。

> **Note**
>
> 雖然您可以將標記套用至 CloudTrail 追蹤，但目前 AWS Billing 無法使用套用至追蹤以進行成本分配的標記。Cost Explorer 可以顯示 CloudTrail Lake 事件資料存放區和整體 CloudTrail 服務的成本。

若要開始使用 AWS 預算，請開啟 AWS Billing and Cost Management，然後選擇左側導覽列中的 [預算]。建議您在建立預算以追蹤 CloudTrail 支出時，設定預算警示。如需如何使用 AWS 預算的詳細資訊，請參閱使用管理成本 AWS Budgets和的最佳做法 AWS Budgets。

追蹤組態

CloudTrail 在帳戶中配置跟踪的方式提供了靈活性。您在設定過程中所做的一些決定需要您瞭解 CloudTrail 帳單的影響。以下是軌跡組態如何影響帳單的範 CloudTrail 例。

建立多重追蹤

每個區域內的第一個管理事件副本是免費提供的。例如，如果您的帳戶有 2 個單一區域追蹤、一個追蹤`us-east-1`和另一個追蹤`us-west-2`，則不會 CloudTrail 收取任何費用，因為每個個別區域中只有一個追蹤記錄事件。不過，如果您的帳戶具有多區域追蹤和額外的單一區域追蹤，則單一區域追蹤會產生費用，因為多區域追蹤已在每個區域中記錄事件。

如果您建立更多追蹤，將相同的管理事件傳遞至其他目的地，則這些後續交付會產生 CloudTrail 成本。您可以執行此操作，允許不同的使用者群組 (如開發人員、安全性人員及 IT 稽核員) 接收日誌檔案的複本。對於資料事件，所有傳送都會產生 CloudTrail 費用，包括第一筆交付。

建立更多追蹤時，應熟悉您的日誌，並了解在您的帳戶內資源產生的事件類型和數量。這有助於您預測與帳戶相關的事件數量，並計畫追蹤費用。例如，在 S3 儲存貯體上使用 AWS KMS受管伺服器端加密 (SSE-KMS) 可能會導致大量的 AWS KMS 管理事件發生。 CloudTrail橫跨多重追蹤的大量事件也會影響費用。

為了協助限制記錄到追蹤的事件數量，您可以在「建立追蹤」 AWS KMS 或「更新追蹤」頁面上選擇「排除 AWS KMS 事件」或「排除 Amazon RDS 資料 API 事件」來篩選掉或 Amazon RDS 資料 API 事件。使用基本事件選取器時，您只能篩選管理事件。但是，您可以使用進階事件選取器同時篩選管理和資料事件。您可以使用進階事件選取器，根據 `resources.type`、`eventName`、`resources.ARN` 和 `readOnly` 欄位來包含或排除資料事件，從而只記錄您感興趣的資料事件。如需如何設定這些欄位的詳細資訊，請參閱AdvancedFieldSelector。如需建立或更新追蹤的詳細資訊，請參閱本指南中的 建立追蹤 或 更新追蹤。

AWS Organizations

當您使用設定「組 Organizations」追蹤時 CloudTrail，會將追蹤 CloudTrail 複製到組織內的每個成員帳戶。除了成員帳戶內的任何現有追蹤之外，也會建立新的追蹤。由於組織追蹤組態會傳播至所有帳戶，因此請確定您的組織追蹤組態符合您想要追蹤為組織內所有帳戶設定的方式。

由於 Organizations 會在各成員帳戶中建立追蹤，因此建立其他追蹤來收集同樣做為 Organizations 追蹤之管理事件的個別成員帳戶便會收集事件的第二個複本。帳戶需要為第二個複本付費。同樣地，如果帳戶擁有多區域追蹤，並在單一區域內建立第二個追蹤，以收集做為多區域追蹤的相同管理事件，則單一區域內的追蹤便會傳遞事件的第二個複本。第二個複本會產生費用。

另請參閱

- AWS CloudTrail 定價
- 管理您的成本 AWS Budgets
- Cost Explorer 入門
- 準備建立組織追蹤

命名要求

本節提供資 CloudTrail 源、Amazon S3 儲存貯體和 KMS 金鑰的命名需求相關資訊。

主題

- CloudTrail 資源命名需求
- Amazon S3 儲存貯體命名需求
- AWS KMS 別名命名需求

CloudTrail 資源命名需求

CloudTrail 資源名稱必須符合下列需求：

- 只包含 ASCII 字母 (a-z、A-Z)、數字 (0-9)、句點 (.)、底線 (_) 或破折號 (-)。
- 開頭是字母或數字，而結尾是字母或數字。
- 介於 3 到 128 個字元之間。
- 沒有相鄰的句點、底線或破折號。my-_namespace 和 my-\-namespace 這類名稱無效。
- 不是 IP 地址格式 (例如，192.168.5.4)。

Amazon S3 儲存貯體命名需求

用於存放 CloudTrail 日誌檔的 Amazon S3 儲存貯體的名稱必須符合非美國標準區域的命名要求。Amazon S3 會將儲存貯體名稱定義為一系列的一或多個標籤 (以句點區隔)。如需查看命名規則的完整清單，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體命名規則。

下列是一些規則：

- 儲存貯體名稱的長度可以介於 3 與 63 個字元之間，而且只能包含小寫字元、數字、句點和破折號。
- 儲存貯體名稱中每個標籤的開頭必須是小寫字母或數字。
- 儲存貯體名稱不能包含底線、結尾為破折號、有連續的句點，或在鄰近句點的位置使用破折號。
- 儲存貯體名稱不能格式化為 IP 地址 (198.51.100.24)。

> **Warning**
>
> 因為 S3 可讓您的儲存貯體做為可公開存取的 URL 使用，所以您選擇的儲存貯體名稱必須是全域唯一的。如果有其他帳戶已使用您選擇的名稱建立儲存貯體，您則必須使用其他名稱。如需詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的儲存貯體限制與局限。

AWS KMS 別名命名需求

建立別名時 AWS KMS key，您可以選擇要識別的別名。例如，您可以選擇別名「KMS-CloudTrail US-us-west-2" 來加密特定追蹤的記錄。

別名必須符合下列需求：

- 介於 1 到 256 (含) 個字元之間
- 包含英數字元 (A-Z、a-z、0-9)、連字號 (-)、正斜線 (/) 和底線 (_)
- 開頭不能是 aws

如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的建立金鑰。

建立多個追蹤

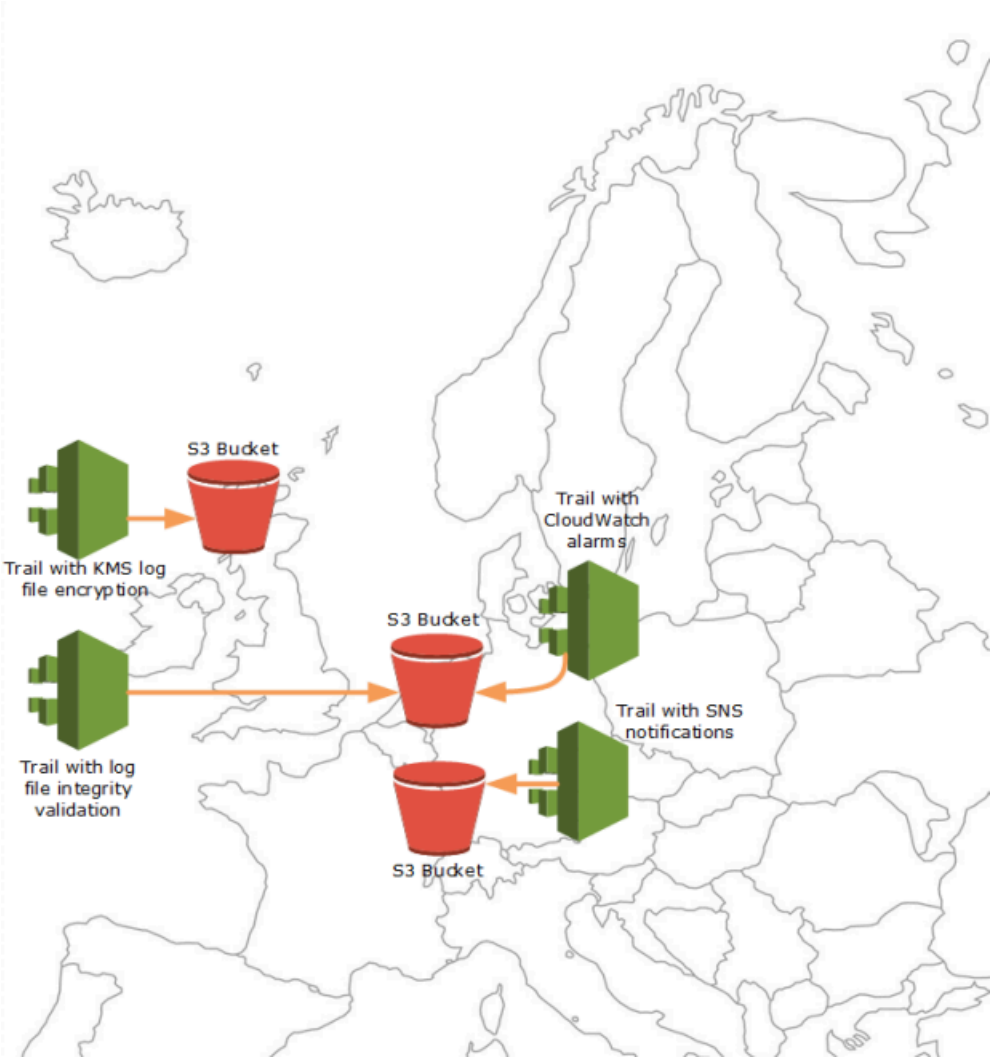
您可以使用 CloudTrail 記錄檔來疑難排解 AWS 帳戶中的操作或安全性問題。您可以為不同使用者建立追蹤，他們可以建立並管理自己的追蹤。您可以設定追蹤將日誌檔案交付到獨立的 S3 儲存貯體或共享的 S3 儲存貯體。

> **Note**
>
> 帳戶中每個管理事件的第一 AWS 區域 個副本是免費的。如果您建立更多追蹤，將相同的管理事件傳遞至其他目的地，則這些後續交付會產生 CloudTrail 成本。如需有關 CloudTrail 成本的詳細資訊，請參閱AWS CloudTrail 定價和管理 CloudTrail 追蹤成本.

例如，您可能有下列使用者：

- 安全管理員在 歐洲 (愛爾蘭) 區域中建立追蹤並設定 KMS 日誌檔案加密。該追蹤將日誌檔案交付到歐洲 (愛爾蘭) 區域中的 S3 儲存貯體。
- IT 稽核人員會在歐洲 (愛爾蘭) 區域建立追蹤，並設定記錄檔完整性驗證，以確保記錄檔自 CloudTrail 傳送之後並未變更。該追蹤經設定會將日誌檔案交付到歐洲 (法蘭克福) 區域中的 S3 儲存貯體
- 開發人員在歐洲 (法蘭克福) 區域建立追蹤，並設定 CloudWatch 警示以接收特定 API 活動的通知。該追蹤與為日誌檔案完整性設定的追蹤共享同一個 S3 儲存貯體。
- 另一個開發人員在歐洲 (法蘭克福) 區域中建立追蹤並設定 SNS。日誌檔案會交付到歐洲 (法蘭克福) 區域中的獨立 S3 儲存貯體。

下圖說明此範例。



> **Note**
>
> 每個最多可以建立五個軌跡 AWS 區域。多區域追蹤計為每個區域的一個追蹤。

您可以使用資源層級權限來管理使用者在上執行特定作業的能力。 CloudTrail

例如，您可以授予某使用者檢視追蹤活動的許可，但禁止使用者啟動或停止記錄追蹤。您可以授予另一位使用者建立和刪除追蹤的完整許可。這可讓您精細控制您的追蹤和使用者存取權。

如需資源層級許可的詳細資訊，請參閱「範例：在特定追蹤建立和套用政策的動作」。

如需有關多個追蹤的詳細資訊，請參閱CloudTrail 常見問題集。

控制 CloudTrail 追蹤的使用者權限

AWS CloudTrail 與 AWS Identity and Access Management (IAM) 整合，協助您控制存取權限 CloudTrail 和其他 CloudTrail 需要的 AWS 資源。這些資源的範例包括 Amazon S3 儲存貯體和 Amazon Simple Notification Service (Amazon SNS) 主題。您可以使用 IAM 控制哪些使用 AWS 者可以建立、設定或刪除 CloudTrail 追蹤、啟動和停止記錄，以及存取包含記錄資訊的值區。如需進一步了解，請參閱的 Identity and Access Management AWS CloudTrail。

下列主題可協助您瞭解權限、原則和 CloudTrail 安全性：

- 授與CloudTrail 管理權限
- Amazon S3 儲存貯體命名規則
- Amazon S3 存儲桶政策 CloudTrail
- 建立組織的追蹤 AWS Command Line Interface 中的組織線索儲存貯體政策的範例
- Amazon SNS 主題政策 CloudTrail
- 使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)
- 複製追蹤事件所需的許可
- 指派委派管理員所需的許可
- 在 CloudTrail 主控台中建立預設 KMS 金鑰原則
- 授與檢視 CloudTrail 主控台 AWS Config 資訊的權限
- 在 AWS 帳戶之間共用 CloudTrail 記錄檔
- 建立組織線索的必要許可
- 使用先前存在的 IAM 角色將組織追蹤的監控新增至 Amazon 日誌 CloudWatch

AWS CloudTrail 與介面 VPC 端點搭配使用

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 託管資 AWS 源，則可以在 VPC 和. 之間建立私有連接。 AWS CloudTrail您可以使用此連線 CloudTrail 來啟用與 VPC 上的資源進行通訊，而無需透過公用網際網路。

Amazon VPC 是一項 AWS 服務，可用於在您定義的虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。使用 VPC 端點時，VPC 和 AWS 服務之間的路由由由 AWS 網路處理，您可以使用 IAM 政策來控制對服務資源的存取。

若要將 VPC 連接到 CloudTrail，您需要為的定義介面 VPC 端點。 CloudTrail介面端點是具有私有 IP 位址的 elastic network interface，可做為傳送至支援 AWS 服務之流量的進入點。端點提供可靠、可擴充的連線能力， CloudTrail 無需網際網路閘道、網路位址轉譯 (NAT) 執行個體或 VPN 連線。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的什麼是 Amazon VPC。

介面 VPC 私人雲端端點的支援是一種使用具有私有 IP 位址的 elastic network interface AWS PrivateLink，在 AWS 服務之間進行私人通訊的 AWS 技術。如需詳細資訊，請參閱AWS PrivateLink。

下列步驟適用於 Amazon VPC 的使用者。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 Amazon VPC 入門。

可用性

CloudTrail 目前支援下列 AWS 區域中的 VPC 端點：

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 非洲 (開普敦)
- 亞太區域 (香港)
- 亞太區域 (海德拉巴)
- 亞太區域 (雅加達)
- 亞太區域 (墨爾本)
- 亞太區域 (孟買)
- 亞太區域 (大阪)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太區域 (雪梨)
- 亞太區域 (東京)
- 加拿大 (中部)
- 加拿大西部 (卡加利)
- 歐洲 (法蘭克福)

- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (米蘭)
- Europe (Paris)
- 歐洲 (西班牙)
- 歐洲 (斯德哥爾摩)
- 歐洲 (蘇黎世)
- 以色列 (特拉維夫)
- Middle East (Bahrain)
- 中東 (阿拉伯聯合大公國)
- 南美洲 (聖保羅)
- AWS GovCloud (美國東部)
- AWS GovCloud (美國西部)

為以下項目建立 VPC 端點 CloudTrail

若要開 CloudTrail 始使用您的 VPC，請為. CloudTrail 如需詳細資訊，請參閱 Amazon VPC AWS 服務使用者指南中的使用介面 VPC 端點存取。

您不需要變更的設定 CloudTrail。 CloudTrail 使用公 AWS 服務 用端點或私有介面 VPC 端點 (以使用中為準) 來呼叫其他端點。

共用子網路

CloudTrail VPC 端點與任何其他 VPC 端點一樣，只能由共用子網路中的擁有者帳戶建立。但是，參與者帳戶可以在與參與者帳戶共用的子網路中使用 CloudTrail VPC 端點。如需有關 Amazon VPC 共用的詳細資訊，請參閱《Amazon VPC 使用者指南》中的與其他帳戶共用 VPC。

AWS 帳戶 封閉和步道

AWS CloudTrail 持續監控並記錄任何使用者、角色或 AWS 服務 AWS 帳戶. 使用者可以建立 CloudTrail 追蹤，在自己擁有的 S3 儲存貯體中接收這些事件的副本。

CloudTrail 是一項基礎安全服務，因此，用戶創建的跟踪即使在關閉之後仍然存在並傳遞事件，除非用戶在關閉 AWS 帳戶 之前明確刪除其中的跟踪。 AWS 帳戶 此行為也適用於由管理帳戶或委派管理員

建立的組織追蹤，以及在組織成員帳戶中建立的多區域組織追蹤。這能確保如果使用者重新開啟已關閉的帳戶，他們能擁有不中斷的帳戶活動記錄。此外還能讓使用者了解任何最終帳戶活動，包括刪除及終止剩餘的帳戶資源和服務。

用戶可以選擇在關閉其之前刪除跟踪 AWS 帳戶，或者在關閉後聯繫AWS Support以請求刪除跟踪。AWS 帳戶

如需關閉的詳細資訊 AWS 帳戶，請參閱關閉 AWS 帳戶.

> **Note**
>
> 如果啟用記 CloudTrail 錄檔驗證，使用者將繼續收到每小時摘要檔案，指出是否已建立任何 CloudTrail 記錄檔。
> CloudTrail 湖泊事件資料存放區、用於整合的 CloudTrail 湖泊通道、 CloudTrail 服務連結通道以及針對追蹤建立的資源 (例如，已關閉帳戶中存在的 Amazon CloudWatch 日誌記錄群組和 Amazon S3 儲存貯體)、遵循帳戶關閉的標準 AWS 行為，並在關閉後期間 (通常為 90 天) 後永久刪除。

進行設 CloudTrail 定

您可以使用主 CloudTrail 控台上的 [設定] 頁面來設定和檢閱 CloudTrail 設定。

存取 「設定」 頁面

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail主控台左側導覽窗格中選擇 [設定]。
3. 視需要檢閱並更新您的設定。

   可用的設定如下：

   - 組織委派管理員 — 如果您有組 AWS Organizations 織，您可以檢視 CloudTrail 委派管理員、新增委派管理員 (最多三個)，以及移除委派管理員。只有組織的管理帳戶可以新增或移除委派管理員。

     組織的管理帳戶可以將組織內的任何帳戶指 CloudTrail 派為委派管理員，以代表組織管理組織的追蹤和事件資料存放區。
   - 服務連結通道— 您可以查看為您的帳戶創建的任何服務鏈接渠道。

     AWS 服務 可以創建服務鏈接渠道以代表您接收 CloudTrail 事件。建立 AWS 服務連結通道的服務會為通道設定進階事件選取器，並指定通道是套用至所有通道 AWS 區域，還是單一通道。AWS 區域

組織委派的管理員

當您與 AWS Organizations 組織 CloudTrail 搭配使用時，您可以指派組織內的任何帳戶，以作為 CloudTrail 委派管理員，以代表組織管理組織的追蹤和事件資料存放區。委派的系統管理員是組織中的成員帳戶，可以執行與管理帳戶相同的管理工作 (除非另有說明)。 CloudTrail

如果您選擇委派的管理員，則此成員帳戶具有組織中所有組織追蹤和事件資料存放區的管理許可。新增委派的管理員不會改變組織追蹤或事件資料存放區的管理或操作。

第一次在 CloudTrail 主控台中新增委派的系統管理員時，或使用 AWS CLI 或 CloudTrail API 時，會 CloudTrail 檢查組織的管理帳戶是否具有服務連結角色。如果管理帳戶沒有服務連結角色，請為管理帳戶 CloudTrail 建立服務連結角色。如需服務連結角色的詳細資訊，請參閱使用服務連結角色 AWS CloudTrail。

> **Note**
>
> 當您使用 AWS Organizations CLI 或 API 作業新增委派的系統管理員時，如果服務連結角色不存在，則不會建立該角色。只有當您從管理帳戶直接呼叫服務時，才會建立 CloudTrail 服務連結角色，例如當您新增委派的系統管理員，或使用 CloudTrail 主控台或 CloudTrail API 建立組織追蹤或事件資料存放區時。 AWS CLI

請注意下列定義委派管理員在中操作方式的因素 CloudTrail。

管理帳戶仍然是委派管理員建立之任何 CloudTrail 組織資源的擁有者。

組織的管理帳戶仍然是委派管理員建立之任何 CloudTrail 組織資源的擁有者，例如追蹤和事件資料存放區。如果委派的管理員變更，這可為組織提供連續性。

移除委派的管理員帳戶並不會刪除他們建立的任何 CloudTrail 組織資源。

當您移除委派的管理員時，不會刪除委派管理員所建立的組織追蹤記錄和事件資料存放區，因為管理帳戶一律會擔任 CloudTrail 組織資源的擁有者，無論這些資源是由委派的管理員還是管理帳戶所建立。

一個組織最多可以有三個 CloudTrail 委派管理員。

每個組織最多可有三個 CloudTrail 委派管理員。如需委派的管理員的詳細資訊，請參閱 移除 CloudTrail 委派管理員。

下表顯示管理帳戶、委派管理員帳戶以及 AWS Organizations 組織內成員帳戶的權能。

功能	管理帳戶	委派管理員帳戶	成員帳戶
新增或移除委派的管理員帳戶	是	否	否
建立組織追蹤。	是	是 [1]	否
檢視組織追蹤清單。	是	是	是
更新組織追蹤。	是	是[1、2]	否
刪除組織追蹤。	是	是	否

功能	管理帳戶	委派管理員帳戶	成員帳戶
為 CloudTrail 事件或組 AWS Config 態項目建立組織事件資料存放區。	是	是	否
啟用組織事件資料存放區上的 Insights。	是	否	否
更新組織事件資料存放區。	是	是[2]	否
啟用組織事件資料存放區上的 Lake 查詢聯合[3]。	是	是	否
停用組織事件資料存放區上的 Lake 查詢聯合。	是	是	否
刪除組織事件資料存放區。	是	是	否
將追蹤事件複製到組織事件資料存放區。	是	否	否
對組織事件資料存放區執行查詢。	是	是	否
檢視組織事件資料存放區的 Lake 儀表板。	是	是	否

[1] 委派的系統管理員只能使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 作業來設定 CloudWatch 記錄檔群組。 CloudWatch 記錄檔記錄群組和記錄角色都必須存在於呼叫帳戶中。

[2] 只有管理帳戶可以將組織追蹤或事件資料存放區轉換為帳戶層級追蹤或事件資料存放區，或將帳戶層級追蹤或事件資料存放區轉換為組織追蹤或事件資料存放區。委派的管理員不允許執行這些動作，因為組織追蹤和事件資料存放區僅存在於管理帳戶中。將組織追蹤或事件資料存放區轉換為帳戶層級追蹤或事件資料存放區時，只有管理帳戶可以存取追蹤或事件資料存放區。

[3]只有一個委派管理員帳戶或管理帳戶可以在組織事件資料存放區上啟用聯合。其他委派管理員帳戶可以使用 Lake Formation 資料共用功能查詢和共享資訊。任何委派管理員帳戶和組織的管理帳戶都能停用聯合。

主題

指派委派管理員所需的許可

指 CloudTrail 派委派管理員時，您必須擁有在中新增和移除委派管理員的權限 CloudTrail，以及下列政策聲明中列出的特定 AWS Organizations API 動作和 IAM 許可。

您可以將下列陳述式新增至現有 IAM 政策的結尾，以授與這些許可：

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
    "Resource": "*"
}
```

新增 CloudTrail 委派管理員

您可以新增委派管理員來管理組織的 CloudTrail 資源，例如追蹤和事件資料存放區。

您可以使用 CloudTrail 主控台或新增 AWS 組織的 CloudTrail 委派管理員 AWS CLI。

在您新增委派的系統管理員之前，請確定他們在您的組織中擁有帳戶，而且您使用組織的管理帳戶登入。如需如何為組織建立新 AWS 帳戶的相關資訊，請參閱在組織中建立 AWS 帳戶。如需如何邀請現有 AWS 帳戶加入組織的詳細資訊，請參閱邀請 AWS 帳戶加入組織。

CloudTrail console

下列程序說明如何使用 CloudTrail 主控台新增 CloudTrail 委派管理員。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 主控台左側導覽窗格中選擇 [設定]。
3. 在 Organization delegated administrators (組織委派的管理員) 區段，選擇 Register administrator (註冊管理員)。
4. 輸入您要指派為組織追蹤記錄和事件資料存放區 CloudTrail 委派管理員之帳戶的十二 AWS 位數帳戶 ID。
5. 選擇 Register administrator (註冊管理員)。

AWS CLI

下列範例會新增 CloudTrail 委派的管理員。

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

此命令如果成功就不會產生輸出。

移除 CloudTrail 委派管理員

您可以使用 CloudTrail 主控台或移除 CloudTrail 委派的管理員 AWS CLI。

CloudTrail console

下列程序說明如何使用 CloudTrail 主控台移除 CloudTrail 委派管理員。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在 CloudTrail 主控台左側導覽窗格中選擇 [設定]。
3. 在 Organization delegated administrators (組織委派的管理員) 區段，選擇您要移除的委派管理員。
4. 選擇 Remove administrator (移除管理員)。
5. 確認您要移除委派的管理員，然後選擇 Remove administrator (移除管理員)。

AWS CLI

下列命令會移除 CloudTrail 委派的管理員。

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

此命令如果成功就不會產生輸出。

服務連結通道

AWS 服務可以建立與服務連結的頻道，以代表您接收 CloudTrail 事件。建立 AWS 服務連結通道的服務會為通道設定進階事件選取器，並指定通道是套用至所有通道 AWS 區域，還是單一通道。 AWS 區域

主題

使用主控台檢視服務連結通道

您可以使用 CloudTrail 主控台檢視服務建立的任何 AWS 服 CloudTrail 務連結通道的相關資訊。如果您的帳戶沒有任何服務連結通道，則表格為空白。

使用以下程序來檢視服務連結通道的相關資訊。

1. 在 CloudTrail 主控台左側導覽窗格中選擇 [設定]。
2. 對於服務連結通道，選擇要檢視其詳細資訊的服務連結通道。
3. 在詳細資訊頁面上，檢閱服務連結通道的設定。

   您可以在詳細資訊頁面上檢視下列資訊。

   - 通道名稱 - 通道的完整名稱。通道名稱格式`aws-service-channel/`*`AWS_service_name`*`/slc`是*`AWS_service_name`*代表管理頻道之 AWS 服務的名稱。
   - 通道 ARN - 通道的 ARN，您可以在 API 請求中用它來取得該通道的相關詳細資訊。
   - 所有區域 - 若通道被設定針對所有 AWS 區域，這個值為 `Yes`。
   - AWS 服務-管理頻道的 AWS 服務名稱。
   - 管理事件 - 顯示為通道設定的任何管理事件。
   - 資料事件 - 顯示為通道設定的任何資料事件。

使用檢視服務連結的通道 AWS CLI

使用 AWS CLI，您可以檢視 AWS 服務所建立之任何服 CloudTrail 務連結通道的相關資訊。

主題

取得 CloudTrail 服務連結通道

下列範例 AWS CLI 命令會傳回特定 CloudTrail 服務連結通道的相關資訊，包括目的地 AWS 服務名稱、為該頻道設定的任何進階選取器，以及該通道是否適用於所有區域或單一區域。

您必須對於 `--channel` 指定 ARN 或 ARN 的 ID 尾碼。

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

以下是回應範例。在此範例中，`AWS_service_name`代表建立通道之 AWS 服務的名稱。

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
                        ]
                    }
                ]
            }
        ]
```

```
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
    ]
}
```

列出所有 CloudTrail 服務連結通道

下列範例 AWS CLI 命令會傳回代表您建立的所有 CloudTrail 服務連結通道的相關資訊。選用參數包括`--max-results`，藉以指定想要命令在單一頁面上傳回的最大結果數。如果結果多於您指定的 `--max-results` 值，請再次執行命令，新增傳回的 `NextToken` 值以取得下一頁的結果。

```
aws cloudtrail list-channels
```

以下是回應範例。在此範例中，`AWS_service_name`代表建立通道之 AWS 服務的名稱。

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS 服務連結通道上的服務事件

管理 AWS 服務連結通道的服務可以在服務連結通道上啟動動作 (例如，建立或更新服務連結通道)。CloudTrail 將這些動作記錄為AWS 服務事件，並將這些事件傳遞至事件歷史記錄，以及為管理事件設定的任何使用中追蹤和事件資料存放區。對於這些事件，`eventType` 欄位是 `AwsServiceEvent`。

以下是用來建立服務連結通道之 AWS 服務事件的記錄檔項目範例。

```
{
```

```
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
   "eventSource":"cloudtrail.amazonaws.com",
   "eventName":"CreateServiceLinkedChannel",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"AWS Internal",
   "requestParameters":null,
   "responseElements":null,
   "requestID":"564f004c-EXAMPLE",
   "eventID":"234f004b-EXAMPLE",
   "readOnly":false,
   "resources":[
      {
         "accountId":"184434908391",
         "type":"AWS::CloudTrail::Channel",
         "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
      }
   ],
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "recipientAccountId":"111122223333",
   "eventCategory":"Management"
}
```

了解 CloudTrail 事件

中的事件 CloudTrail 是 AWS 帳戶中活動的記錄。此活動可以是 IAM 身分或可監控的服務所 CloudTrail採取的動作。 CloudTrail 事件提供透過 AWS Management Console、 AWS SDK、命令列工具及其他進行的 API 和非 API 帳戶活動的歷史記錄。 AWS 服務

CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此事件不會以任何特定順序顯示。

有三種類型的 CloudTrail 事件：

- 管理事件
- 資料事件
- 洞察活動

依預設，追蹤和事件資料存放區會記錄管理事件，但不會記錄資料或 Insights 事件。

所有事件類型都使用 CloudTrail JSON 記錄格式。日誌會包含您帳戶中的資源請求資訊，例如請求的提出者、使用過的服務、執行過的動作，以及動作的參數。事件資料都包含在 `Records` 陣列中。

如需 CloudTrail 事件記錄欄位的資訊，請參閱CloudTrail 記錄內容。

管理事件

管理事件提供有關對您 AWS 帳戶中資源執行之管理作業的相關資訊。這些也稱為控制平面操作。範例管理事件包含：

- 設定安全性 (例如 AWS Identity and Access Management `AttachRolePolicy` API 作業)。
- 註冊裝置 (例如，Amazon EC2 `CreateDefaultVpc` API 操作)。
- 設定規則以路由資料 (例如，Amazon EC2 `CreateSubnet` API 操作)。
- 設定記錄 (例如 AWS CloudTrail `CreateTrail` API 作業)。

管理事件也可以包含您帳戶中發生的非 API 事件。例如，當使用者登入您的帳戶時，會 CloudTrail 記錄`ConsoleLogin`事件。如需詳細資訊，請參閱 擷取的非 API 事件 CloudTrail。如需記 CloudTrail 錄 AWS 服務的管理事件清單，請參閱CloudTrail 支援的服務與整合。

下列範例顯示管理事件的單一記錄檔記錄。在此情況下，名為的 IAM 使用者會Mary_Major執行aws cloudtrail start-logging命令來呼叫 CloudTrail StartLogging動作，以便在名為的追蹤上啟動記錄程序myTrail。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
```

```
    "sessionCredentialFromConsole": "true"
}
```

在這個後續範例中，名為 Paulo_Santos 的 IAM 使用者執行 aws cloudtrail start-event-data-store-ingestion 命令呼叫 StartEventDataStoreIngestion 動作，以便在事件資料存放區上開始擷取。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
```

```
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

資料事件

資料事件提供在資源上執行或於資源中執行之資源操作的相關資訊。這些也稱為資料平面操作。資料事件通常是大量資料的活動。

範例資料事件包含：

- S3 儲存貯體中物件上的 Amazon S3 物件層級 PutObject API 活動 (例如DeleteObject，和 API 操作)。GetObject
- AWS Lambda 函數執行活動 (InvokeAPI)。
- CloudTrail PutAuditEventsCloudTrail Lake 頻道上的活動，用於從外部記錄事件 AWS。
- 主題上的 Amazon SNS Publish 和 PublishBatch API 操作。

下表顯示可用於追蹤和事件資料存放區的資料事件類型。資料事件類型 (主控台) 欄顯示主控台中的適當選取項目。resource .type 值欄會顯示您要指定以使用或 API 將該類型的資料事件納入追蹤或事件資料存放區中的resources.type AWS CLI 值。 CloudTrail

對於追蹤，您可以使用基本或進階事件選取器來記錄 Amazon S3 物件、Lambda 函數和 DynamoDB 表格的資料事件 (顯示在表格的前三列中)。您只能使用進階事件選取器來記錄剩餘列中顯示的資料事件類型。

對於事件資料存放區，您只能使用進階事件選取器來包含資料事件。

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon DynamoDB	資料表上的 Amazon DynamoDB 項目層級 API 活動 (例如PutItemDeleteIte	DynamoDB	AWS::DynamoDB::Table

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	m 、和 UpdateItem API 操作)。 **Note** 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table 。如果您指定 AWS::DynamoDB::Table 作為 resources.type ，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在eventName		

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	欄位上新增篩選器。		
AWS Lambda	AWS Lambda 函數執行活動 (InvokeAPI)。	Lambda	AWS::Lambda::Function
Amazon S3	S3 儲存貯體中物件上的 Amazon S3 物件層級 PutObject API 活動 (例如DeleteObject ，和 API 操作)。GetObject	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 設定作業的 API 活動，例如呼叫StartConfiguration Session 和GetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration
AWS 數據交換	用於轉換器作業的 B2B 資料交換 API 活動，例如呼叫 GetTransformerJob 和 StartTransformerJob 。	B2B 資料交換	AWS::B2BI::Transformer
Amazon Bedrock	代理程式別名上的 Amazon Bedrock API 活動。	Bedrock 代理程式別名	AWS::Bedrock::AgentAlias

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	知識庫中的 Amazon Bedrock API 活動。	Bedrock 知識庫	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront 上的 API 活動 KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map 命名空間上的 API 活動。	AWS Cloud Map 命名空間	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map 服務上的 API 活動。	AWS Cloud Map 服務	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` CloudTrail Lake 頻道上的活動，用於從外部記錄事件 AWS。	CloudTrail 渠道	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	在自定義 Amazon CodeWhisperer API 活動。	CodeWhisperer 定制	`AWS::CodeWhisperer::Customization`
	設定檔上的 Amazon CodeWhisperer API 活動。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito 身分集區上的 Amazon Cognito API 活動。	Cognito 身分池	`AWS::Cognito::IdentityPool`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon DynamoDB	串流上的 Amazon DynamoDB API 活動。	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) direct API，例如 Amazon EBS 快照上的 `PutSnapshotBlock` 、`GetSnapshotBlock` ，以及 `ListChangedBlocks` 。	Amazon EBS direct API	`AWS::EC2::Snapshot`
Amazon EMR	預寫日誌工作區上的 Amazon EMR API 活動。	EMR 預寫日誌工作區	`AWS::EMRWAL::Workspace`
Amazon FinSpace	環境上的 Amazon FinSpace API 活動。	FinSpace	`AWS::FinSpace::Environment`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
AWS Glue	AWS Glue 由 Lake Formation 創建的表上的 API 活動。 **Note** AWS Glue 目前僅在下列區域支援資料表的資料事件： • 美國東部 (維吉尼亞北部) • 美國東部 (俄亥俄) • 美國西部 (奧勒岡) • 歐洲 (愛爾蘭) • 亞太 (東京) 區域	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	檢測器的 Amazon GuardDuty API 活動。	GuardDuty 探測器	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging 資料存放區上的 API 活動。	醫學影像資料存放區	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT 憑證上的 API 活動。	IoT 證書	`AWS::IoT::Certificate`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	AWS IoT 事物上的 API 活動。	IoT 的事	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	來自組件版本的 Greengrass 核心設備的 API 活動。 **Note** Greengrass 不會記錄訪問被拒絕的事件。	IoT Greengrass 件版本	`AWS::GreengrassV2::ComponentVersion`
	部署上來自 Greengrass 核心裝置的 API 活動。 **Note** Greengrass 不會記錄訪問被拒絕的事件。	IoT 環境部署	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	資產上的 IoT SiteWise API 活動。	IoT SiteWise 資產	`AWS::IoTSiteWise::Asset`
	時間序列上的 IoT SiteWise API 活動。	IoT SiteWise 時間序列	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	實體上的 IoT TwinMaker API 活動。	IoT TwinMaker 實體	`AWS::IoTTwinMaker::Entity`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	工作區上的 IoT TwinMaker API 活動。	IoT TwinMaker 工作區	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	重新評分執行計畫上的 Amazon Kendra Intelligent Ranking API 活動。	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (適用於 Apache Cassandra)	表上的 Amazon Keyspaces API 活動。	卡桑德拉表	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	串流上的 Kinesis Data Streams 流 API 活動。	Kinesis 流	`AWS::Kinesis::Stream`
	串流取用者的室運動資料串流 API 活動。	Kinesis 流消費者	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	Kinesis Video Streams 片串流上的 API 活動，例如呼叫`GetMedia`和`PutMedi`	Kinesis 視訊串流	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	網路上的 Amazon Managed Blockchain API 活動。	Managed Blockchain 網路	`AWS::ManagedBlockchain::Network`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Ethereum 節點上的 Amazon Managed Blockchain JSON-RPC 呼叫，例如 `eth_getBalance` 或 `eth_getBlockByNumber` 。	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Neptune 圖形	Neptune 圖形上的資料 API 活動，例如查詢、演算法或向量搜尋。	Neptune 圖形	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA 作用中目錄 API 活動的連接器。	AWS Private CA 作用中目錄的連接器	`AWS::PCAConnectorAD::Connector`
Amazon Q 應用	Amazon Q 應用程式上的資料 API 活動。	Amazon Q 應用	`AWS::QApps:QApp`
Amazon Q Business	應用程式上的 Amazon Q Business API 活動。	Amazon Q Business 應用程式	`AWS::QBusiness::Application`
	資料來源上的 Amazon Q Business API 活動。	Amazon Q Business 資料來源	`AWS::QBusiness::DataSource`
	索引上的 Amazon Q Business API 活動。	Amazon Q Business 索引	`AWS::QBusiness::Index`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Web 體驗上的 Amazon Q Business API 活動。	Amazon Q Business Web 體驗	`AWS::QBusiness::WebExperience`
Amazon RDS	資料庫叢集上的 Amazon RDS API 活動。	RDS 數據 API-數據庫集群	`AWS::RDS::DBCluster`
Amazon S3	存取點上的 Amazon S3 API 活動。	S3 存取點	`AWS::S3::AccessPoint`
	Amazon S3 物件 Lambda 存取點 API 活動，例如呼叫`CompleteMultipartUpload` 和`GetObject`。	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Outposts 上 Amazon S3 物件層級的 API 活動。	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	端點上的 Amazon SageMaker `InvokeEndpointWithResponseStream` 活動。	SageMaker 端點	`AWS::SageMaker::Endpoint`
	功能商店上的 Amazon SageMaker API 活動。	SageMaker feature store	`AWS::SageMaker::FeatureGroup`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	實驗試用元件上的 Amazon SageMaker API 活動。	SageMaker 度量實驗試驗元件	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	平台端點上的 Amazon SNS `Publish` API 操作。	SNS 平台端點	`AWS::SNS::PlatformEndpoint`
	主題上的 Amazon SNS `Publish` 和 `PublishBatch` API 操作。	SNS 主題	`AWS::SNS::Topic`
Amazon SQS	訊息上的 Amazon SQS API 活動。	SQS	`AWS::SQS::Queue`
AWS Step Functions	Step Functions 狀態機上的 API 活動。	Step Functions 狀態機器	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain 執行個體上的 API 活動。	供應鏈	`AWS::SCN::Instance`
Amazon SWF	網域上的 Amazon SWF API 活動。	SWF 網域名稱	`AWS::SWF::Domain`
AWS Systems Manager	控制通道上的 Systems Manager API 活動。	Systems Manager	`AWS::SSMMessages::ControlChannel`
	受管節點上的系統管理員 API 活動。	系統管理員管理節點	`AWS::SSM::ManagedNode`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon Timestream	資料庫上的 Amazon Timestream Query API 活動。	Timestream 資料庫	AWS::Timestream::Database
	資料庫上的 Amazon Timestream Query API 活動。	Timestream 資料表	AWS::Timestream::Table
Amazon Verified Permissions	政策存放區上的 Amazon Verified Permissions API 活動。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces 瘦客戶端	WorkSpaces 裝置上的精簡型用戶端 API 活動。	精簡型客戶端裝置	AWS::ThinClient::Device
	WorkSpaces 環境上的精簡型用戶端 API 活動。	精簡型客戶端環境	AWS::ThinClient::Environment
AWS X-Ray	軌跡上的 X-Ray API 活動。	X-Ray 軌跡	AWS::XRay::Trace

依預設，在您建立追蹤或事件資料存放區時，不會記錄資料事件。若要記錄資 CloudTrail 料事件，您必須明確新增要收集活動的支援資源或資源類型。如需詳細資訊，請參閱 建立追蹤 及 使用主控台為CloudTrail事件建立事件資料存放區。

記錄資料事件需支付額外的費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

下列範例顯示 Amazon SNS Publish 動作之資料事件的單一日誌記錄。

```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
```

```
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
```

```
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}
```

下一個範例顯示 Amazon Cognito GetCredentialsForIdentity 動作之資料事件的單一日誌記錄。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
```

```
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```

洞察活動

CloudTrail 洞察事件會透過分析 CloudTrail 管理活動，擷取您 AWS 帳戶中異常的 API 呼叫率或錯誤率活動。Insights 事件會提供相關資訊，例如關聯的 API、錯誤代碼、事件時間及統計資料，以協助您了解並針對異常活動採取行動。與 CloudTrail 追蹤或事件資料存放區中擷取的其他類型事件不同，Insights 事件只有在 CloudTrail 偵測到帳戶 API 使用情況或錯誤率記錄的變更時，才會記錄與帳戶的一般使用模式明顯不同。

可能產生 Insights 事件的活動範例包括：

- 您的帳戶通常每分鐘記錄不超過 20 個 Amazon S3 `deleteBucket` API 呼叫，但是您的帳戶開始記錄到每分鐘平均 100 個 `deleteBucket` API 呼叫。異常活動開始時會記錄 Insights 事件，並記錄另一個 Insights 事件以標示異常的活動結束。
- 您的帳戶通常每分鐘記錄 20 個 Amazon EC2 `AuthorizeSecurityGroupIngress` API 呼叫，但您的帳戶開始記錄到零個 `AuthorizeSecurityGroupIngress` 呼叫。異常活動開始時會記錄 Insights 事件，並在十分鐘後，當異常活動結束時，記錄另一個 Insights 事件以標示異常的活動結束。
- 您的帳戶於 7 天內在 AWS Identity and Access Management API 上記錄通常少於一個的 `AccessDeniedException` 錯誤，`DeleteInstanceProfile`。您的帳戶開始在 `DeleteInstanceProfile` API 呼叫中記錄每分鐘 12 個 `AccessDeniedException` 錯誤的平均值。異常錯誤率活動開始時會記錄 Insights 事件，並記錄另一個 Insights 事件以標示異常活動的結束。

這些範例僅供說明之用。您的結果可能會根據您的使用案例而有所不同。

若要記錄 CloudTrail Insights 事件，您必須在新的或現有的追蹤或事件資料存放區上明確啟用 Insights 事件。如需建立線索的詳細資訊，請參閱 建立追蹤。如需有關建立事件資料存放區的詳細資訊，請參閱 使用主控台為 CloudTrail Insights 事件建立事件資料存放區。

Insights 事件會產生額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

在 CloudTrail Insights 中記錄了兩個事件，以顯示異常活動：開始事件和結束事件。下列範例顯示 Application Auto Scaling API `CompleteLifecycleAction` 被呼叫異常次數時發生的開始 Insights 事件的單一日誌記錄。對於 Insights 事件，`eventCategory` 的值為 `Insight`。`insightDetails` 區塊會識別事件狀態、來源、名稱、Insights 類型和內容，包括統計資料和歸因。如需 `insightDetails` 區塊的詳細資訊，請參閱 CloudTrail 見解`insightDetails`元素。


```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
```

```
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
                    }]
                }]
            }
        },
        "eventCategory": "Insight"
    }
```

記錄管理事件

依預設，追蹤和事件資料存放區會記錄管理事件，但不會包含資料或 Insights 事件。

資料或 Insights 事件需支付額外費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

內容

管理事件

管理事件可讓您查看對 AWS 帳戶中資源執行的管理作業。這些也稱為控制平面操作。範例管理事件包含：

- 設定安全性 (例如，IAM `AttachRolePolicy` API 操作)
- 註冊裝置 (例如，Amazon EC2 `CreateDefaultVpc` API 操作)
- 設定規則以路由資料 (例如，Amazon EC2 `CreateSubnet` API 操作)
- 設定記錄 (例如 AWS CloudTrail `CreateTrail` API 作業)

管理事件也可以包含您帳戶中發生的非 API 事件。例如，當使用者登入您的帳戶時，會 CloudTrail 記錄`ConsoleLogin`事件。如需詳細資訊，請參閱 擷取的非 API 事件 CloudTrail。

依預設，追蹤和事件資料存放區被設定用來記錄管理事件。

> **Note**
>
> CloudTrail 事件歷史記錄功能僅支援管理事件。您無法從事件歷史記錄中排除 AWS KMS 或從事件歷史記錄中排除 Amazon RDS Data API 事件；套用至追蹤或事件資料存放區的設定不適用於事件歷史記錄。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。

記錄管理事件 AWS Management Console

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 若要更新追蹤，請開啟 CloudTrail 主控台的「追蹤」頁面，然後選擇追蹤名稱。

   若要更新事件資料存放區，請開啟 CloudTrail 主控台的「事件資料存放區」頁面，然後選擇事件資料存放區名稱。
3. 針對管理活動，選擇 Edit (編輯)。

   - 選擇您是否希望追蹤或事件資料存放區記錄讀取事件、寫入事件，或兩者。
   - 選擇 [排除 AWS KMS 事件] 以將 AWS Key Management Service (AWS KMS) 追蹤或事件資料存放區中的事件篩選出來。預設設定是包含所有 AWS KMS 事件。

     只有在追蹤或 AWS KMS 事件資料存放區中記錄管理事件時，才能使用記錄或排除事件的選項。如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

     AWS KMS 動作，例如`Encrypt`、`Decrypt`，`GenerateDataKey`通常會產生大量 (超過 99%) 的事件。這些動作現在會記錄為 Read (讀取) 事件。低容量的相關 AWS KMS 動作，例如`DisableDelete`、和 `ScheduleKey` (通常佔 AWS KMS 事件磁碟區的 0.5% 以下) 會記錄為「寫入」事件。

     若要排除、和等大量事件 `Encrypt` `Decrypt`，`GenerateDataKey`但仍記錄相關事件 (例如`Disable`、`Delete`和`ScheduleKey`)，請選擇記錄 Write 管理事件，然後清除 [排除 AWS KMS 事件] 的核取方塊。
   - 選擇排除 Amazon RDS Data API 事件，從追蹤或事件資料存放區中篩選出 Amazon Relational Database Service Data API 事件。預設設定是包含所有 Amazon RDS Data API 事件。如需 Amazon RDS Data API 事件的詳細資訊，請參閱《Amazon RDS 使用者指南 (Aurora)》中的使用 AWS CloudTrail記錄資料 API 呼叫。

4. 完成時，請選擇儲存變更。

讀取和寫入事件

當您設定您的追蹤或事件資料存放區以記錄管理事件時，您可以指定要記錄唯讀事件、唯寫事件，還是都記錄。

- 讀取

  唯讀事件包含讀取您的資源，但不予變更的 API 操作。例如，唯讀事件包含 Amazon EC2 `DescribeSecurityGroups` 和 `DescribeSubnets` API 操作。這些操作僅傳回 Amazon EC2 資源的相關資訊，但不變更您的組態。
- 寫入

  Write-only (唯寫) 事件只包含會修改 (或可能修改) 您資源的 API 操作。例如，Amazon EC2 `RunInstances` 和 `TerminateInstances` API 操作會修改您的執行個體。

範例：記錄不同追蹤的讀和寫事件

以下範例說明如何設定追蹤，將帳戶的日誌活動分割成不同的 S3 儲存貯體：一個儲存貯體接收唯讀事件，第二個儲存貯體收到唯寫事件。

1. 您要建立一個線索，然後選擇名為 `read-only-bucket` 的 S3 儲存貯體接收日誌檔案。接著，您要更新線索，指定您要讀管理事件。
2. 您要建立第二個線索，然後選擇名為 `write-only-bucket` 的 S3 儲存貯體接收日誌檔案。接著，您要更新線索，指定您要寫管理事件。
3. Amazon EC2 `DescribeInstances` 和 `TerminateInstances` API 操作發生在您的帳戶中。
4. `DescribeInstances` API 操作是唯讀事件，且符合第一個追蹤的設定。追蹤會記錄事件並將它交付到 `read-only-bucket`。
5. `TerminateInstances` API 操作是唯寫事件，且符合第二個追蹤的設定。追蹤會記錄事件並將它交付到 `write-only-bucket`。

使用 AWS Command Line Interface記錄事件

您可以使用 AWS CLI設定您的追蹤或事件資料存放區，以記錄管理事件。

主題

- 範例：記錄追蹤的管理事件
- 範例：記錄事件資料存放區的管理事件

範例：記錄追蹤的管理事件

若要檢視您的線索是否記錄管理事件，請執行 get-event-selectors 命令。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

以下範例會傳回預設的線索設定。根據預設，線索會記錄所有管理事件、記錄來自所有事件來源的事件，但不記錄資料事件。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

您可以使用基本或進階事件選取器來記錄管理事件。您不能同時將事件選取器和進階事件選取器套用於追蹤。如果您將進階事件選取器套用至追蹤，則會覆寫任何現有的基本事件選取器。下列各節提供如何使用進階事件選取器和基本事件選取器來記錄管理事件的範例。

主題

- 範例：使用進階事件選取器記錄追蹤的管理事件
- 範例：使用基本事件選取器記錄追蹤的管理事件

範例：使用進階事件選取器記錄追蹤的管理事件

下列範例會針對名*TrailName*為包含唯讀和唯寫管理事件的追蹤建立進階事件選取器 (藉由省略`readOnly`選取器)，但要排除 AWS Key Management Service (AWS KMS) 事件。由於 AWS KMS 事件會被視為管理事件，而且可能會有大量事件，因此如果您有多個追蹤可擷取管理事件的追蹤，這些事件可能會對 CloudTrail 帳單產生重大影響。

如果您選擇不記錄管理事件，則不會記錄 AWS KMS 事件，而且您無法變更 AWS KMS 事件記錄設定。

若要再次開始將 AWS KMS 事件記錄到追蹤，請移除`eventSource`選取器，然後再次執行命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

範例傳回針對追蹤設定的進階事件選取器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
```

```
}
```

若要再次開始記錄排除的事件至追蹤，請從移除 eventSource 選取器，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

下一個範例會為名*TrailName*為包含唯讀和唯寫管理事件的追蹤建立進階事件選取器 (透過省略readOnly選取器)，但排除 Amazon RDS Data API 管理事件。若要排除 Amazon RDS 資料 API 管理事件，請在以下eventSource欄位的字串值中指定 Amazon RDS 資料 API 事件來源：rdsdata.amazonaws.com。

如果您選擇不記錄管理事件，則不會記錄 Amazon RDS 資料 API 管理事件，而且您無法變更 Amazon RDS 資料 API 事件記錄設定。

若要重新開始將 Amazon RDS 資料 API 管理事件記錄到追蹤，請移除eventSource選取器，然後再次執行命令。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

範例傳回針對追蹤設定的進階事件選取器。

```
{
```

```
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

若要再次開始記錄排除的事件至追蹤，請從移除 eventSource 選取器，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

範例：使用基本事件選取器記錄追蹤的管理事件

若要設定您的線索記錄管理事件，請執行 put-event-selectors 命令。以下範例說明如何設定您的線索以包含兩個 S3 物件的所有管理事件。您可以為追蹤指定 1 到 5 個事件選取器。您可以為追蹤指定 1 到 250 項資料資源。

> **Note**
>
> 無論事件選取器有多少個，S3 資料資源的上限數為 250。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

以下範例會傳回為線索設定的事件選取器。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

若要從追蹤記錄中排除 AWS Key Management Service (AWS KMS) 事件，請執行`put-event-selectors`命令並新增值為`ExcludeManagementEventSources`的屬性`kms.amazonaws.com`。下列範例會針對名*TrailName*為包含唯讀和唯寫管理事件但排除 AWS KMS 事件的追蹤建立事件選取器。由於 AWS KMS 可以產生大量的事件，因此此範例中的使用者可能想要限制事件以管理追蹤的成本。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

此範例會傳回為追蹤設定的事件選取器。

```
{
```

```
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

若要從追蹤的日誌中排除 Amazon RDS 資料 API 管理事件，請執行`put-event-selectors`命令並新增值為`ExcludeManagementEventSources`的屬性`rdsdata.amazonaws.com`。下列範例會為名為的追蹤建立事件選取器，*TrailName*以包含唯讀和唯寫管理事件，但排除 Amazon RDS Data API 管理事件。由於 Amazon RDS Data API 可以產生大量的管理事件，因此此範例中的使用者可能想要限制事件以管理追蹤的成本。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
}
```

若要重新開始記錄日誌記錄 AWS KMS 或 Amazon RDS Data API 管理事件至追蹤，請傳遞一個空字串作為的值`ExcludeManagementEventSources`，如下列命令所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

若要將相關 AWS KMS 事件記錄到追蹤 (例如DisableScheduleKey、Delete和)，但排除大量 AWS KMS 事件 (例如EncryptDecrypt、GenerateDataKey、和) 記錄唯寫管理事件，並保留記錄 AWS KMS 事件的預設設定，如下列範例所示。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

範例：記錄事件資料存放區的管理事件

若要檢視您的事件資料存放區是否包括管理事件，請執行 get-event-data-store 命令。

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下是回應範例。建立時間和上次更新時間的格式為 timestamp。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
```

```
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

若要建立包括全部管理事件的事件資料存放區，您可以執行 create-event-data-store 命令。您不需要指定任何進階事件選取器以包括全部管理事件。

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

若要建立排除 AWS Key Management Service (AWS KMS) 事件的事件資料倉庫，請執行指`create-event-data-store`令並指定`eventSource`不相等的命令`kms.amazonaws.com`。下列範例會建立事件資料存放區，其中包含唯讀和唯寫管理事件，但排除 AWS KMS 事件。

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
```

```
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

若要建立排除 Amazon RDS 資料 API 管理事件的事件資料存放區，請執行`create-event-data-store`命令並指定`eventSource`不相等的命令`rdsdata.amazonaws.com`。下列範例會建立包含唯讀和唯寫管理事件的事件資料存放區，但排除 Amazon RDS Data API 事件。

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
```

```
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

使用 AWS 開發套件記錄事件

使用此GetEventSelectors作業來查看追蹤是否記錄追蹤的管理事件。您可以設定追蹤，以便透過PutEventSelectors作業記錄管理事件。如需詳細資訊，請參閱 AWS CloudTrail API 參考。

執行GetEventDataStore作業以查看您的事件資料存放區是否包含管理事件。您可以透過執行CreateEventDataStore或UpdateEventDataStore作業，將事件資料存放區設定為包含管理事件。如需詳細資訊，請參閱建立、更新和管理事件資料存放區 AWS CLI和 AWS CloudTrail API 參考。

將事件傳送到 Amazon CloudWatch 日誌

對於追蹤， CloudTrail 支援將資料和管理事件傳送至 CloudWatch 記錄檔。當您將追蹤設定為將事件傳送至 CloudWatch 記錄檔記錄群組時，只 CloudTrail 會傳送您在追蹤中指定的事件。例如，如果您將追蹤設定為僅記錄管理事件，則追蹤只會將管理事件傳送至您的 CloudWatch 記錄檔記錄群組。如需更多詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。

記錄資料事件

本節說明如何使用CloudTrail 主控台和記錄資料事件AWS CLI。

依預設，追蹤和事件資料存放區不會記錄資料事件。資料事件需支付額外的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

資料事件可讓您深入了解對資源執行或在資源中執行的資源操作。這些也稱為資料平面操作。資料事件通常是大量資料的活動。

範例資料事件包含：

- S3 儲存貯體中物件上的 Amazon S3 物件層級 PutObject API 活動 (例如DeleteObject，和 API 操作)。GetObject

- AWS Lambda 函數執行活動 (InvokeAPI)。
- CloudTrail PutAuditEventsCloudTrail Lake 頻道上用來記錄外部事件的活動 AWS。
- 主題上的 Amazon SNS Publish 和 PublishBatch API 操作。

您可以使用進階事件選取器來建立精細的選取器，只記錄使用案例感興趣的特定事件，藉此協助您控制成本。例如，您可以透過在eventName欄位上新增篩選器，使用進階事件選取器來記錄特定的 API 呼叫。如需詳細資訊，請參閱 使用進階事件選取器篩選資料事件。

> **Note**
>
> 您的跟踪記錄的事件可在 Amazon 中使用 EventBridge。例如，如果您選擇記錄 S3 物件的資料事件，但不記錄管理事件，則您的追蹤只會處理並記錄所指定之 S3 物件的資料事件。這些 S3 物件的資料事件可在 Amazon 中使用 EventBridge。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南中的來自 AWS 服務的事件。

內容

    - eventName使用篩選資料事件 AWS Management Console
    - eventName使用篩選資料事件 AWS CLI
  - 篩選資料事件的依據 resources.ARN
    - resources.ARN使用篩選資料事件 AWS Management Console
    - resources.ARN使用篩選資料事件 AWS CLI
  - 依readOnly值篩選資料事件
    - 使用readOnly值篩選資料事件 AWS Management Console
    - 使用readOnly值篩選資料事件 AWS CLI
- 記錄資料事件以確保 AWS Config 合規
- 使用 AWS SDK 記錄資料事件
- 將事件傳送到 Amazon CloudWatch 日誌

資料事件

下表顯示可用於追蹤和事件資料存放區的資料事件類型。資料事件類型 (主控台) 欄顯示主控台中的適當選取項目。resource .type 值欄會顯示您要指定的**`resources.type`**值，以便在使用或 API 的追蹤或事件資料存放區中包含該類型的資料事件。 AWS CLI CloudTrail

對於追蹤，您可以使用基本或進階事件選取器來記錄 Amazon S3 物件、Lambda 函數和 DynamoDB 表格的資料事件 (顯示在表格的前三列中)。您只能使用進階事件選取器來記錄剩餘列中顯示的資料事件類型。

對於事件資料存放區，您只能使用進階事件選取器來包含資料事件。

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon DynamoDB	資料表上的 Amazon DynamoDB 項目層級 API 活動 (例如`PutItem`、`DeleteItem` 、和 `UpdateItem` API 操作)。	DynamoDB	`AWS::DynamoDB::Table`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Note 對於已啟用串流的資料表，資料事件中的 `resources` 欄位會同時包含 `AWS::DynamoDB::Stream` 和 `AWS::DynamoDB::Table` 。如果您指定 `AWS::DynamoDB::Table` 作為 `resources.type` ，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在 `eventName` 欄位上新增篩選器。		

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
AWS Lambda	AWS Lambda 函數執行活動 (InvokeAPI)。	Lambda	AWS::Lambda::Function
Amazon S3	S3 儲存貯體中物件上的 Amazon S3 物件層級 PutObject API 活動 (例如DeleteObject ，和 API 操作)。GetObject	S3	AWS::S3::Object
AWS AppConfig	AWS AppConfig 設定作業的 API 活動，例如呼叫StartConfiguration Session 和GetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration
AWS 數據交換	用於轉換器作業的 B2B 資料交換 API 活動，例如呼叫 GetTransformerJob 和 StartTransformerJob 。	B2B 資料交換	AWS::B2BI::Transformer
Amazon Bedrock	代理程式別名上的 Amazon Bedrock API 活動。	Bedrock 代理程式別名	AWS::Bedrock::AgentAlias
	知識庫中的 Amazon Bedrock API 活動。	Bedrock 知識庫	AWS::Bedrock::KnowledgeBase

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon CloudFront	CloudFront 上的 API 活動 KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map 命名空間上的 API 活動。	AWS Cloud Map 命名空間	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map 服務上的 API 活動。	AWS Cloud Map 服務	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` CloudTrail Lake 頻道上用來記錄外部事件的活動 AWS。	CloudTrail 渠道	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	在自定義 Amazon CodeWhisperer API 活動。	CodeWhisperer 定制	`AWS::CodeWhisperer::Customization`
	設定檔上的 Amazon CodeWhisperer API 活動。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito 身分集區上的 Amazon Cognito API 活動。	Cognito 身分池	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	串流上的 Amazon DynamoDB API 活動。	DynamoDB Streams	`AWS::DynamoDB::Stream`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon Elastic Block Store	Amazon Elastic Block Store (EBS) direct API，例如 Amazon EBS 快照上的 PutSnapshotBlock 、GetSnapshotBlock ，以及 ListChangedBlocks 。	Amazon EBS direct API	AWS::EC2::Snapshot
Amazon EMR	預寫日誌工作區上的 Amazon EMR API 活動。	EMR 預寫日誌工作區	AWS::EMRWAL::Workspace
Amazon FinSpace	環境上的 Amazon FinSpace API 活動。	FinSpace	AWS::FinSpace::Environment

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
AWS Glue	AWS Glue 由 Lake Formation 創建的表上的 API 活動。 **Note** AWS Glue 目前僅在下列區域支援資料表的資料事件： • 美國東部 (維吉尼亞北部) • 美國東部 (俄亥俄) • 美國西部 (奧勒岡) • 歐洲 (愛爾蘭) • 亞太 (東京) 區域	Lake Formation	`AWS::Glue::Table`
Amazon GuardDuty	檢測器的 Amazon GuardDuty API 活動。	GuardDuty 探測器	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging 資料存放區上的 API 活動。	醫學影像資料存放區	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT 憑證上的 API 活動。	IoT 證書	`AWS::IoT::Certificate`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	AWS IoT 事物上的 API 活動。	IoT 的事	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	來自組件版本的 Greengrass 核心設備的 API 活動。 Note Greengrass 不會記錄訪問被拒絕的事件。	IoT Greengrass 件版本	`AWS::GreengrassV2::ComponentVersion`
	部署上來自 Greengrass 核心裝置的 API 活動。 Note Greengrass 不會記錄訪問被拒絕的事件。	IoT 環境部署	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	資產上的 IoT SiteWise API 活動。	IoT SiteWise 資產	`AWS::IoTSiteWise::Asset`
	時間序列上的 IoT SiteWise API 活動。	IoT SiteWise 時間序列	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	實體上的 IoT TwinMaker API 活動。	IoT TwinMaker 實體	`AWS::IoTTwinMaker::Entity`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	工作區上的 IoT TwinMaker API 活動。	IoT TwinMaker 工作區	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra Intelligent Ranking	重新評分執行計畫上的 Amazon Kendra Intelligent Ranking API 活動。	Kendra Ranking	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (適用於 Apache Cassandra)	表上的 Amazon Keyspaces API 活動。	卡桑德拉表	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	串流上的 Kinesis Data Streams 流 API 活動。	Kinesis 流	`AWS::Kinesis::Stream`
	串流取用者的室運動資料串流 API 活動。	Kinesis 流消費者	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	Kinesis Video Streams 片串流上的 API 活動，例如呼叫GetMedia和PutMedi	Kinesis 視訊串流	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	網路上的 Amazon Managed Blockchain API 活動。	Managed Blockchain 網路	`AWS::ManagedBlockchain::Network`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Ethereum 節點上的 Amazon Managed Blockchain JSON-RPC 呼叫，例如 `eth_getBalance` 或 `eth_getBlockByNumber` 。	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Neptune 圖形	Neptune 圖形上的資料 API 活動，例如查詢、演算法或向量搜尋。	Neptune 圖形	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA 作用中目錄 API 活動的連接器。	AWS Private CA 作用中目錄的連接器	`AWS::PCAConnectorAD::Connector`
Amazon Q 應用	Amazon Q 應用程式上的資料 API 活動。	Amazon Q 應用	`AWS::QApps:QApp`
Amazon Q Business	應用程式上的 Amazon Q Business API 活動。	Amazon Q Business 應用程式	`AWS::QBusiness::Application`
	資料來源上的 Amazon Q Business API 活動。	Amazon Q Business 資料來源	`AWS::QBusiness::DataSource`
	索引上的 Amazon Q Business API 活動。	Amazon Q Business 索引	`AWS::QBusiness::Index`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	Web 體驗上的 Amazon Q Business API 活動。	Amazon Q Business Web 體驗	AWS::QBusiness::WebExperience
Amazon RDS	資料庫叢集上的 Amazon RDS API 活動。	RDS 數據 API-數據庫集群	AWS::RDS::DBCluster
Amazon S3	存取點上的 Amazon S3 API 活動。	S3 存取點	AWS::S3::AccessPoint
	Amazon S3 物件 Lambda 存取點 API 活動，例如呼叫CompleteMultipartUpload 和GetObject 。	S3 Object Lambda	AWS::S3ObjectLambda::AccessPoint
Amazon S3 on Outposts	Outposts 上 Amazon S3 物件層級的 API 活動。	S3 Outposts	AWS::S3Outposts::Object
Amazon SageMaker	端點上的 Amazon SageMaker InvokeEndpointWithResponseStream 活動。	SageMaker 端點	AWS::SageMaker::Endpoint
	功能商店上的 Amazon SageMaker API 活動。	SageMaker feature store	AWS::SageMaker::FeatureGroup

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
	實驗試用元件上的 Amazon SageMaker API 活動。	SageMaker 度量實驗試驗元件	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	平台端點上的 Amazon SNS `Publish` API 操作。	SNS 平台端點	`AWS::SNS::PlatformEndpoint`
	主題上的 Amazon SNS `Publish` 和 `PublishBatch` API 操作。	SNS 主題	`AWS::SNS::Topic`
Amazon SQS	訊息上的 Amazon SQS API 活動。	SQS	`AWS::SQS::Queue`
AWS Step Functions	Step Functions 狀態機上的 API 活動。	Step Functions 狀態機器	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain 執行個體上的 API 活動。	供應鏈	`AWS::SCN::Instance`
Amazon SWF	網域上的 Amazon SWF API 活動。	SWF 網域名稱	`AWS::SWF::Domain`
AWS Systems Manager	控制通道上的 Systems Manager API 活動。	Systems Manager	`AWS::SSMMessages::ControlChannel`
	受管節點上的系統管理員 API 活動。	系統管理員管理節點	`AWS::SSM::ManagedNode`

AWS 服務	描述	資料事件類型 (主控台)	resources.type 值
Amazon Timestream	資料庫上的 Amazon Timestream Query API 活動。	Timestream 資料庫	AWS::Timestream::Database
	資料庫上的 Amazon Timestream Query API 活動。	Timestream 資料表	AWS::Timestream::Table
Amazon Verified Permissions	政策存放區上的 Amazon Verified Permissions API 活動。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces 瘦客戶端	WorkSpaces 裝置上的精簡型用戶端 API 活動。	精簡型客戶端裝置	AWS::ThinClient::Device
	WorkSpaces 環境上的精簡型用戶端 API 活動。	精簡型客戶端環境	AWS::ThinClient::Environment
AWS X-Ray	軌跡上的 X-Ray API 活動。	X-Ray 軌跡	AWS::XRay::Trace

若要記錄資 CloudTrail 料事件，您必須明確新增要為其收集活動的每個資源類型。如需詳細資訊，請參閱 建立追蹤 及 使用主控台為 CloudTrail事件建立事件資料存放區。

在單一區域追蹤或事件資料存放區上，您只能針對該區域可存取的資源記錄資料事件。雖然 S3 儲存貯體是全域儲存貯體，但 AWS Lambda 函式和 DynamoDB 資料表是區域性的。

記錄資料事件需支付額外的費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

範例：記錄 Amazon S3 物件的資料事件

記錄的 S3 儲存貯體中所有 S3 物件的資料事件

下例示範當您設定記錄名為 *bucket-1* 之 S3 儲存貯體的所有資料事件時，記錄如何運作。在此範例中， CloudTrail 使用者指定了空白前置詞，以及同時記錄讀取和寫入資料事件的選項。

1. 使用者將物件上傳至 bucket-1。
2. PutObject API 操作是 Amazon S3 物件層級的 API。它會在中記錄為資料事件 CloudTrail。由於 CloudTrail 使用者指定了帶有空前綴的 S3 儲存貯體，因此會記錄該儲存貯體中任何物件上發生的事件。追蹤或事件資料存放區會處理並記錄事件。
3. 另一位使用者將物件上傳至 bucket-2。
4. 發生在 S3 儲存貯體物件上的 PutObject API 操作，並未針對追蹤或事件資料存放區指定。追蹤或事件資料存放區不會記錄事件。

記錄特定 S3 物件的資料事件

以下範例示範當您設定追蹤或事件資料存放區記錄特定 S3 物件的事件時，記錄如何運作。在此範例中， CloudTrail 使用者指定了一個名為 ***bucket-3*** 的 S3 儲存貯體，其前置詞為 ***my-images***，以及僅記錄寫入資料事件的選項。

1. 使用者刪除儲存貯體中使用 my-images 前綴開頭的物件，例如 arn:aws:s3:::bucket-3/my-images/example.jpg。
2. DeleteObject API 操作是 Amazon S3 物件層級的 API。它會在中記錄為寫入資料事件 CloudTrail。物件上發生的事件符合追蹤或事件資料存放區中指定的 S3 儲存貯體和字首。追蹤或事件資料存放區會處理並記錄事件。
3. 另一位使用者刪除 S3 儲存貯體中使用不同前綴的物件，例如 arn:aws:s3:::bucket-3/my-videos/example.avi。
4. 物件上發生的事件不符合您的追蹤或事件資料存放區中指定的字首。追蹤或事件資料存放區不會記錄事件。
5. 使用者為物件 arn:aws:s3:::bucket-3/my-images/example.jpg 呼叫 GetObject API 操作。
6. 事件發生在追蹤或事件資料存放區中指定的儲存貯體和字首上，但 GetObject 是讀取類型的 Amazon S3 物件層級 API。它會在中記錄為「讀取資料」事件 CloudTrail，且追蹤或事件資料存放區未設定為記錄「讀取」事件。追蹤或事件資料存放區不會記錄事件。

> **Note**
>
> 對於追蹤，如果您要記錄特定 Amazon S3 儲存貯體的資料事件，我們不建議您使用要記錄其資料事件的 Amazon S3 儲存貯體，來接收您在資料事件區段中為追蹤指定的日誌檔案。使用同一個 Amazon S3 儲存貯體，會讓您的追蹤在日誌檔案每次交付到您的 Amazon S3 儲存貯體時，記錄資料事件。日誌檔案是依時間間隔交付的彙總事件，所以事件和日誌檔案的比例不是一比一；此事件會記錄在下一個日誌檔案中。例如，當 CloudTrail 交付日誌時，`PutObject`事件發生在 S3 儲存貯體上。如果資料事件區段中也指定了此 S3 儲存貯體，追蹤就會處理 `PutObject` 事件，並記錄為資料事件。這動作是另一個 `PutObject` 事件，而追蹤會再次處理並記錄事件。
>
> 如果您設定追蹤以記錄 AWS 帳戶中的所有 Amazon S3 資料事件，若要避免為接收日誌檔的 Amazon S3 儲存貯體記錄資料事件，請考慮將日誌檔交付到屬於另一個 AWS 帳戶的 Amazon S3 儲存貯體。如需詳細資訊，請參閱 從多個帳戶接收 CloudTrail 日誌文件。

記錄其他 AWS 帳戶中 S3 物件的資料事件

當您設定追蹤以記錄資料事件時，您也可以指定屬於其他 AWS 帳戶的 S3 物件。在指定的物件上發生事件時，會 CloudTrail 評估事件是否符合每個帳戶中的任何追蹤。如果事件符合追蹤的設定，則追蹤會處理並記錄該帳戶的事件。通常，API 呼叫者和資源擁有者都可以接收事件。

如果您擁有 S3 物件，並在您的追蹤中指定了此物件，您的追蹤會記錄發生在您帳戶中此物件的事件。因為您擁有此物件，所以您的追蹤也會記錄其他帳戶呼叫此物件時的事件。

如果您在您的追蹤中指定了 S3 物件，但另一個帳戶擁有此物件，您的追蹤就只會記錄發生在您帳戶中該物件的事件。您的追蹤不會記錄發生在其他帳戶的事件。

範例：記錄兩個 AWS 帳戶中一個 Amazon S3 物件的資料事件

下列範例顯示兩個 AWS 帳戶如 CloudTrail 何設定以記錄相同 S3 物件的事件。

1. 在您的帳戶中，您希望您的追蹤將所有物件的資料事件記錄在您名為 `owner-bucket` 的 S3 儲存貯體中。您可以透過指定有空物件前綴的 S3 儲存貯體，來設定追蹤。
2. Bob 的獨立帳戶可以存取 S3 儲存貯體。Bob 也想記錄同一個 S3 儲存貯體中所有物件的資料事件。他為自己的追蹤設定了追蹤，並指定有空物件前綴的同一個 S3 儲存貯體。
3. Bob 使用 `PutObject` API 操作將物件上傳到 S3 儲存貯體。
4. 這個事件發生在他的帳戶中，而且符合他的追蹤設定。Bob 的追蹤會處理並記錄此事件。

5. 因為您擁有此 S3 儲存貯體，而且此事件符合您的追蹤設定，所以您的追蹤也會處理並記錄相同的事件。由於現在有兩個事件副本（一個登錄在 Bob 的跟踪中，一個已登錄您的），所以 CloudTrail 收取兩個數據事件副本的費用。
6. 您將物件上傳至 S3 儲存貯體。
7. 這個事件發生在您的帳戶中，而且符合您的追蹤設定。您的追蹤會處理並記錄此事件。
8. 由於 Bob 的帳戶中不會發生事件，而且他不擁有 S3 儲存貯體，Bob 的追蹤不會記錄事件。CloudTrail 此資料事件只會收取一份副本的費用。

範例：記錄所有儲存貯體的資料事件，包括兩個 AWS 帳戶使用的 S3 儲存貯體

下列範例顯示針對收集帳戶中資料事件的追蹤啟用 [選取帳戶中的所有 S3 儲存貯體] 時的記錄行為 AWS 。

1. 在您的帳戶中，您希望您的追蹤記錄所有 S3 儲存貯體的資料事件。您可以針對資料事件中的所有目前和未來的 S3 儲存貯體選擇讀取事件、寫入事件，或兩者都選擇。
2. Bob 的獨立帳戶可以存取您帳戶中的 S3 儲存貯體。他希望針對有權存取的儲存貯體記錄資料事件。他會將自己的追蹤設定為取得所有 S3 儲存貯體的資料事件。
3. Bob 使用 `PutObject` API 操作將物件上傳到 S3 儲存貯體。
4. 這個事件發生在他的帳戶中，而且符合他的追蹤設定。Bob 的追蹤會處理並記錄此事件。
5. 因為您擁有此 S3 儲存貯體，而且此事件符合您的追蹤設定，所以您的追蹤也會處理並記錄事件。由於現在有兩個事件副本（一個登錄在 Bob 的跟踪中，另一個已登錄您的），因此請向每個帳戶 CloudTrail 收取數據事件副本的費用。
6. 您將物件上傳至 S3 儲存貯體。
7. 這個事件發生在您的帳戶中，而且符合您的追蹤設定。您的追蹤會處理並記錄此事件。
8. 由於 Bob 的帳戶中不會發生事件，而且他不擁有 S3 儲存貯體，Bob 的追蹤不會記錄事件。CloudTrail 您帳戶中只會收取一份此資料事件副本的費用。
9. 第三位使用者 Mary 可存取 S3 儲存貯體，並在儲存貯體上執行 `GetObject` 作業。她在帳戶中具有設為記錄所有 S3 儲存貯體之資料事件的追蹤。因為她是 API 呼叫者，所以會在她的追蹤中 CloudTrail 記錄資料事件。雖然 Bob 可以存取儲存貯體，但他不是資源擁有者，所以這次沒有任何事件記錄在他的追蹤中。身為資源擁有者，您會在追蹤中收到有關 Mary 呼叫之`GetObject`作業的事件。 CloudTrail向您的帳戶和 Mary 的帳戶收取每個數據事件副本的費用：一個在瑪麗的跟踪中，一個在您的。

唯讀和唯寫事件

當您設定您的追蹤或事件資料存放區以記錄資料和管理事件時，您可以指定要記錄唯讀事件、唯寫事件，還是都記錄。

- 讀取

  讀事件包含讀取您的資源，但不予變更的 API 操作。例如，唯讀事件包含 Amazon EC2 `DescribeSecurityGroups` 和 `DescribeSubnets` API 操作。這些操作僅傳回 Amazon EC2 資源的相關資訊，但不變更您的組態。

- 寫入

  Write (寫) 事件只包含會修改 (或可能修改) 您資源的 API 操作。例如，Amazon EC2 `RunInstances` 和 `TerminateInstances` API 操作會修改您的執行個體。

範例：記錄不同追蹤的讀和寫事件

以下範例說明如何設定追蹤，將帳戶的日誌活動分割成不同的 S3 儲存貯體：一個儲存貯體接收唯讀事件，第二個儲存貯體收到唯寫事件。

1. 您要建立一個追蹤，然後選擇名為 `read-only-bucket` 的 S3 儲存貯體接收日誌檔案。接著，您要更新追蹤，指定您要讀管理事件和資料事件。
2. 您要建立第二個追蹤，然後選擇名為 `write-only-bucket` 的 S3 儲存貯體接收日誌檔案。接著，您要更新追蹤，指定您要寫管理事件和資料事件。
3. Amazon EC2 `DescribeInstances` 和 `TerminateInstances` API 操作發生在您的帳戶中。
4. `DescribeInstances` API 操作是唯讀事件，且符合第一個追蹤的設定。追蹤會記錄事件並將它交付到 `read-only-bucket`。
5. `TerminateInstances` API 操作是唯寫事件，且符合第二個追蹤的設定。追蹤會記錄事件並將它交付到 `write-only-bucket`。

記錄資料事件 AWS Management Console

下列程序描述如何更新現有的事件資料存放區或追蹤，以使用 AWS Management Console記錄資料事件。如需有關如何建立事件資料存放區以記錄資料事件的資訊，請參閱 使用主控台為 CloudTrail事件建立事件資料存放區。如需有關如何建立追蹤以記錄資料事件的資訊，請參閱 在主控台中建立追蹤。

針對追蹤，記錄資料事件的步驟會因您使用的是進階事件選取器或基本事件選取器而有所不同。您可以使用進階事件選取器記錄所有資料事件類型的資料事件，但如果使用基本事件選取器，則只能記錄 Amazon S3 儲存貯體和儲存貯體物件、 AWS Lambda 函數和 Amazon DynamoDB 表的資料事件。

更新現有事件資料存放區以記錄 AWS Management Console

使用以下程序更新現有的事件資料存放區，以便記錄資料事件。如需有關使用進階事件選取器的詳細資訊，請參閱本主題使用進階事件選取器篩選資料事件中的。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 在事件資料存放區頁面上，選擇您想要更新的事件資料存放區。

> **Note**
>
> 您只能在包含事件的事件資料存放區上啟用資料 CloudTrail 事件。您無法針對 AWS Config 設定項目、 CloudTrail Insights CloudTrail 事件或非事件啟用事件資料存放區上的資料AWS 事件。

4. 在詳細資訊頁面上，選擇資料事件中的編輯。
5. 如果您尚未記錄資料事件，請選擇 Data events (資料事件) 核取方塊。
6. 針對資料事件類型，選擇您想要記錄資料事件的資源類型。
7. 選擇記錄選取器範本。 CloudTrail 包括記錄資源類型的所有資料事件的預先定義範本。若要建立自訂記錄選取器範本，請選擇 Custom (自訂)。
8. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 `Name` 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。
9. 在進階事件選取器，請為您想要記錄資料事件的特定資源建立表達式。如果您使用預先定義的日誌範本，則可略過此步驟。

    a. 從下列欄位選取。

    - **`readOnly`**-`readOnly` 可以設定為等於`true`或的值`false`。唯讀資料事件是不會變更資源狀態的事件，例如 `Get*` 或 `Describe*` 事件. 寫入事件新增、變更或刪除資源、屬性或成品，例如 `Put*`、`Delete*` 或 `Write*` 事件。若要同時記錄 `read` 和 `write` 事件，請勿新增 `readOnly` 選擇器。

- **eventName**-eventName可以使用任何運算子。您可以使用它來包含或排除記錄到的任何資料事件 CloudTrailPutBucket，例如GetItem、或GetSnapshotBlock。
- **resources.ARN**-您可以將任何運算子搭配使用resources.ARN，但是如果您使用 equals 或不等於，則值必須完全符合您在範本中指定為值之類型之有效資源的 ARN。resources.type

  下表顯示每種 resources.type 的有效 ARN 格式。

  > **Note**
  >
  > 您無法使用resources.ARN欄位來篩選沒有 ARN 的資源類型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	resources.ARN
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	ARN 必須採用下列其中一種格式： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必須採用下列其中一種格式： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*

resources.type	resources.ARN
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您指定 AWS::DynamoDB::Table 作為 resources.type，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在eventName欄位上新增篩選器。

[2] 若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 StartsWith 運算子，並僅包含儲存貯體 ARN 作為相符值。末尾斜線是有意保留，請勿排除。

[3] 若要在 S3 存取點中的所有物件上記錄事件，建議您僅使用存取點 ARN、不要包含物件路徑，並使用 StartsWith 或 NotStartsWith 運算子。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的動作、資源及條件金鑰。

b. 針對每個欄位，選擇 + 條件，視需要新增任意數目的條件，所有條件最多可指定 500 個值。例如，若要從事件資料存放區記錄的資料事件中排除兩個 S3 儲存貯體的資料事件，您可以將欄位設定為 Resources .arn，將運算子設定為「不開始於」，然後貼上 S3 儲存貯體 ARN，或瀏覽不想記錄事件的 S3 儲存貯體。

若要新增第二個 S3 儲存貯體，請選擇 + 條件，然後重複上述指令，在 ARN 中粘貼或瀏覽不同的儲存貯體。

> **Note**
>
> 對於事件資料存放區上的所有選取器，您最多可以有 500 個值。這包括一個選擇器的多個值的陣列，如 `eventName`。如果所有選擇器都有單個值，則最多可以有 500 個條件新增至選擇器。

c. 選擇 + 欄位以根據需要新增其他欄位。為避免發生錯誤，請勿為欄位設定衝突或重複的值。例如，不要在一個選擇器中指定 ARN 等於一個值，然後指定 ARN 不等於另一個選取器中的相同值。

10. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。重複步驟 6 到此步驟，以設定資料事件類型的進階事件選取器。
11. 檢閱並驗證您的選擇後，選擇儲存變更。

使用中的進階事件選取器更新現有追蹤以記錄資料事件 AWS Management Console

在中 AWS Management Console，如果您的追蹤使用進階事件選取器，您可以從預先定義的範本中進行選擇，以記錄所選資源上的所有資料事件。選擇日誌選取器範本之後，您可以自訂範本，以僅包含您最想要查看的資料事件。如需有關使用進階事件選取器的詳細資訊，請參閱本主題使用進階事件選取器篩選資料事件中的。

1. 在 CloudTrail 主控台的 [儀表板] 或 [追蹤] 頁面上，選擇您要更新的追蹤。
2. 在詳細資訊頁面上，選擇資料事件中的編輯。
3. 如果您尚未記錄資料事件，請選擇 Data events (資料事件) 核取方塊。
4. 針對資料事件類型，選擇您想要記錄資料事件的資源類型。
5. 選擇記錄選取器範本。 CloudTrail 包括記錄資源類型的所有資料事件的預先定義範本。若要建立自訂記錄選取器範本，請選擇 Custom (自訂)。

> **Note**
>
> 為 S3 儲存貯體選擇預先定義的範本，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的值區上執行。
>
> 如果追蹤僅套用至一個區域，選取預先定義的記錄所有 S3 儲存貯體的範本可針對下列儲存貯體啟用記錄資料事件：與您追蹤相同之區域中的所有儲存貯體，以及您稍後在該區域

中建立的任何儲存貯體。它不會記錄帳戶中其他區域中 Amazon S3 儲存貯體的 AWS 資料事件。
如果您要為所有區域建立追蹤，選擇 Lambda 函數的預先定義範本可啟用 AWS 帳戶中目前所有函數的資料事件記錄，以及您在任何區域建立追蹤後可能在任何區域建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (針對追蹤，這只能使用使用 AWS CLI)，則此選項會啟用 AWS 帳戶中該區域目前所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。
記錄所有函數的資料事件也可讓您記錄 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於其他 AWS 帳戶的函數上執行。

6. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。

7. 在進階事件選取器，請為您想要記錄資料事件的特定資源建立表達式。如果您使用預先定義的日誌範本，則可略過此步驟。

   a. 從下列欄位選取。

   - **readOnly**-readOnly 可以設定為等於true或的值false。唯讀資料事件是不會變更資源狀態的事件，例如 Get* 或 Describe* 事件. 寫入事件新增、變更或刪除資源、屬性或成品，例如 Put*、Delete* 或 Write* 事件。若要同時記錄 read 和 write 事件，請勿新增 readOnly 選擇器。
   - **eventName**-eventName可以使用任何運算子。您可以使用它來包含或排除記錄到的任何資料事件 CloudTrailPutBucket，例如GetItem、或GetSnapshotBlock。
   - **resources.ARN**-您可以將任何運算子搭配使用resources.ARN，但是如果您使用 equals 或不等於，則值必須完全符合您在範本中指定為值之類型之有效資源的 ARN。resources.type

     下表顯示每種 resources.type 的有效 ARN 格式。

     > **Note**
     >
     > 您無法使用resources.ARN欄位來篩選沒有 ARN 的資源類型。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*

resources.type	resources.ARN
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*

resources.type	resources.ARN
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*

resources.type	resources.ARN
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*

resources.type	resources.ARN
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*

resources.type	resources.ARN
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必須採用下列其中一種格式： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	ARN 必須採用下列其中一種格式： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 對於已啟用串流的資料表，資料事件中的 `resources` 欄位會同時包含 `AWS::DynamoDB::Stream` 和 `AWS::DynamoDB::Table`。如果您指定 `AWS::DynamoDB::Table` 作為 `resources.type`，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在`eventName`欄位上新增篩選器。

[2] 若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 `StartsWith` 運算子，並僅包含儲存貯體 ARN 作為相符值。末尾斜線是有意保留，請勿排除。

[3] 若要在 S3 存取點中的所有物件上記錄事件，建議您僅使用存取點 ARN、不要包含物件路徑，並使用 `StartsWith` 或 `NotStartsWith` 運算子。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的動作、資源及條件金鑰。

b. 針對每個欄位，選擇 + 條件，視需要新增任意數目的條件，所有條件最多可指定 500 個值。例如，若要從追蹤記錄的資料事件中排除兩個 S3 儲存貯體的資料事件，您可以將欄位設定為 Resources .arn，將運算子設定為「不開始於」，然後貼上 S3 儲存貯體 ARN，或瀏覽您不想記錄事件的 S3 儲存貯體。

若要新增第二個 S3 儲存貯體，請選擇 + 條件，然後重複上述指令，在 ARN 中粘貼或瀏覽不同的儲存貯體。

> **Note**
>
> 追蹤上的所有選取器，您最多可以有 500 個值。這包括一個選擇器的多個值的陣列，如 `eventName`。如果所有選擇器都有單個值，則最多可以有 500 個條件新增至選擇器。

c. 選擇 + 欄位以根據需要新增其他欄位。為避免發生錯誤，請勿為欄位設定衝突或重複的值。例如，不要在一個選擇器中指定 ARN 等於一個值，然後指定 ARN 不等於另一個選取器中的相同值。

8. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。重複步驟 4 到此步驟，以設定資料事件類型的進階事件選取器。
9. 檢閱並驗證您的選擇後，選擇儲存變更。

使用中的基本事件選取器更新現有的追蹤，以記錄資料事件 AWS Management Console

依照以下程序，使用基本事件選取器更新現有的追蹤，以便記錄資料事件。

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 開啟主 CloudTrail 控台的「追蹤」頁面，然後選擇追蹤名稱。

> **Note**
>
> 雖然您可以編輯現有的追蹤來記錄資料事件，但是作為最佳實務，請考慮建立單獨追蹤記錄資料事件。

3. 針對資料事件，選擇 Edit (編輯)。
4. 對於 Amazon S3 儲存貯體：
   a. 對於 Data source (資料來源)，請選擇 S3。
   b. 您可以選取記錄所有目前和未來的 S3 儲存貯體，也可以指定個別儲存貯體或函數。依預設，會記錄所有目前和未來 S3 儲存貯體的資料事件。

> **Note**
>
> 保留預設的 [所有目前和 future 的 S3 儲存貯體] 選項，可為 AWS 帳戶中目前的所有儲存貯體以及您在完成追蹤建立後建立的任何儲存貯體啟用資料事件記錄。它還可以記錄您 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的值區上執行。
> 如果您要為單一區域建立追蹤 (使用完成 AWS CLI)，請選取 [選取帳戶中的所有 S3 儲存貯體] 選項，啟用與追蹤相同區域中的所有儲存貯體的資料事件記錄，以及稍後在該區域中建立的任何儲存貯體的資料事件記錄。它不會記錄帳戶中其他區域中 Amazon S3 儲存貯體的 AWS 資料事件。

   c. 如果您保留預設值，所有目前和未來的 S3 儲存貯體，選擇記錄讀事件、寫事件，或兩者。
   d. 若要選擇個別儲存貯體，請清空所有目前和未來的 S3 儲存貯體的讀和寫核取方塊。在個別儲存貯體選擇中，瀏覽要記錄資料事件的儲存貯體。若要尋找特定儲存貯體，請輸入所需儲存貯體的儲存貯體字首。您可以在此視窗中選取多個儲存貯體。選擇新增儲存貯體以記錄更多儲存貯體的資料事件。選擇記錄 Read (讀取) 事件 (例如 `GetObject`)、Write (寫) 事件 (例如 `PutObject`) 還是兩者。

此設定的優先順序高於您針對個別儲存貯體所設定的個別設定。例如，如果您指定記錄所有 S3 儲存貯體之 Read (讀取) 事件，然後選擇新增要記錄資料事件的特定儲存貯體，則您新增的儲存貯體會直接選取 Read (讀取)。您無法清除選取項目。您只能設定 Write (寫入) 的選項。

若要從記錄中移除儲存貯體，請選擇 X。

5. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。
6. 針對 Lambda 函數：

   a. 針對資料事件來源中，選擇 Lambda。

   b. 在 Lambda 函數中，選擇所有區域來記錄所有的 Lambda 函數，或者輸入函數作為 ARN以記錄特定函數的資料事件。

   若要記錄 AWS 帳戶中所有 Lambda 函數的資料事件，請選取 Log all current and future functions (記錄所有目前和未來的函數)。此設定的優先順序高於您針對個別函數所設定的個別設定。皆會記錄所有函數，縱使未顯示全部的函數。

   > **Note**
   >
   > 如果您要建立所有區域的追蹤，則此選取項目可針對下列函數啟用記錄資料事件：目前在您 AWS 帳戶中的所有函數，以及在您完成建立追蹤之後可能在任何區域中建立的任何 Lambda 函數。如果您要為單一區域建立追蹤 (透過使用完成 AWS CLI)，此選項會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立追蹤後可能在該區域中建立的任何 Lambda 函數。並不會為其他區域中所建立之 Lambda 函數啟用記錄資料事件。
   > 記錄所有函數的資料事件也可讓您記錄 AWS 帳戶中任何使用者或角色所執行的資料事件活動，即使該活動是在屬於其他 AWS 帳戶的函數上執行。

   c. 如果您選擇輸入函數作為 ARN，請輸入 Lambda 函數的 ARN。

   > **Note**
   >
   > 如果您的帳戶中有超過 15,000 個 Lambda 函數，則無法在建立追蹤時在 CloudTrail 主控台中檢視或選取所有函數。您仍然可以選取記錄所有函數的選項，縱使其未全部顯示。如果您要記錄特定函數之資料事件，則可以在得知該函數的 ARN 後手動加以新增。您也可以在主控台中完成追蹤的建立，然後使用 AWS CLI 和put-event-

selectors命令為特定 Lambda 函數設定資料事件記錄。如需詳細資訊，請參閱 管理軌跡 AWS CLI。

7. 若要新增其他要記錄資料事件的資料類型，請選擇 Add data event type (新增資料事件類型)。
8. 針對 DynamoDB 資料表：
   a. 針對資料事件來源中，選擇 DynamoDB。
   b. 在 DynamoDB 資料表選取中，選擇 Browse (瀏覽) 以選取表格，或貼到您有權存取的 DynamoDB 資料表的 ARN 中。DynamoDB 資料表 ARN 採用以下格式：

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

   若要新增其他資料表，請選擇 Add row (新增資料列)，然後瀏覽資料表或貼上您可以存取之資料表的 ARN。
9. 選擇儲存變更。

記錄資料事件 AWS Command Line Interface

您可以使用 AWS CLI設定您的追蹤或事件資料存放區，以記錄資料事件。

主題

- 記錄跟踪的數據事件 AWS CLI
- 記錄事件資料存放區的資料事件 AWS CLI

記錄跟踪的數據事件 AWS CLI

您可以設定您的追蹤，使用 AWS CLI記錄管理和資料事件。

> **Note**
>
> - 請注意，如果您的帳戶記錄多個管理事件副本，則會產生費用。記錄資料事件始終需支付費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。
> - 您可以使用進階事件選取器或基本事件選取器，但不能同時使用兩者。如果您將進階事件選取器套用至追蹤，則會覆寫任何現有的基本事件選取器。
> - 如果您的追蹤使用基本事件選取器，您只能記錄下列資源類型：

- `AWS::DynamoDB::Table`
- `AWS::Lambda::Function`
- `AWS::S3::Object`

您將需要使用進階事件選取器才能記錄其他資源類型。若要將追蹤轉換為進階事件選取器，請執行 get-event-selectors 命令以確認目前的事件選取器，然後將進階事件選取器的涵蓋範圍設定為與先前的事件選取器相同，再為您想記錄資料事件的任何資源類型新增選取器。

- 您可以使用進階事件選取器來根據 `eventName`、`resources.ARN` 和 `readOnly` 欄位的值進行篩選，從而只記錄您感興趣的資料事件。如需有關設定這些欄位的詳細資訊，請參閱 AdvancedFieldSelectorAWS CloudTrailAPI 參考和本主題使用進階事件選取器篩選資料事件中的。

若要查看您的追蹤是記錄管理還是資料事件，請執行 `get-event-selectors` 命令。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

此命令會傳回軌跡的事件選取器。

主題

- 使用進階事件選取器記錄事件
- 使用進階事件選取器記錄 Amazon S3 儲存貯體的所有 Amazon S3 事件
- 使用進階事件選取器將 Amazon S3 記錄在 AWS Outposts 事件
- 使用基本事件選取器記錄事件

使用進階事件選取器記錄事件

> **Note**
>
> 如果您將進階事件選取器套用至追蹤，則會覆寫任何現有的基本事件選取器。在設定進階事件選取器前，請執行 get-event-selectors 命令以確認目前的事件選取器，然後將進階事件選取器的涵蓋範圍設定為與先前的事件選取器相同，再為您想記錄的任何其他資料事件新增選取器。

下列範例會為名*TrailName*為包含讀取和寫入管理事件的追蹤建立自訂進階事件選取器 (透過省略選`readOnly`取器)，以`PutObject`及所有 Amazon S3 儲存貯體/前綴組合的`DeleteObject`資

料事件 (名為的儲存貯體sample_bucket_name和名為函數的資料事件除外)。 AWS Lambda MyLambdaFunction因為這些都是自訂進階事件選取器，所以每組選取器都有一個描述性的名稱。請注意，尾步斜線是 S3 儲存貯體 ARN 值的一部分。

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

範例傳回針對追蹤設定的進階事件選取器。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
```

```
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
```

```
}
```

使用進階事件選取器記錄 Amazon S3 儲存貯體的所有 Amazon S3 事件

> **Note**
>
> 如果您將進階事件選取器套用至追蹤，則會覆寫任何現有的基本事件選取器。

以下範例說明如何設定您的追蹤在特定 S3 儲存貯體中包含所有 Amazon S3 物件的所有管理和資料事件。`resources.type` 欄位的 S3 事件的值是 `AWS::S3::Object`。由於 S3 物件和 S3 儲存貯體的 ARN 值略有不同，因此您必須為 `resources.ARN` 新增 `StartsWith` 運算子以擷取所有事件。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
```

```
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                }
            ]
        }
    ]
}
```

使用進階事件選取器將 Amazon S3 記錄在 AWS Outposts 事件

> **Note**
>
> 如果您將進階事件選取器套用至追蹤，則會覆寫任何現有的基本事件選取器。

以下範例說明如何設定您的追蹤以在 Outpost 中的 Outposts 物件上包含所有 Amazon S3 的所有資料事件。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
```

```
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

使用基本事件選取器記錄事件

以下是顯示基本事件選取器的 get-event-selectors 命令的範例結果。依預設，當您使用建立追蹤時 AWS CLI，追蹤會記錄所有管理事件。根據預設，追蹤不會記錄資料事件。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

若要設定您的追蹤記錄管理和資料事件，請執行 put-event-selectors 命令。

以下範例說明如何使用基本事件選取器設定您的追蹤，以便包含兩個 S3 儲存貯體字首中的 S3 物件之全部管理和資料事件。您可以為追蹤指定 1 到 5 個事件選取器。您可以為追蹤指定 1 到 250 項資料資源。

> **Note**
>
> 如果您選擇使用基本事件選取器限制資料事件，S3 資料資源的數目上限為 250。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

此範例會傳回為追蹤設定的事件選取器。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

記錄事件資料存放區的資料事件 AWS CLI

您可以使用 AWS CLI設定您的事件資料存放區，以包含資料事件。使用 create-event-data-store 命令來建立用於記錄資料事件的新事件資料存放區。使用 update-event-data-store 命令來為現有的事件資料存放區更新進階事件選取器。

若要了解您的事件資料存放區是否包括資料事件，請執行 get-event-data-store 命令。

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

此命令會傳回事件資料存放區的設定。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

主題

- 包含儲存貯體的所有 Amazon S3 事件
- 包含 AWS Outposts 上的 Amazon S3 的事件

包含儲存貯體的所有 Amazon S3 事件

以下範例說明如何建立事件資料存放區，以包含特定 S3 儲存貯體中所有 Amazon S3 物件的全部資料事件。`resources.type` 欄位的 S3 事件的值是 `AWS::S3::Object`。由於 S3 物件和 S3 儲存貯體的 ARN 值略有不同，因此您必須為 `resources.ARN` 新增 `StartsWith` 運算子以擷取所有事件。

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

命令會傳回下列範例輸出。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
```

```
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

包含 AWS Outposts 上的 Amazon S3 的事件

以下範例說明如何建立事件資料存放區，以包含 Outpost 中所有 Outposts 上的 Amazon S3 物件的全部資料事件。

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

命令會傳回下列範例輸出。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
```

```
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

使用進階事件選取器篩選資料事件

本節說明如何使用進階事件選取器來建立精細的選取器，只記錄感興趣的特定資料事件，藉此協助您控制成本。

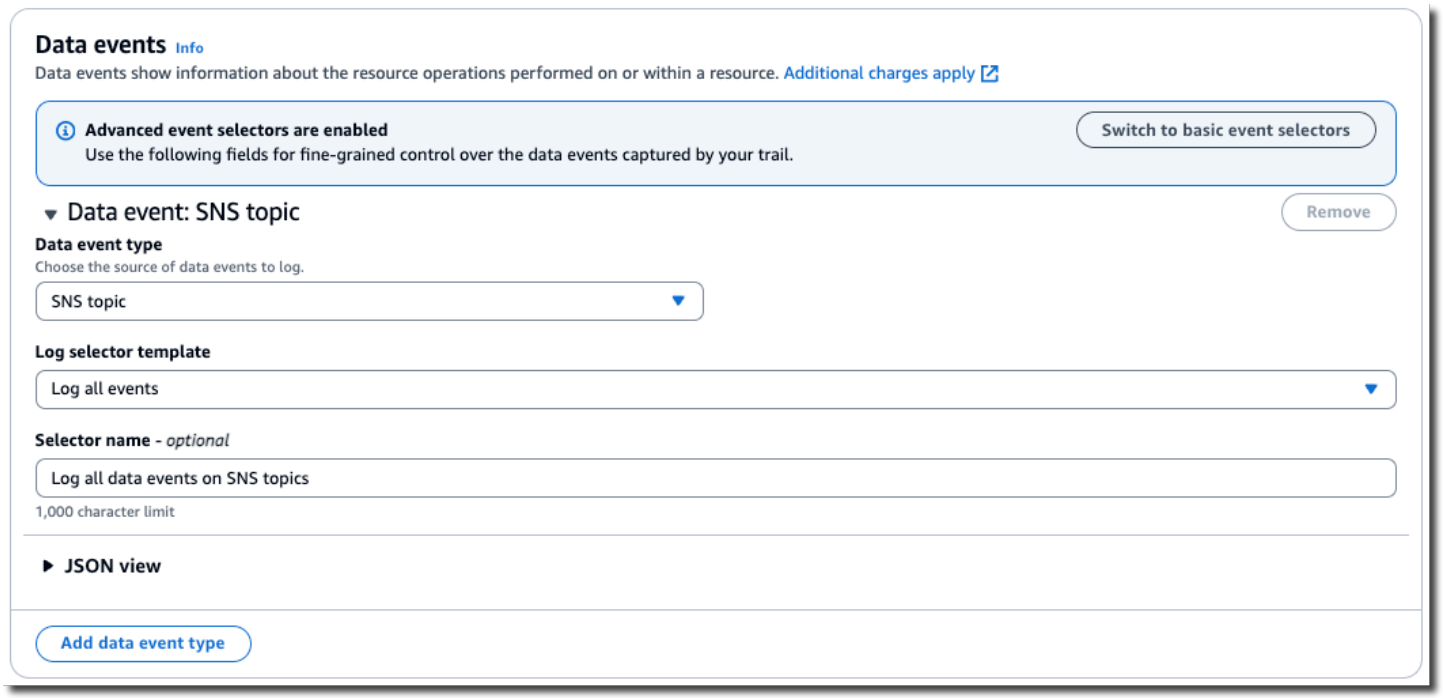
例如：

- 您可以在eventName欄位上新增篩選器，以包含或排除特定的 API 呼叫。
- 您可以在resources.ARN欄位上新增篩選器，以包含或排除特定資源的記錄。例如，如果您要記錄 S3 資料事件，您可以針對追蹤排除 S3 儲存貯體的記錄。
- 您可以在欄位上新增篩選器，選擇僅記錄唯寫事件或唯讀事件。readOnly

下表提供有關進階事件選取器之可設定欄位的其他資訊。

欄位	必要	有效運算子	描述
eventCategory	是	Equals	此欄位設定Data為記錄資料事件。
resources.type	是	Equals	此欄位用於選取您要記錄其資料事件的資源類型。「資料事件」表格會顯示可能的值。
readOnly	否	Equals	這是選擇性欄位，用於根據readOnly值包含或排除資料事件。true記錄檔的值僅讀取事件。false記錄檔的值僅寫入事件。如果您未新增此欄位，則會同時 CloudTrail 記錄讀取和寫入事件。
eventName	否	任何	這是一個選擇性的欄位，用來搜尋或搜尋任何記錄到的資料事件 CloudTrail，例如或。PutBucket GetSnapshotBlock 如果您使用的是 AWS CLI，您可以使用逗號分隔每個值來指定多個值。 如果您使用主控台，您可以為每eventName 個要篩選的項目建立條件來指定多個值。
resources.ARN	否	任何	這是選擇性欄位，用來排除或包含特定資源的資料事件，方法是提供resources.ARN 。您可以使用任何運算子resources.ARN ，但如果您使用Equals或NotEquals ，值必須完全符合resoureces.type 您指定的有效資源的 ARN。 如果您使用的是 AWS CLI，您可以使用逗號分隔每個值來指定多個值。 如果您使用主控台，您可以為每resources .ARN 個要篩選的項目建立條件來指定多個值。

若要使用 CloudTrail 主控台記錄資料事件，請選擇 [資料事件] 選項，然後在建立或更新追蹤或事件資料存放區時選取感興趣的資料事件類型。「資料事件」表格會顯示您可以在 CloudTrail 主控台上選擇的可能資料事件類型。



若要使用記錄資料事件 AWS CLI，請將`--advanced-event-selector`參數設定為`eventCategory`等於，`Data`且`resources.type`值等於您要記錄資料事件的資源類型值。「資料事件」表格會列出可用的資源類型。

例如，如果您想要記錄所有 Cognito Identity 集區的資料事件，請將`--advanced-event-selectors`參數設定為如下所示：

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
     }
]'
```

上述範例會記錄身分集區上的所有 Cognito 資料事件。您可以進一步調整進階事件選取器，以篩選`eventName`、`readOnly`、和`resources.ARN`欄位，以記錄感興趣的特定事件或排除不感興趣的事件。

您可以設定進階事件選取器，以根據多個條件篩選資料事件。例如，您可以設定進階事件選取器來記錄所有 Amazon S3 PutObject 和 DeleteObject API 呼叫，但排除特定 S3 儲存貯體的事件記錄，如下列範例所示。

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
]'
```

您可以使用進階事件選取器來記錄管理事件和資料事件。若要記錄多種資源類型的資料事件，請為您要記錄資料事件的每個資源類型新增欄位選取器陳述式。

> **Note**
>
> 追蹤可以使用基本事件選取器或進階事件選取器，但不能同時使用兩者。如果您將進階事件選取器套用至追蹤，則會覆寫任何現有的基本事件選取器。

主題

- 篩選資料事件的依據 eventName
- 篩選資料事件的依據 resources.ARN
- 依readOnly值篩選資料事件

篩選資料事件的依據 **eventName**

使用進階事件選取器，您可以根據eventName欄位的值包含或排除事件。篩選eventName可協助控制成本，因為當您記錄資料事件 AWS 服務 以增加對新資料 API 的支援時，可避免產生成本。

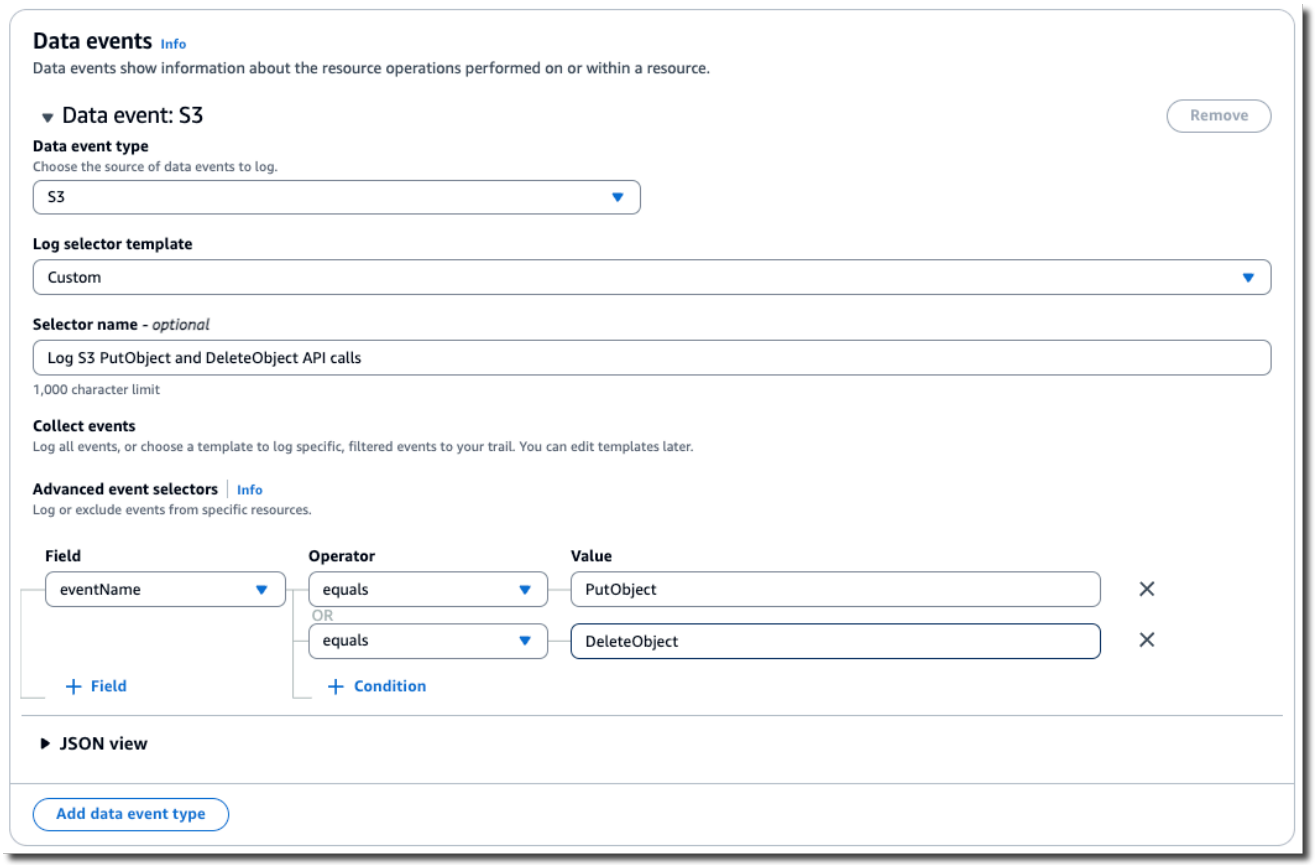
您可以在eventName欄位中使用任何運算子。您可以使用它來搜尋或搜尋記錄到的任何資料事件 CloudTrail，例如或。PutBucket GetSnapshotBlock

主題

eventName使用篩選資料事件 AWS Management Console

採取以下步驟使用 CloudTrail 控制台在eventName字段上進行過濾。

1. 請遵循建立追蹤程序中的步驟，或遵循建立事件資料存放區程序中的步驟。
2. 當您按照步驟建立追蹤或事件資料倉庫時，請進行下列選擇：
    a. 選擇 [資料事件]。
    b. 選擇您要記錄其資料事件的資料事件類型。
    c. 在記錄選取器範本中，選擇自訂。
    d. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。
    e. 在進階事件選取器中，執行下列動作以篩選eventName：
        i. 在 [欄位] 中，選擇 eventName。
        ii. 在「運算子」中，選擇條件運算子。在此範例中，我們將選擇 equals，因為我們想要記錄特定的 API 呼叫。
        iii. 在值中，輸入您要篩選的事件名稱。
        iv. 若要篩選另一個eventName，請選擇 [+ 條件]。



f. 選擇 [+ 欄位] 可在其他欄位上新增篩選條件。

eventName使用篩選資料事件 AWS CLI

使用 AWS CLI，您可以篩選eventName欄位以包含或排除特定事件。

下列範例會在追蹤上記錄 S3 資料事件。設定--advanced-event-selectors為僅記錄GetObject、PutObject和 DeleteObject API 呼叫的資料事件。

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
```

```
  }
]'
```

下一個範例會建立新的事件資料存放區，以記錄 EBS Direct API 的資料事件，但不包括 `ListChangedBlocks` API 呼叫。您可以使用指update-event-data-store令更新既有事件資料倉庫。

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
         ]
    }
]'
```

篩選資料事件的依據 `resources.ARN`

使用進階事件選取器，您可以篩選`resources.ARN`欄位的值。

您可以將任何運算子搭配使用`resources.ARN`，但如果您使用`Equals`或`NotEquals`，則值必須完全符合您所指定`resources.type`值之有效資源的 ARN。若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 `StartsWith` 運算子，並僅包含儲存貯體 ARN 作為相符值。

下表顯示每種 `resources.type` 的有效 ARN 格式。

> **Note**
>
> 您無法使用`resources.ARN`欄位來篩選沒有 ARN 的資源類型。

resources.type	resources.ARN
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`

resources.type	resources.ARN
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*

resources.type	resources.ARN
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*

resources.type	resources.ARN
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*

resources.type	resources.ARN
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*

resources.type	resources.ARN
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*

resources.type	resources.ARN
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*

resources.type	resources.ARN
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN 必須採用下列其中一種格式： • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN 必須採用下列其中一種格式： • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*

resources.type	resources.ARN
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] 對於已啟用串流的資料表，資料事件中的 resources 欄位會同時包含 AWS::DynamoDB::Stream 和 AWS::DynamoDB::Table。如果您指定 AWS::DynamoDB::Table 作為 resources.type，則會根據預設同時記錄 DynamoDB 資料表和 DynamoDB 串流事件。若要排除串流事件，請在eventName欄位上新增篩選器。

[2] 若要記錄特定 S3 儲存貯體中所有物件的所有資料事件，請使用 StartsWith 運算子，並僅包含儲存貯體 ARN 作為相符值。末尾斜線是有意保留，請勿排除。

[3] 若要在 S3 存取點中的所有物件上記錄事件，建議您僅使用存取點 ARN、不要包含物件路徑，並使用 StartsWith 或 NotStartsWith 運算子。

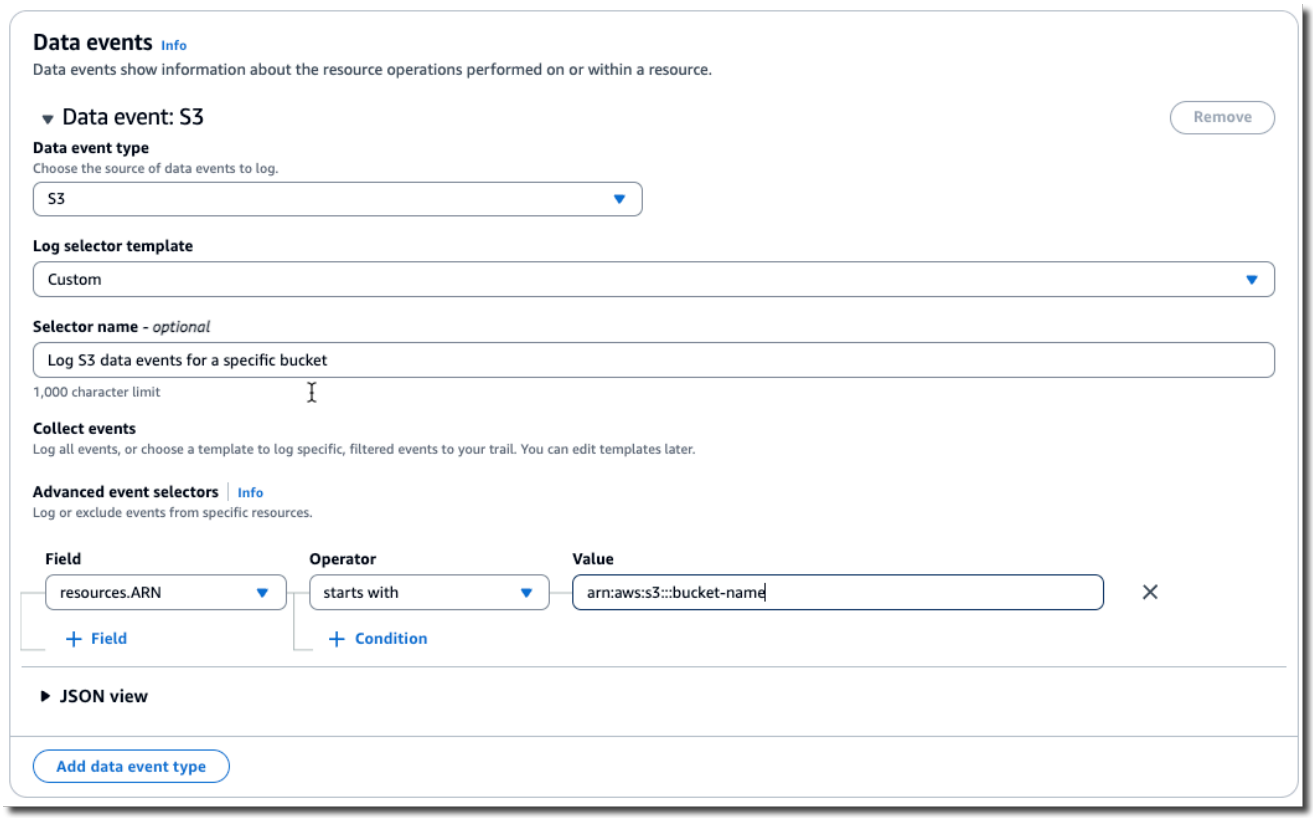
主題

- resources.ARN使用篩選資料事件 AWS Management Console
- resources.ARN使用篩選資料事件 AWS CLI

resources.ARN使用篩選資料事件 AWS Management Console

採取以下步驟使用 CloudTrail 控制台在`resources.ARN`字段上進行過濾。

1. 請遵循建立追蹤程序中的步驟，或遵循建立事件資料存放區程序中的步驟。
2. 當您按照步驟建立追蹤或事件資料倉庫時，請進行下列選擇：
   a. 選擇 [資料事件]。
   b. 選擇您要記錄其資料事件的資料事件類型。
   c. 在記錄選取器範本中，選擇自訂。
   d. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「僅為兩個 S3 儲存貯體記錄資料事件」。選取器名稱會被作為 Name 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。
   e. 在進階事件選取器中，執行下列動作以篩選`resources.ARN`：
      i. 對於欄位，選擇 resources.ARN。
      ii. 在「運算子」中，選擇條件運算子。在此範例中，我們將選擇「開始為」，因為我們想要記錄特定 S3 儲存貯體的資料事件。
      iii. 在值中，輸入您的資源類型的 ARN (例如，*arn: aw:* s3:: 儲存貯體名稱)。
      iv. 若要篩選另一個`resources.ARN`，請選擇 [+ 條件]。



f. 選擇 [+ 欄位] 可在其他欄位上新增篩選條件。

`resources.ARN`使用篩選資料事件 AWS CLI

使用 AWS CLI，您可以篩選`resources.ARN`欄位以記錄特定 ARN 的事件，或排除特定 ARN 的記錄。

以下範例說明如何設定您的追蹤在特定 S3 儲存貯體中包含所有 Amazon S3 物件的所有管理和資料事件。`resources.type` 欄位的 S3 事件的值是 `AWS::S3::Object`。由於 S3 物件和 S3 儲存貯體的 ARN 值略有不同，因此您必須為 `resources.ARN` 新增 `StartsWith` 運算子以擷取所有事件。

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
```

```
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:aws:s3:::bucket_name/"] }
            ]
    }
]'
```

依**readOnly**值篩選資料事件

使用進階事件選取器，您可以根據readOnly欄位的值進行篩選。

您只能在readOnly欄位中使用Equals運算子。您可以將readOnly值設定為true或false。如果您未新增此欄位，則會同時 CloudTrail 記錄讀取和寫入事件。true記錄檔的值僅讀取事件。false記錄檔的值僅寫入事件。

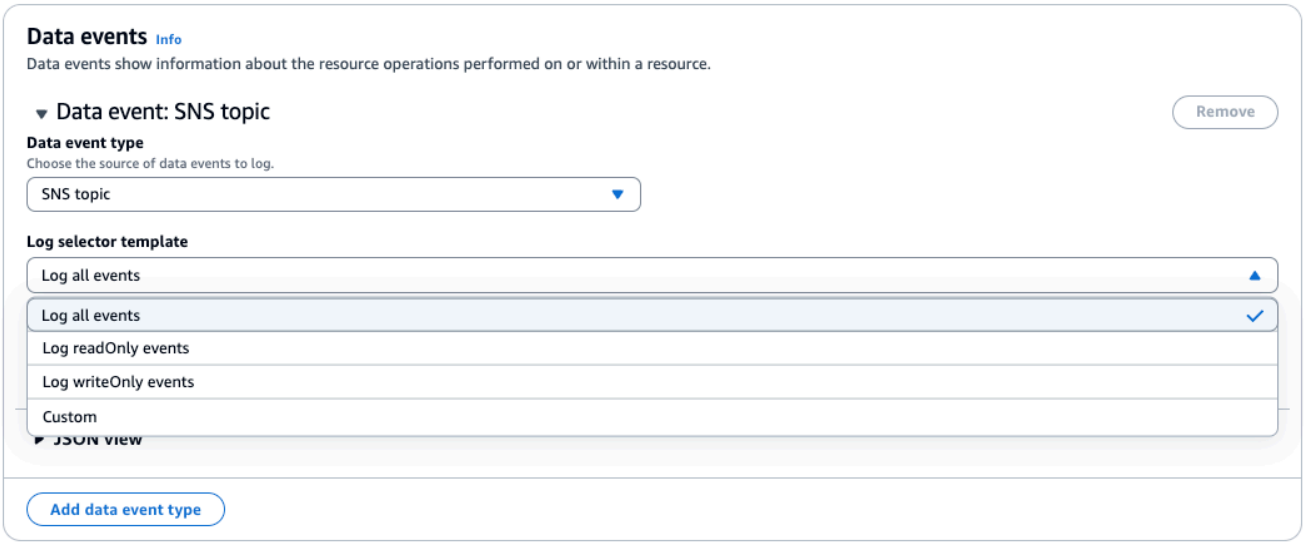
主題

- 使用readOnly值篩選資料事件 AWS Management Console
- 使用readOnly值篩選資料事件 AWS CLI

使用**readOnly**值篩選資料事件 AWS Management Console

採取以下步驟使用 CloudTrail 控制台在readOnly字段上進行過濾。

1. 請遵循建立追蹤程序中的步驟，或遵循建立事件資料存放區程序中的步驟。
2. 當您按照步驟建立追蹤或事件資料倉庫時，請進行下列選擇：
    a. 選擇 [資料事件]。
    b. 選擇您要記錄其資料事件的資料事件類型。
    c. 針對記錄選取器範本，選擇適合您使用案例的範本。



如果你打算這樣做	選擇此記錄檔選取器範本
僅記錄讀取事件，不套用其他篩選器 (例如，在`resources.ARN` 值上)。	記錄唯讀事件
僅記錄寫入事件，不套用其他篩選器 (例如，在`resources.ARN` 值上)。	記錄唯寫事件

如果你打算這樣做	選擇此記錄檔選取器範本
篩選readOnly值並套用其他篩選器 (例如，在resources.ARN 值上)。	Custom (自訂) 在進階事件選取器中，執行下列動作以篩選readOnly值： 若要記錄寫入事件 a. 對於欄位，選擇 readOnly。 b. 對於運算子，選擇 equals。 c. 針對數值，輸入 **false**。 d. 選擇 [+ 欄位] 可在其他欄位上新增篩選條件。 若要記錄讀取事件 a. 對於欄位，選擇 readOnly。 b. 對於運算子，選擇 equals。 c. 針對數值，輸入 **true**。 d. 選擇 [+ 欄位] 可在其他欄位上新增篩選條件。

使用**readOnly**值篩選資料事件 AWS CLI

使用 AWS CLI，您可以篩選readOnly欄位。

您只能在readOnly欄位中使用Equals運算子。您可以將readOnly值設定為true或false。如果您未新增此欄位，則會同時 CloudTrail記錄讀取和寫入事件。true記錄檔的值僅讀取事件。false記錄檔的值僅寫入事件。

下列範例顯示如何設定追蹤，以記錄所有 Amazon S3 物件的唯讀資料事件。

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors '[
    {
```

```
            "Name": "Log read-only S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "readOnly", "Equals": ["true"] }
            ]
    }
]'
```

下一個範例會建立新的事件資料存放區，該資料存放區僅記錄 EBS Direct API 的唯寫資料事件。您可以使用指update-event-data-store令更新既有事件資料倉庫。

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName" \
--advanced-event-selectors \
'[
    {
            "Name": "Log write-only EBS Direct API data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
                { "Field": "readOnly", "Equals": ["false"] }
            ]
     }
]'
```

記錄資料事件以確保 AWS Config 合規

如果您使用一 AWS Config 致性套件來協助企業維持正式標準的合規性，例如聯邦風險與授權管理計畫 (FedRAMP) 或美國國家標準與技術研究所 (NIST) 所要求的標準，則合規框架的一致性套件通常需要您至少記錄 Amazon S3 儲存貯體的資料事件。合規架構的一致性套件包括稱為 `cloudtrail-s3-dataevents-enabled` 的受管規則，可檢查您的帳戶中的 S3 資料事件記錄。許多與合規架構無關的一致性套件也需要 S3 資料事件記錄。以下是包含此規則的一致性套件範例。

- Well-Architec AWS ted 的架構安全性支柱的營運最佳實務
- FDA 標題 21 CFR 操作最佳實務第 11 部分
- FFIEC 的操作最佳實務
- FedRAMP (適中) 的操作最佳實務
- HIPAA 安全的操作最佳實務
- K-ISMS 的操作最佳實務

- 記錄的操作最佳實務

如需中提供的範例一致性套件的完整清單 AWS Config，請參閱開發人員指南中的一致性套件範例範本。AWS Config

使用 AWS SDK 記錄資料事件

執行GetEventSelectors作業以查看追蹤是否正在記錄資料事件。您可以透過執行作業來設定追蹤記錄資料事PutEventSelectors件。如需詳細資訊，請參閱 AWS CloudTrail API 參考。

執行GetEventDataStore作業以查看您的事件資料存放區是否正在記錄資料事件。您可以透過執行CreateEventDataStore或UpdateEventDataStore作業並指定進階事件選取器，將事件資料存放區設定為包含資料事件。如需詳細資訊，請參閱建立、更新和管理事件資料存放區 AWS CLI和 AWS CloudTrail API 參考。

將事件傳送到 Amazon CloudWatch 日誌

CloudTrail 支援將資料事件傳送至 CloudWatch 記錄檔。當您將追蹤設定為將事件傳送至 CloudWatch 記錄檔記錄群組時，只 CloudTrail 會傳送您在追蹤中指定的事件。例如，如果您將追蹤設定為僅記錄資料事件，則追蹤只會將資料事件傳送至您的 CloudWatch 記錄檔記錄群組。如需更多詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。

記錄 Insights 事件

AWS CloudTrail 透過持續分析 CloudTrail 管理事件，深入解析可協助 AWS 使用者識別並回應與 API 呼叫和 API 錯誤率相關的異常活動。 CloudTrail Insights 會分析您的 API 呼叫量和 API 錯誤率 (也稱為基準) 的正常模式，並在呼叫量或錯誤率超出正常模式時產生 Insights 事件。其會針對 `write` 管理 API 產生 API 呼叫量的 Insights 事件，並針對 `read` 和 `write` 管理 API 產生 API 錯誤率的 Insights 事件。

> **Note**
>
> 若要在 API 呼叫量上記錄 Insights 事件，追蹤或事件資料存放區必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，追蹤或事件資料存放區必須記錄 `read` 或 `write` 管理事件。

CloudTrail Insights 會分析單一區域 (而非全球) 中發生的管理事件。In CloudTrail sights 事件會在與產生其支援管理事件的相同區域中產生。

Insights 事件會產生額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需詳細資訊，請參閱 AWS CloudTrail 定價。

內容

了解 Insights 事件傳遞

與其他 CloudTrail 擷取的事件類型不同，Insights 事件只有在 CloudTrail 偵測到帳戶 API 使用情況的變更 (與帳戶的典型使用模式明顯不同) 時，才會記錄 Insights 事件。

追蹤和事件資料存放區之間 CloudTrail 傳送事件的位置以及接收 Insights 事件所需的時間不同。

追蹤的 Insights 事件傳遞

如果您已在追蹤上啟用 Insights 事件並 CloudTrail 偵測到異常活動，請將 Insights 事件 CloudTrail 傳遞至所選目標 S3 儲存貯體中的`/CloudTrail-Insight`資料夾以供追蹤使用。在追蹤上首次啟用「 CloudTrail 深入解析」之後，如果偵測到異常活動，最多可能需 CloudTrail 要 36 小時才能傳遞第一個「見解」事件。

如果您關閉追蹤上的 Insights 事件記錄，然後重新啟用 Insights 事件，或者停止並重新啟動追蹤記錄，如果偵測到異常活動，則重新啟動 Insights 事件最多可能需 CloudTrail 要 36 小時才能重新傳遞。

事件資料存放區的 Insights 事件傳遞

如果您已在來源事件資料存放區上啟用 Insights 事件，則會將 Insights 事件 CloudTrail 傳遞至目的地事件資料存放區。在來源事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能將第一個 Insights 事件傳送至目的地事件資料存放區。

如果您關閉來源事件資料存放區上的 Insights 事件記錄，然後重新啟用 Insights 事件，或停止並重新啟動來源事件資料存放區上的事件擷取，如果偵測到異常活動，則重新啟動 Insights 事件的傳送最多可能需 CloudTrail 要 7 天。在 CloudTrail 湖泊擷取見解事件需要支付額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需 CloudTrail 定價的相關資訊，請參閱AWS CloudTrail 定價。

記錄見解事件 AWS Management Console

您可以使用主控台，在追蹤或事件資料存放區上啟用 Insights 事件。

主題

- 在現有追蹤上啟用 CloudTrail 見解事件
- 在現有事件資料存放區上啟用 CloudTrail 見解事件

在現有追蹤上啟用 CloudTrail 見解事件

使用下列程序來啟用現有追蹤上的 CloudTrail 深入解析事件。預設情況下，不會啟用 Insights 事件。

1. 在 CloudTrail 主控台的左側導覽窗格中，開啟「追蹤」頁面，然後選擇追蹤名稱。
2. 在 Insights 事件中，選擇 Edit (編輯)。

   > **Note**
   >
   > 記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱AWS CloudTrail 定價。

3. 在 Event type (事件類型) 中，選擇 Insights events (Insights 事件)。
4. 在 Insights events (Insights 事件) 中的 Choose Insights types (選擇 Insights 類型) 下，選擇 API call rate (API 呼叫率) 或 API error rate (API 錯誤率) (或兩者)。您的追蹤必須記錄寫入管理事件，以記錄 API 呼叫率的 Insights 事件。您的追蹤必須記錄讀取或寫入管理事件，以便記錄 API 錯誤率的 Insights 事件。

5. 選擇儲存變更，以儲存您所做的變更。

如果偵測到異常活動，最多可能需 CloudTrail 要 36 小時才能傳遞第一個 Insights 事件。

在現有事件資料存放區上啟用 CloudTrail 見解事件

使用下列程序可在現有事件資料存放區上啟用 CloudTrail Insights 事件。預設情況下，不會啟用 Insights 事件。

在 CloudTrail 湖泊擷取見解事件需要支付額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需 CloudTrail 定價的相關資訊，請參閱AWS CloudTrail 定價。

> **Note**
>
> 您只能在包含 CloudTrail 管理事件的事件資料存放區上啟用 CloudTrail Insights 事件。您無法在其他事件資料存放區類型上啟用 CloudTrail Insights 事件。

1. 在 CloudTrail 主控台左側導覽窗格的 [Lake] 下，選擇 [事件資料存放區]。
2. 選擇事件資料存放區名稱。
3. 在管理事件中，選擇編輯。
4. 選擇啟用 Insights。
5. 選擇 CloudTrail 將提供見解事件的目的地事件資料存放區。目的地事件資料存放區將依據此事件資料存放區中的管理事件活動收集 Insights 事件。如需有關如何建立目的地事件資料存放區的資訊，請參閱 若要建立會記錄 Insights 事件的目的地事件資料存放區。
6. 在選擇 Insights 類型下方，選擇 API 呼叫率、API 錯誤率，或兩者。您的事件資料存放區必須記錄寫入管理事件，以便為 API 呼叫率記錄 Insights 事件。您的事件資料存放區必須記錄讀取或寫入管理事件，以便為 API 錯誤率記錄 Insights 事件。
7. 選擇儲存變更，以儲存您所做的變更。

如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能傳遞第一個 Insights 事件。

記錄見解事件 AWS Command Line Interface

您可以使用 AWS CLI設定您的追蹤和事件資料存放區，以記錄 Insights 事件。

> **Note**
>
> 若要在 API 呼叫量上記錄 Insights 事件，追蹤或事件資料存放區必須記錄 `write` 管理事件。若要在 API 錯誤率上記錄 Insights 事件，追蹤或事件資料存放區必須記錄 `read` 或 `write` 管理事件。

主題

- 記錄使用的追蹤的見解事件 AWS CLI
- 記錄事件資料存放區的見解事件使用 AWS CLI

記錄使用的追蹤的見解事件 AWS CLI

若要檢視您的追蹤是否記錄 Insights 事件，請執行 `get-insight-selectors` 命令。

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

以下結果展示追蹤的預設設定。依預設，追蹤不會記錄 Insights 事件。`InsightType` 屬性值是空的，且未指定 Insight 事件選取器，因為未啟用 Insights 事件收集。

如果您未新增 Insights 選取器，get-insight-selectors命令會傳回下列錯誤訊息：「呼叫 GetInsightSelectors 作業時發生錯誤 (InsightNotEnabledException)：追蹤##未啟用 Insights。Edit the trail settings to enable Insights, and then try the operation again." (呼叫 GetInsightSelectors 操作時，發生錯誤 (InsightNotEnabledException)：追蹤名稱未啟用 Insights。編輯追蹤設定以啟用 Insights，然後再試一次操作。)

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

若要設定您的追蹤記錄 Insights 事件，請執行 `put-insight-selectors` 命令。下面的範例顯示如何設定追蹤以包含 Insights 事件。Insights 選取器值可以是 `ApiCallRateInsight` 或 `ApiErrorRateInsight` (或兩者)。

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

下列結果顯示針對追蹤設定的 Insights 事件選取器。

```
{
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

記錄事件資料存放區的見解事件使用 AWS CLI

若要在事件資料存放區上啟用 Insights 事件，您需要擁有會記錄管理事件的來源事件資料存放區和會記錄 Insights 事件的目的地事件資料存放區。

若要檢視是否在事件資料存放區上啟用 Insights 事件，請執行 get-insight-selectors 命令。

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

若要檢視事件資料存放區是否設定為接收 Insights 事件或管理事件，請執行 get-event-data-store 命令。

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

以下程序將向您說明如何建立目的地和來源事件資料存放區，然後啟用 Insights 事件。

1. 執行 aws cloudtrail create-event-data-store 命令來建立會收集 Insights 事件的目的地事件資料存放區。`eventCategory` 的值必須為 `Insight`。取代*`retention-period-days`*為您希望在事件資料存放區中保留事件的天數。

   如果您使用 AWS Organizations 組織的管理帳戶登入，如果您想要授予委派管理員對事件資料存放區的存取權，請包含`--organization-enabled`參數。

   ```
   aws cloudtrail create-event-data-store \
   ```

```
--name insights-event-data-store \
--no-multi-region-enabled \
--retention-period retention-period-days \
--advanced-event-selectors '[
    {
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

以下是回應範例。

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

您將使用來自回應的 ARN (或 ARN 的 ID 尾碼)，作為步驟 3 中 `--insights-destination` 參數的值。

2. 執行 aws cloudtrail create-event-data-store 命令以建立記錄管理事件的來源事件資料存放區。依預設，事件資料存放區會記錄所有管理事件。如果想要記錄所有管理事件，您不需要指定進階事件選取器。取代*retention-period-days*為您希望在事件資料存放區中保留事件的天數。若您要建立組織事件資料存放區，請加入 `--organization-enabled` 參數。

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

您將使用來自回應的 ARN (或 ARN 的 ID 尾碼)，作為步驟 3 中 `--event-data-store` 參數的值。

3. 執行 put-insight-selectors 命令以啟用 Insights 事件。Insights 選取器值可以是 `ApiCallRateInsight` 或 `ApiErrorRateInsight` (或兩者)。對於 `--event-data-store` 參數，指定來源事件資料存放區的 ARN (或 ARN 的 ID 尾碼)，該存放區會記錄管理事件並且將啟用 Insights。對於 `--insights-destination` 參數，指定目的地事件資料存放區的 ARN (或 ARN 的 ID 尾碼)，該存放區將會記錄 Insights 事件。

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

下列結果顯示針對事件資料存放區設定的 Insights 事件選取器。

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

在事件資料存放區首次啟用 CloudTrail Insights 之後，如果偵測到異常活動，最多可能需 CloudTrail 要 7 天的時間才能傳遞第一個 Insights 事件。

CloudTrail Insights 會分析單一區域 (而非全球) 中發生的管理事件。In CloudTrail sights 事件會在與產生其支援管理事件的相同區域中產生。

對於組織事件資料存放區，分 CloudTrail 析來自每個成員帳戶的管理事件，而不是分析組織所有管理事件的彙總。

在 CloudTrail 湖泊擷取見解事件需要支付額外費用。如果您同時為追蹤和事件資料存放區啟用 Insights，則將分別支付它們的費用。如需 CloudTrail 定價的相關資訊，請參閱AWS CloudTrail 定價。

使用 AWS SDK 記錄事件

執行GetInsightSelectors作業以查看追蹤或事件資料存放區是否啟用 Insights 事件。您可以設定追蹤或事件資料存放區，以便透過PutInsightSelectors作業啟用 Insights 事件。如需詳細資訊，請參閱 AWS CloudTrail API 參考。

追蹤的其他資訊

本節將提供特定於追蹤的其他資訊。本節說明如何從 CloudTrail 主控台的 [見解] 頁面檢視已訂閱追蹤的事件，以及如何選擇性地將這些事件傳送至 CloudWatch 記錄檔以進行監視。

主題

- 在主控台中檢視追蹤的 Insights 事件
- 將追蹤事件傳送至 Amazon CloudWatch 日誌

在主控台中檢視追蹤的 Insights 事件

對於追蹤，您也可以在 CloudTrail 主控台的「見解」頁面上存取和檢視「深入解析」事件。如需如何在主控台中以及使用存取和檢視 Insights 事件的詳細資訊 AWS CLI，請參閱本指南檢視追蹤的 CloudTrail 見解事件中的。

以下圖片顯示了追蹤的 Insights 事件的範例。您可以從 Dashboard (儀表板) 或 Insights (深入分析) 頁面選擇 Insights 事件名稱，以開啟 Insights 事件的詳細資訊頁面。

如果您停用追蹤上的 CloudTrail 深入解析，或停止追蹤記錄 (停用 CloudTrail Insights)，您可能會在目的地 S3 儲存貯體中存放 Insights 事件，或顯示在主控台的「見解」頁面上 (自您先前啟用了 Insights) 開始的那一天。

篩選欄

左邊欄列出與主旨 API 相關，並具有相同的 Insights 事件類型的 Insights 事件。此欄可讓您選擇想要更多資訊的 Insights 事件。當您在此欄中選擇事件時，事件會在 Insights 圖表索引標籤突出顯示。根據

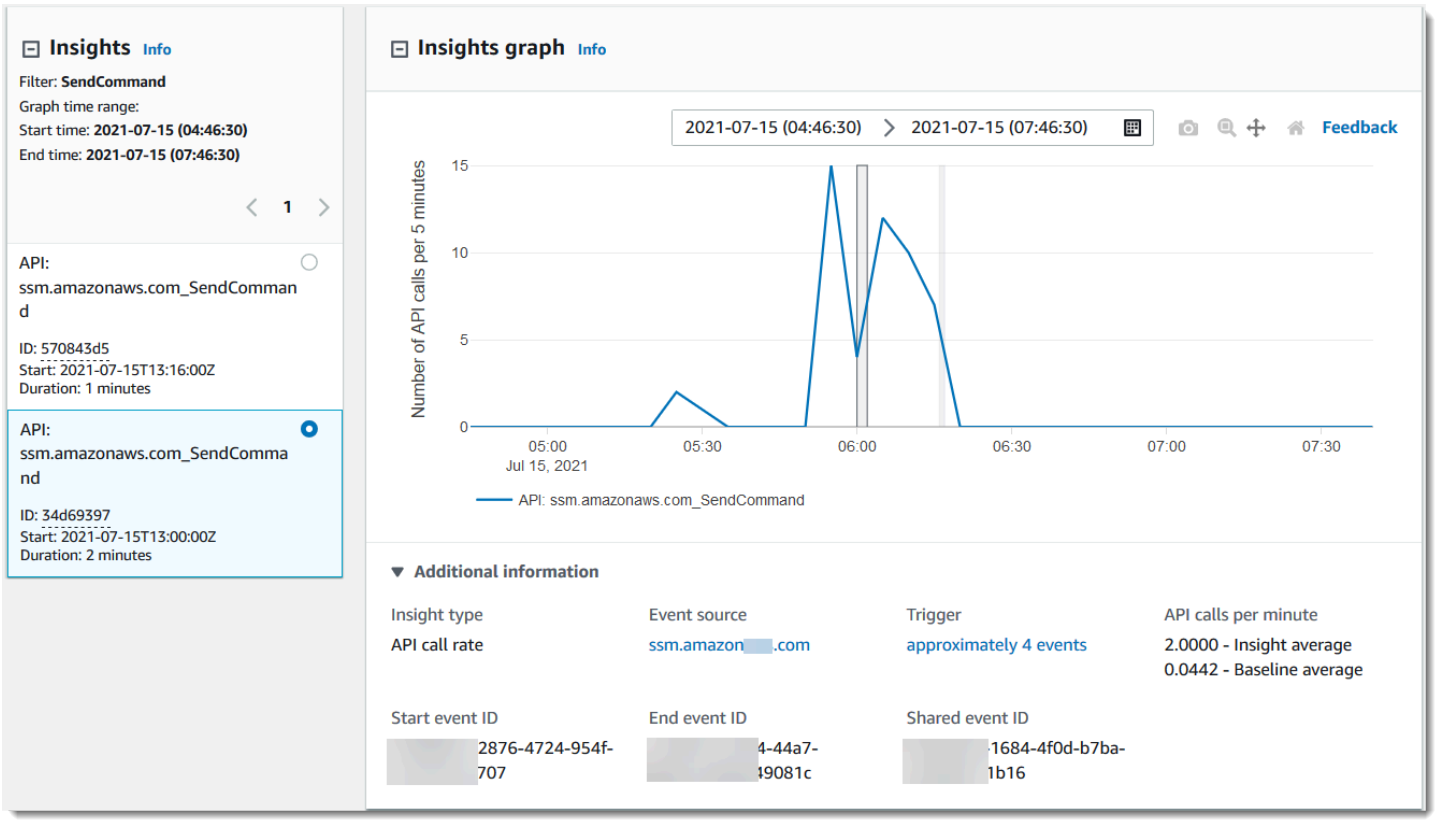
預設，會 CloudTrail 套用篩選器，將事件索引標籤上顯示的CloudTrail事件限制在觸發 Insights 事件的異常活動期間呼叫的特定 API 相關事件。若要顯示在異常活動期間呼叫的所有 CloudTrail事件，包括與「見解」事件無關的事件，請關閉篩選器。

Insights 圖表索引標籤

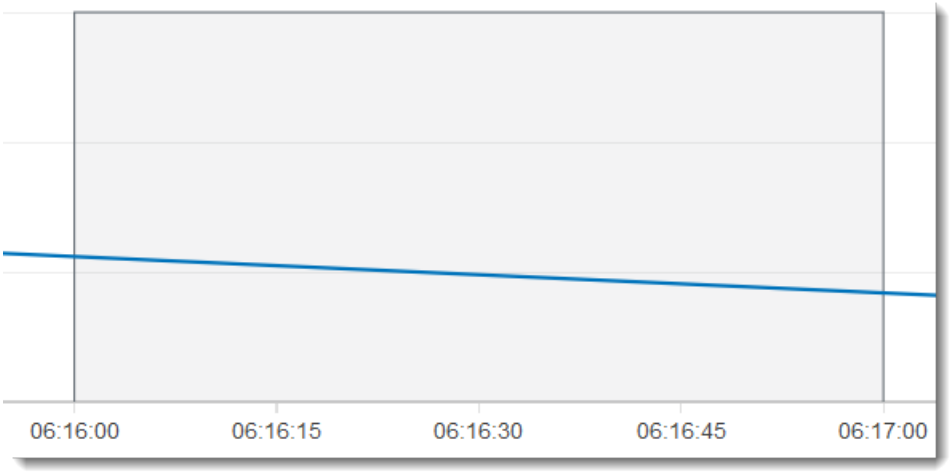
在 Insights graph (Insights 圖表) 索引標籤上，Insights 事件的詳細資訊頁面會顯示在記錄一或多個 Insights 事件之前和之後的一段時間內，所發生 API 呼叫量或錯誤率的圖形。在圖表中，會以垂直長條圖強調顯示 Insights 事件，並以長條圖寬度顯示 Insights 事件的開始和結束時間。

在此範例中，垂直反白顯示區段會顯示帳戶中不尋常的 AWS Systems Manager SendCommand API 呼叫數目。在反白顯示的區域中，由於SendCommand通話數量超過帳戶每分鐘 0.0442 個呼叫的基準平均值，因此在偵測到異常活動時 CloudTrail 記錄了 Insights 事件。根據 Insights 事件記錄，在凌晨 5:50 到 5:55 之間的五分鐘內，進行了多達 15 次的 SendCommand 呼叫。這比帳戶的每分鐘預期值多出兩次 API 呼叫。在此範例中，圖表的時間範圍是三小時：凌晨 4:30。2021 年 7 月 15 日至上午 7:30，太平洋夏令時間。2021 年 7 月 15 日，太平洋夏令時間。此事件的開始時間為早上 6:00。2021 年 7 月 15 日，太平洋夏令時間，結束時間為兩分鐘後。結束的 Insights 事件 (未反白顯示) 顯示異常活動在上午 6:16 左右結束。

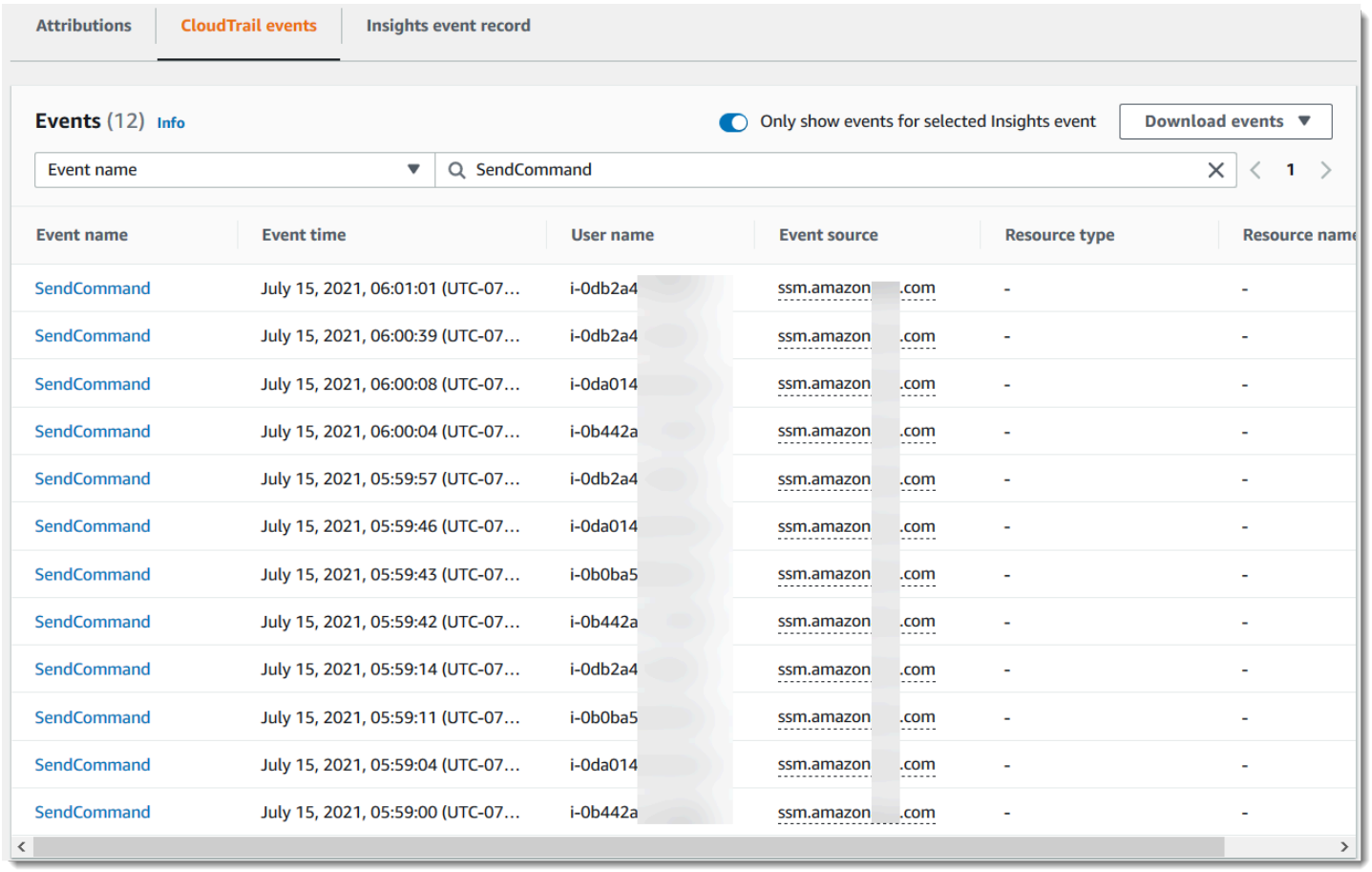
基準是在 Insights 事件開始前七天內計算。雖然基準持續時間 (CloudTrail 分析 API 上正常活動的期間) 的值大約為 7 天，但將基準持續時間 CloudTrail 捨入為整數天，以便精確的基準持續時間可能會有所不同。



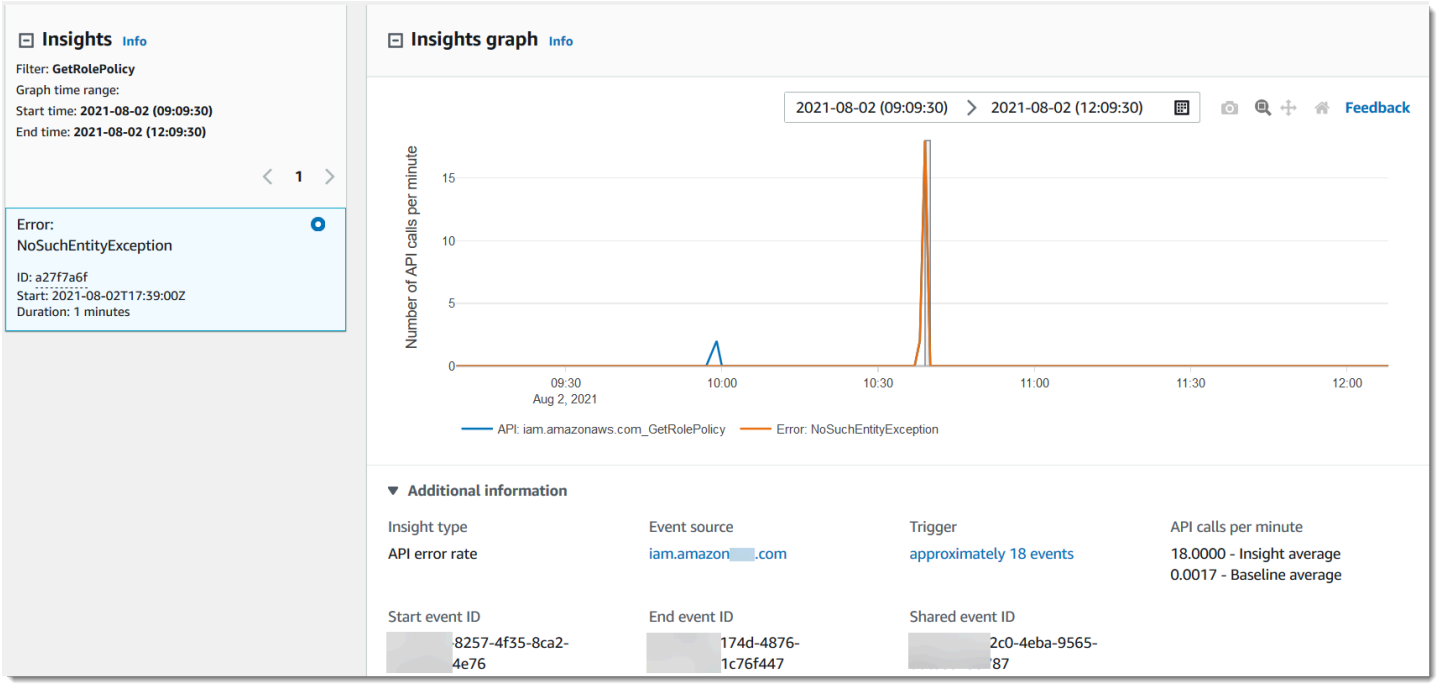
您可以使用工具列上的 Zoom (放大) 命令來放大結束的 Insights 事件，並顯示開始和結束時間。在此範例中，選擇 Zoom (放大)，然後拖曳 Zoom (放大) 游標放在反白顯示的 Insights 事件的一個邊緣上，會展開 Insights 事件並顯示更多時間表詳細資訊。



若要檢視 CloudTrail 已分析以判斷異常活動的事件，請開啟CloudTrail 事件索引標籤。在此範例中，CloudTrail 分析了 12 個事件，其中四個觸發見解事件。

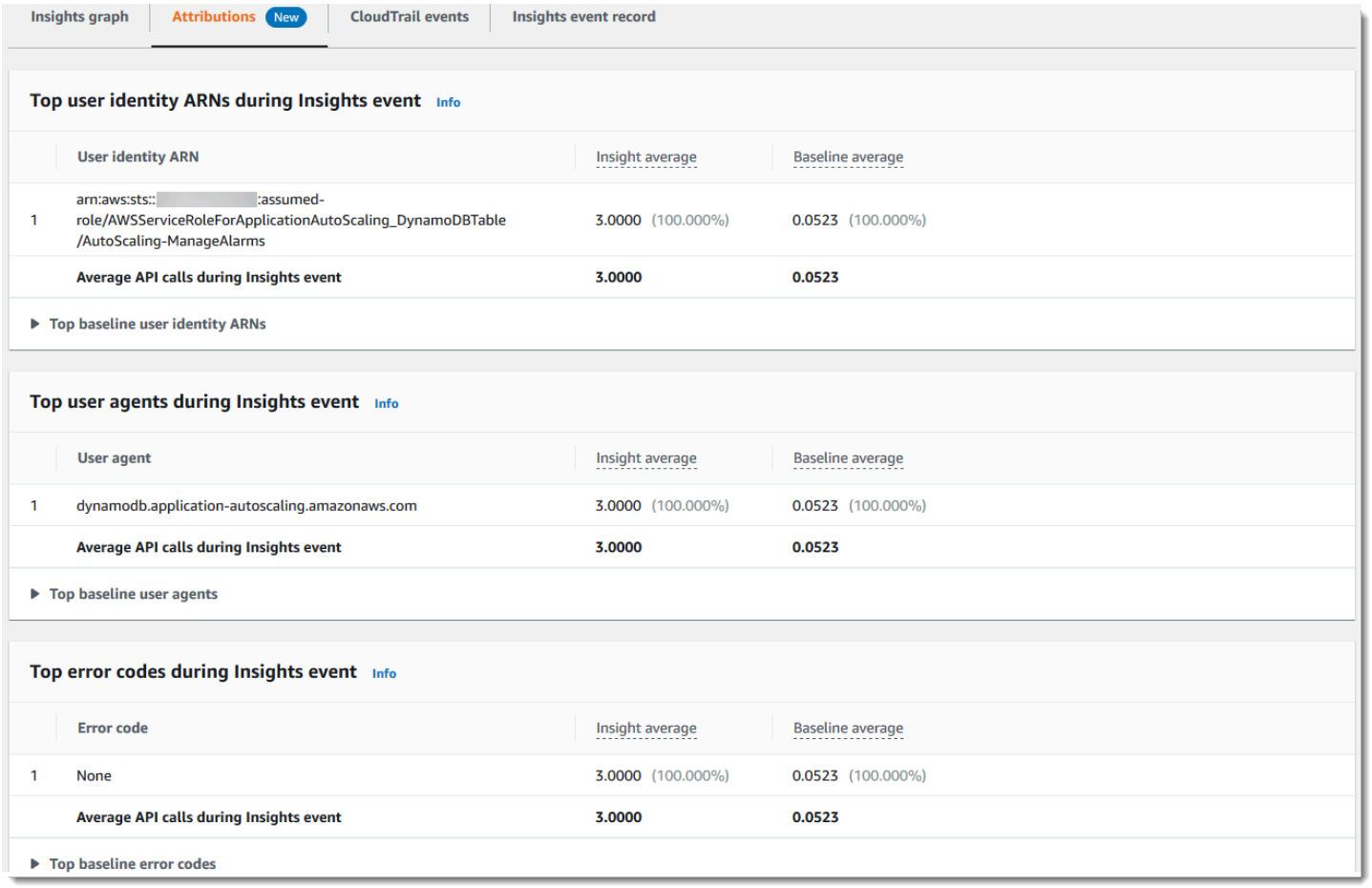


下列圖片顯示了 API 錯誤率 Insights 事件的 Insights 圖表索引標籤。反白顯示的區域顯示記錄了 Insights 事件，因為 `GetRolePolicy` IAM API 呼叫的 `NoSuchEntityException` 錯誤發生率高於此 API 呼叫每分鐘 0.0017 個 `NoSuchEntityException` 錯誤的基準平均值，在 Insights 期間平均每分鐘 18 個錯誤。在此範例中，觸發「見解」 CloudTrail 事件的事件數目符合「深入解析」平均值在一分鐘內發`NoSuchEntityException`生 18 個錯誤。與 API 呼叫率圖表不同，API 錯誤率會以對比色彩顯示兩條線：一條 (`GetRolePolicy`) 測量對 IAM API 的呼叫，這些呼叫導致了不尋常的錯誤數量，另一條 (`NoSuchEntityException`) 則測量記錄異常活動的錯誤。

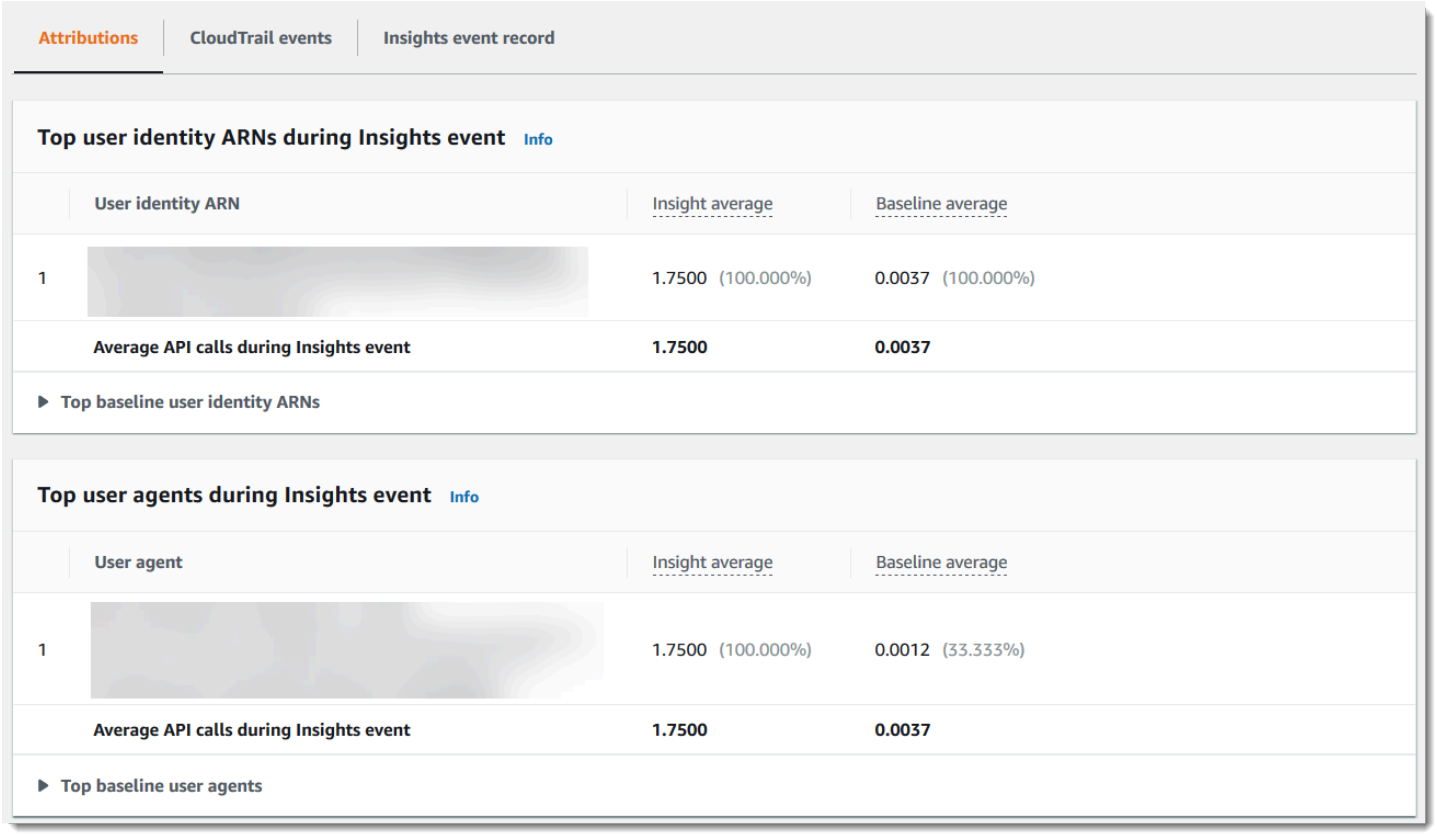


Attributions (歸因) 索引標籤

Attributions (歸因) 索引標籤顯示 Insights 事件的下列資訊。關於 Attributions (歸因) 索引標籤的資訊可協助您找出 Insights 活動的原因和來源。展開主要基準區域，以將正常期間的使用者身分、使用者代理程式和錯誤代碼活動，與 Insights 活動期間歸因的活動進行比較。在 Top baseline user identity ARNs (主要基準使用者身分 ARN)、Top baseline user agents (主要基準使用者代理程式) 及 Top baseline error codes (主要基準錯誤代碼) 中，僅會顯示基準平均值 — Insights 事件開始時間前約七天內，由使用者身分、使用者代理程式記錄或導致錯誤代碼的 API 事件歷史平均值。



Attributions (歸因) 索引標籤只會顯示錯誤率 Insight 事件的主要使用者身分 ARN 和主要使用者代理程式，如下圖所示。錯誤率 Insights 事件不需要主要錯誤代碼。



- 熱門使用者身分 ARN-此表格顯示在異常活動和基準期間促成 API 呼叫的前五名使 AWS 用者或 IAM 角色 (使用者身分)，依所貢獻的 API 呼叫平均數降序排列。括號中顯示了作為促成異常活動的活動總數的平均值百分比。如果超過五個使用者身分 ARN 造成異常活動，則其活動總結在 Other (其他) 資料列。
- 熱門使用者代理程式-此表格顯示在異常活動和基準期間，使用者身分對 API 呼叫做出貢獻的前五個 AWS 工具，依所貢獻的 API 呼叫平均數量遞減順序排列。這些工具包括 AWS Management Console AWS CLI、或 AWS SDK。例如，名為 `ec2.amazonaws.com` 表示 Amazon EC2 主控台是用來呼叫 API 的工具之一。括號中顯示了作為促成異常活動的活動總數的平均值百分比。如果超過五個使用者代理程式對異常活動做出貢獻，他們的活動總結在 Other (其他) 資料列。
- Top error codes (主要錯誤代碼) - 僅針對 API call rate (API 呼叫率) Insights 事件顯示。此表格最多顯示在異常活動和基準期間 API 呼叫上發生的前五個錯誤代碼，按從 API 呼叫次數最多到最少的降序排列。括號中顯示了作為促成異常活動的活動總數的平均值百分比。如果在異常或基準活動期間發生超過五個錯誤碼，其活動會彙總在 Other (其他) 資料列。

  值為 None 做為前五個錯誤碼值的其中一個，表示造成 Insights 事件的呼叫中有很大百分比不會導致錯誤。如果錯誤碼值為 None，而且資料表中沒有其他錯誤碼，則 Insights 平均值和基準平均值欄中的值與 Insights 事件整體的值相同。您也可以查看 Insights 圖表索引標籤上每分鐘 API 呼叫次數下 Insights 平均值和基準平均值圖例中顯示的這些值。

基準平均值和 Insights 平均值

Baseline average (基準平均值) 和 Insights average (Insights 平均值) 針對主要使用者身分、主要使用者代理程式和主要錯誤代碼顯示。

- Baseline average (基準平均值) - 記錄 Insights 事件的 API 的每分鐘典型發生率 (大約前 7 天內在您帳戶的特定區域中測量)。
- Insights average (Insights 平均值) - 觸發 Insights 事件的此 API 的呼叫率或錯誤率。開始事件的「 CloudTrail 見解」平均值是指觸發見解事件之 API 上每分鐘的呼叫率或錯誤數。通常情況下，這是異常活動的第一分鐘。結束事件的 Insights 平均值是在異常活動持續期間 (開始 Insights 事件和結束 Insights 事件之間)，每分鐘 API 呼叫率或錯誤率。

CloudTrail 事件標籤

在CloudTrail 事件索引標籤上，檢視 CloudTrail分析的相關事件，以判斷發生異常活動。依預設，Insights 事件名稱已套用篩選器，這也是相關 API 的名稱。若要顯示異常活動期間所 CloudTrail 記錄的所有事件，請關閉「僅顯示所選深入解析」事件的事件。CloudTrail 事件索引標籤會顯示 CloudTrail 與 Insights 事件的開始和結束時間之間發生的主旨 API 相關的管理事件。這些事件可協助您執行更深入的分析，以判斷 Insights 事件的可能原因，以及異常 API 和錯誤率活動的原因。

Insights 事件記錄索引標籤

就像任何 CloudTrail 事件一樣， CloudTrail 見解事件是 JSON 格式的記錄。Insights 事件記錄索引標籤會顯示 Insights 開始和結束事件的 JSON 結構和內容，有時稱為事件酬載。如需 Insights 事件記錄的欄位和內容，請參閱本指南中的 Insights 事件記錄欄位 和 CloudTrail 見解`insightDetails`元素。

將追蹤事件傳送至 Amazon CloudWatch 日誌

CloudTrail 支援將追蹤的見解事件傳送至 CloudWatch 記錄檔。當您將追蹤設定為將 Insights 事件傳送至 CloudWatch 記錄檔記錄群組時， CloudTrail Insights 只會傳送您在追蹤中指定的事件。例如，如果您將追蹤設定為記錄管理和 Insights 事件，您的追蹤就會將管理和 Insights 事件傳遞給您的 CloudWatch 記錄日誌記錄群組。如需更多詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。

CloudTrail 記錄內容

記錄主體所包含的欄位可協助您判斷請求的動作，以及提出請求的時機和位置。Optional (選用) 的值為 True 時，欄位只有在套用至服務、API 或事件類型時才會出現。選用值 False 表示欄位永遠存在，

或其存在不依賴服務、API 或事件類型。範例為 `responseElements`，其存在於進行變更的動作 (建立、更新或刪除動作) 事件中。

CloudTrail 如果欄位的內容超過欄位大小上限，則會截斷欄位。如果截斷欄位，`omitted` 存在的值為 `true`。

`eventTime`

完成請求的日期和時間 (國際標準時間 (UTC))。事件的時間戳記來自本機主機，該主機提供 API 呼叫所在的服務 API 端點。例如，在美國西部 (奧勒岡) 區域執行的 CreateBucket API 事件會從執行 Amazon S3 端點的 AWS 主機上取得其時間戳記`s3.us-west-2.amazonaws.com`。一般而言，AWS 服務會使用網路時間通訊協定 (NTP) 來同步其系統時鐘。

來自：1.0

選用：False

`eventVersion`

日誌事件格式的版本。目前的版本是 1.10。

`eventVersion` 值是主要和次要版本，格式為 *`major_version`*.*`minor_version`*。例如，您可以有一個值為 `1.09` 的 `eventVersion`，其中 `1` 是主要版本，`09` 是次要版本。

CloudTrail 如果對不向後相容的事件結構進行變更，則會增加主要版本。這包括移除已存在的 JSON 欄位，或變更欄位內容的表示方式 (例如，日期格式)。 CloudTrail 如果變更將新欄位新增至事件結構，則會增加次要版本。如果為某些或所有現有事件提供新資訊，或只有新事件類型才提供新資訊，就可能會發生這種情況。應用程式應略過新欄位，以與新次要版本的事件結構維持相容。

如果 CloudTrail 引入了新的事件類型，但事件的結構未改變，則事件版本不會改變。

為確保您的應用程式可以剖析事件結構，我們建議您對主要版本編號執行「等於」比較。為了確保您的應用程式預期的欄位存在，我們也建議您對次要版本執行 greater-than-or-equal-To 比較。次要版本中沒有前導零。您可以將 *`major_version`* 和 *`minor_version`* 解釋為數字，並執行比較操作。

來自：1.0

選用：False

`userIdentity`

有關提出請求之 IAM 身分的資訊。如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

來自：1.0

選用：False

eventSource

要請求的服務。此名稱通常是較短形式的服務名稱，即沒有空格再加上 .amazonaws.com。例如：

- AWS CloudFormation 是cloudformation.amazonaws.com。
- Amazon EC2 是 ec2.amazonaws.com。
- Amazon Simple Workflow Service 為 swf.amazonaws.com。

此慣例有一些例外狀況。例如，對eventSource於 Amazon CloudWatch 是monitoring.amazonaws.com.

來自：1.0

選用：False

eventName

請求的動作，這是該服務中之 API 的其中一個動作。

來自：1.0

選用：False

awsRegion

提 AWS 區域 出要求的對象，例如us-east-2。請參閱CloudTrail 支援的地區。

來自：1.0

選用：False

sourceIPAddress

提出請求的 IP 地址。對於源自服務主控台的動作，所報告的地址適用於基礎客戶資源，而非主控台 Web 伺服器。對於中的服務 AWS，只會顯示 DNS 名稱。

> **Note**
>
> 對於源自 AWS的事件，此欄位通常是 `AWS Internal/#`，其中 `#` 是用於內部用途的號碼。

來自：1.0

選用：False

`userAgent`

透過其發出要求的代理程式 AWS Management Console，例如 AWS 服務、 AWS SDK 或. AWS CLI此欄位的大小上限為 1 KB；超過該限制的內容會被截斷。範例值如下：

- `lambda.amazonaws.com` - 使用 AWS Lambda提出請求。
- `aws-sdk-java` - 使用 AWS SDK for Java提出請求。
- `aws-sdk-ruby` - 使用 AWS SDK for Ruby提出請求。
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— 請求是在 Linux 上 AWS CLI 安裝的情況下提出的。

> **Note**
>
> 對於起源的事件 AWS，如果 CloudTrail 知道是哪一個 AWS 服務 進行呼叫，此欄位就是呼叫服務的事件來源 (例如`ec2.amazonaws.com`)。否則，此欄位為`AWS Internal/#`，其中`#`是用於內部用途的數字。

來自：1.0

選用：True

`errorCode`

如果請求返回錯誤，則 AWS 服務錯誤。如需顯示此欄位的範例，請參閱 錯誤代碼和訊息日誌範例。此欄位的大小上限為 1 KB；超過該限制的內容會被截斷。

來自：1.0

選用：True

errorMessage

如果請求傳回錯誤，則會是該錯誤的描述。此訊息包含授權失敗的訊息。 CloudTrail 會擷取服務在其例外狀況處理中記錄的訊息。如需範例，請參閱錯誤代碼和訊息日誌範例。此欄位的大小上限為 1 KB；超過該限制的內容會被截斷。

> **Note**
>
> 某些 AWS 服務會在事件中提供`errorCode`和`errorMessage`做為頂層欄位。其他 AWS 服務在 `responseElements` 的部分提供錯誤資訊。

來自：1.0

選用：True

requestParameters

請求時所傳送的參數 (如果有的話)。這些參數記錄在適當 AWS 服務的 API 參考文件中。此欄位的大小上限為 100 KB；超過該限制的內容會被截斷。

來自：1.0

選用：False

responseElements

進行變更（建立、更新或刪除動作）的回應元素（如果有）。如果動作 不返回響應元素，此字段是`null`。如果 動作不會變更狀態 (例如，取得或列出物件的要求)、 這個元素被省略。動作的回應元素會記錄在 API 參考資料中 適當的文檔 AWS 服務。此欄位的大小上限 100 KB；超過該限制的內容會被截斷。

該`responseElements`值對於幫助您跟踪請求很有用 與 AWS Support. 兩者`x-amz-request-id`和 `x-amz-id-2` 包含可協助您追蹤要求的資訊 AWS Support。這些值是 與服務在響應請求時返回的內容相同 啟動事件，以便您可以使用它們將事件與 請求。

來自：1.0

選用：False

additionalEventData

不屬於請求或回應之事件的額外資料。此欄位的大小上限為 28 KB；超過該限制的內容會被截斷。

來自：1.0

選用：True

requestID

識別請求的值。所呼叫的服務會產生此值。此欄位的大小上限為 1 KB；超過該限制的內容會被截斷。

來自：1.01

選用：True

eventID

由產生的 GUID CloudTrail 以唯一識別每個事件。您可以使用這個值來識別單一事件。例如，您可以使用此 ID 做為主索引鍵，從可搜尋的資料庫中擷取日誌資料。

來自：1.01

選用：False

eventType

識別已產生事件記錄的事件類型。這可以是下列其中一個值：

- `AwsApiCall` - 呼叫 API。
- `AwsServiceEvent` - 服務產生與您追蹤相關的事件。例如，這可能會在另一個帳戶對您擁有的資源進行呼叫時發生。
- `AwsConsoleAction`- 在主控台中採取的動作不是 API 呼叫。
- `AwsConsoleSignIn`— 您帳戶中的使用者 (根、IAM、同盟、SAML 或 SwitchRole) 登入. AWS Management Console

- AwsCloudTrailInsight— 如果啟用了 Insights 事件，則 CloudTrail 會在 CloudTrail 偵測到異常操作活動 (例如資源佈建中的峰值或 AWS Identity and Access Management (IAM) 動作爆發時產生見解事件。

  AwsCloudTrailInsight 事件不使用以下欄位：

  - eventName
  - eventSource
  - sourceIPAddress
  - userAgent
  - userIdentity

來自：1.02

選用：False

apiVersion

識別與 AwsApiCall eventType 值相關聯的 API 版本。

來自：1.01

選用：True

managementEvent

可識別事件是否為管理事件的布林值。若 eventVersion 為 1.06 或更新版本，且事件類型為下列其中一項，則 managementEvent 會顯示在事件記錄中：

- AwsApiCall
- AwsConsoleAction
- AwsConsoleSignIn
- AwsServiceEvent

來自：1.06

選用：True

readOnly

識別此操作是否為唯讀操作。這可以是下列其中一個值：

- `true` - 此操作是唯讀的 (例如，`DescribeTrails`)。
- `false` - 此操作是唯寫的 (例如，`DeleteTrail`)。

來自：1.01

選用：True

resources

事件中存取之資源的清單。欄位可能包含下列資訊：

- 資源 ARN
- 資源擁有者的帳戶 ID
- 資源類型識別符，格式為：`AWS::aws-service-name::data-type-name`

例如，記錄 `AssumeRole` 事件時，`resources` 欄位可能顯示如下：

- ARN：`arn:aws:iam::123456789012:role/myRole`
- 帳戶 ID：`123456789012`
- 資源類型識別符：`AWS::IAM::Role`

如需具有`resources`欄位的記錄範例，請參閱 IAM 使用指南中的記 CloudTrail 錄檔中的AWS STSAWS KMS API 事件或AWS Key Management Service 開發人員指南中的記錄 API 呼叫。

來自：1.01

選用：True

recipientAccountId

代表收到此事件的帳戶 ID。`recipientAccountID` 可能與 CloudTrail userIdentity 元素 `accountId` 不同。這可能發生在跨帳戶資源存取中。例如，如果個別帳戶使用 KMS 金鑰 (也稱為 AWS KMS key) 呼叫加密 API，則對於交付至提出呼叫之帳戶的事件，`accountId` 和 `recipientAccountID` 值會相同，但對於交付至擁有 KMS 金鑰之帳戶的事件，這些值就會不同。

來自：1.02

選用：True

`serviceEventDetails`

識別服務事件，包含觸發事件的項目和結果。如需詳細資訊，請參閱 AWS 服務事件。此欄位的大小上限為 100 KB；超過該限制的內容會被截斷。

來自：1.05

選用：True

`sharedEventID`

由所產生的 GUID， CloudTrail 以唯一識別傳送至不同 AWS 帳戶的相同 AWS 動作中的 CloudTrail 事件。

例如，當帳戶使用屬於其他帳戶AWS KMS key的帳戶時，使用 KMS 金鑰的帳戶和擁有 KMS 金鑰的帳戶會針對相同動作收到個別 CloudTrail 事件。為此 AWS 動作傳送的每個 CloudTrail 事件都共用相同`sharedEventID`，但也有一個唯一的`eventID`和`recipientAccountID`。

如需詳細資訊，請參閱 sharedEventID 範例。

> **Note**
>
> 僅當 CloudTrail 事件傳遞至多個帳戶時，此`sharedEventID`欄位才會顯示。如果呼叫者和所有者是相同的 AWS 帳戶，則僅 CloudTrail 發送一個事件，而該`sharedEventID`字段不存在。

來自：1.03

選用：True

`vpcEndpointId`

識別從 VPC 向另一個 AWS 服務提出請求的 VPC 端點 (例如 Amazon S3)。

來自：1.04

選用：True

eventCategory

顯示事件類別。用eventCategory於管理和見解事件的LookupEvents呼叫。

- 對於管理事件，值為 Management。
- 對於資料事件，值為 Data。
- 對於 Insights 事件，的值為 Insight。

自：1.07

選用：False

addendum

如果事件傳遞延遲，或有關現有事件的其他資訊會在記錄事件之後變成可用，附錄欄位會顯示事件延遲原因的相關資訊。如果現有事件中缺少，附錄欄位會包含缺少的資訊，以及缺失的原因。內容包括以下：

- **reason** - 事件或其部分內容遺失的原因。可為以下任何一個值。
  - **DELIVERY_DELAY**- 發生延遲傳遞事件。這可能是由於高網路流量、連線問題或 CloudTrail 服務問題所造成。
  - **UPDATED_DATA**- 事件記錄中的欄位遺失或值不正確。
  - **SERVICE_OUTAGE**— 將事件記錄為 CloudTrail 發生中斷，且無法將事件記錄到的服務 CloudTrail。這是非常罕見的情況。
- **updatedFields** - 附錄所更新的事件記錄欄位。只有當原因是 UPDATED_DATA 才提供此資訊。
- **originalRequestID** - 請求的原始唯一 ID。只有當原因是 UPDATED_DATA 才提供此資訊。
- **originalEventID** - 原始事件 ID。只有當原因是 UPDATED_DATA 才提供此資訊。

自：1.08

選用：True

sessionCredentialFromConsole

顯示事件是否源自 AWS Management Console 階段作業。此欄位不會顯示，除非值為 true，這意味著用於進行 API 呼叫的客戶端是代理或外部客戶端。如果已使用 Proxy 用戶端，tlsDetails 事件欄位不會顯示。

自：1.08

選用：True

edgeDeviceDetails

顯示作為要求目標之 Edge 裝置的相關資訊。目前，S3 Outposts 裝置事件包含此欄位。此欄位的大小上限為 28 KB；超過該限制的內容會被截斷。

自：1.08

選用：True

tlsDetails

顯示傳輸層安全性 (TLS) 版本、加密套件，以及用戶端提供的主機名稱 (通常是服務端點的 FQDN) 之用戶端提供的主機名稱的完整網域名稱 (FQDN) 的相關資訊。 CloudTrail如果預期的資訊遺失或空白，仍會記錄部分 TLS 詳細資料。例如，如果 TLS 版本和加密套件存在，但HOST標頭是空的，則可用的 TLS 詳細資料仍會記錄在 CloudTrail 事件中。

- **tlsVersion** - 要求的 TLS 版本。
- **cipherSuite** - 請求的密碼套件 (使用的安全演算法的組合)。
- **clientProvidedHostHeader** - 服務 API 呼叫中用戶端所提供的主機名稱，通常是服務端點的 FQDN。

> **Note**
>
> 在有些情形中，事件記錄中不顯示 tlsDetails 欄位。
>
> - 如果 API 呼叫是由代表您進行，則tlsDetails欄位不存 AWS 服務在。userIdentity 元素中的 invokedBy 欄位可識別執行 API 呼叫的 AWS 服務 。
> - 如果 sessionCredentialFromConsole 存在的值為 true，只有在使用外部用戶端來進行 API 呼叫時，tlsDetails 才會出現在事件記錄中。

自：1.08

選用：True

Insights 事件記錄欄位

以下是顯示在 Insights 事件 JSON 結構中的屬性，這些屬性與管理或資料事件中的屬性不同。

`sharedEventId`

A `sharedEventID` for CloudTrail Insights 事件不同`sharedEventID`於 CloudTrail事件的管理和資料類型。在見解事件中，a `sharedEventID` 是由見 CloudTrail 解產生的 GUID，用於唯一識別洞察事件。 `sharedEventID`在開始和結束 Insights 事件之間很常見，有助於連接這兩個事件以唯一識別異常活動。您可以將 `sharedEventID` 視為整體 Insights 事件 ID。

自：1.07

選用：False

`insightDetails`

僅限 Insights 事件。顯示 Insights 事件基本觸發程序的相關資訊，例如事件來源、使用者代理程式、統計資料、API 名稱，以及事件是否為 Insights 事件的開始或結束。如需 `insightDetails` 區塊之內容的詳細資訊，請參閱 CloudTrail 見解`insightDetails`元素。

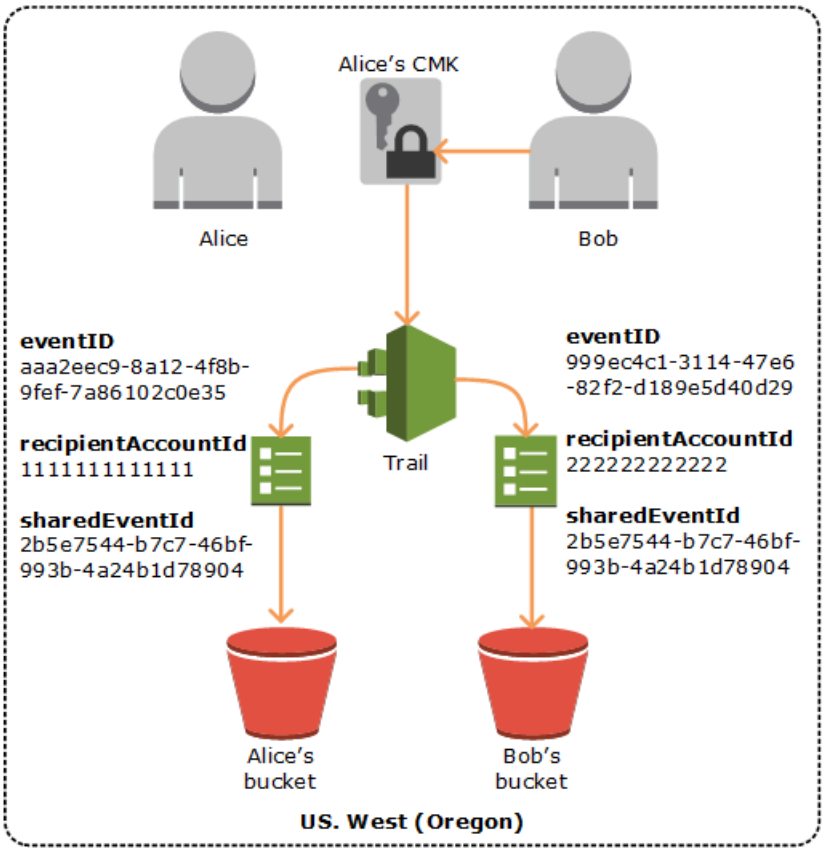
自：1.07

選用：False

sharedEventID 範例

下列範例說明如何針對相同動作 CloudTrail 傳遞兩個事件：

1. 愛麗絲有 AWS 帳戶（1111111111），並創建了一個. AWS KMS key她是此 KMS 金鑰的擁有者。
2. 鮑勃有 AWS 帳戶（2222222222）。Alice 會將使用 KMS 金鑰的許可授予 Bob。
3. 每個帳戶都會有追蹤和個別儲存貯體。
4. Bob 使用 KMS 金鑰呼叫 `Encrypt` API。
5. CloudTrail 發送兩個單獨的事件。
   - 一個事件會傳送給 Bob。事件顯示他已使用 KMS 金鑰。
   - 一個事件會傳送給 Alice。事件顯示 Bob 已使用 KMS 金鑰。
   - 兩個事件具有相同的 `sharedEventID`，但 `eventID` 和 `recipientAccountID` 是唯一的。



CloudTrail 深入解析中的共用事件 ID

A `sharedEventID` for CloudTrail Insights 事件不同`sharedEventID`於 CloudTrail 事件的管理和資料類型。在洞察事件中，a `sharedEventID` 是由見解產生的 GUID，用於唯一識別 CloudTrail 洞察事件的開始和結束對。 `sharedEventID`在開始和結束 Insights 事件之間很常見，有助於在兩個事件之間建立關聯性，以唯一識別不尋常的活動。

您可以將 `sharedEventID` 視為整體 Insights 事件 ID。

CloudTrail userIdentity 元素

AWS Identity and Access Management (IAM) 提供不同類型的身分識別。`userIdentity` 元素包含提出請求之 IAM 身分類型及所使用之登入資料的詳細資訊。如果使用暫時性登入資料，此元素會說明登入資料的取得方式。

內容

- 具有 SAML 和網路身分聯盟的 AWS STS API 的值
- AWS STS 來源身份

範例

具有 IAM 使用者憑證的 **userIdentity**

下列範例顯示使用名為 userIdentity 的 IAM 使用者登入資料提出之簡單請求的 Alice 元素。

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

使用暫時性安全登入資料的 **userIdentity**

下列範例顯示使用透過擔任 IAM 角色取得的暫時性安全登入資料提出之請求的 userIdentity 元素。此元素包含為取得登入資料所擔任之角色的其他詳細資訊。

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
    }
```

```
}
```

用於代表 IAM Identity Center 使用者提出請求的 **userIdentity**

以下範例顯示用於代表 IAM Identity Center 使用者提出請求的 userIdentity 元素。

```
"userIdentity": {
 "type": "IdentityCenterUser",
 "accountId": "123456789012",
 "onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
 },
 "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

欄位

userIdentity 元素中可能會顯示下列欄位。

type

身分的類型。可能的值如下：

- Root— 請求是使用您的 AWS 帳戶 憑據提出的。如果 userIdentity 類型為 Root，而且您為帳戶設定了別名，則 userName 欄位會包含您的帳戶別名。如需詳細資訊，請參閱您的 AWS 帳戶 ID 和其別名。
- IAMUser - 使用 IAM 使用者的登入資料提出請求。
- AssumedRole - 透過呼叫 AWS Security Token Service (AWS STS) AssumeRole API 取得的臨時安全憑證及角色提出請求。這可能包括適用於 Amazon EC2 和跨帳戶 API 存取的角色。
- Role – 使用具有特定許可的持久 IAM 身分提出請求。角色工作階段的發起者永遠都是該角色。如需有關角色的詳細資訊，請參閱《IAM 使用者指南》中的角色術語和概念。
- FederatedUser— 請求是使用通過對 AWS STS GetFederationTokenAPI 調用獲得的臨時安全憑據進行的。sessionIssuer 元素指出 API 是以超級或 IAM 使用者登入資料來呼叫。

  如需暫時安全登入資料的詳細資訊，請參閱《IAM 使用者指南》中的暫時安全登入資料。
- Directory - 已對 Directory Service 提出請求，且類型未知。目錄服務包括以下內容：Amazon WorkDocs 和 Amazon QuickSight。
- AWSAccount— 請求是由另一個人提出 AWS 帳戶

- AWSService— 請求 AWS 帳戶 是由屬於 AWS 服務. 例如， AWS Elastic Beanstalk 假設您的帳戶中有 IAM 角色，以代表您呼叫其他 AWS 服務 角色。
- IdentityCenterUser – 代表 IAM Identity Center 使用者提出請求。
- Unknown— 使用無法確定的身份類型 CloudTrail 提出請求。

選用：False

如果有使用您擁有之 IAM 角色的跨帳戶存取，您日誌中的 type 會顯示 AWSAccount 和 AWSService。

範例：由其他 AWS 帳戶啟動的跨帳戶存取

1. 您在帳戶中擁有 IAM 角色。
2. 另一個 AWS 帳戶會切換至該角色，以擔任您帳戶的角色。
3. 由於您擁有 IAM 角色，因此會收到日誌，顯示其他帳戶擔任該角色。type 為 AWSAccount。如需範例記錄項目，請參閱 CloudTrail 記錄檔中的AWS STS API 事件。

範例：由服務啟動的 AWS 跨帳戶存取

1. 您在帳戶中擁有 IAM 角色。
2. AWS 服務擁有的 AWS 帳戶會擔任該角色。
3. 由於您擁有 IAM 角色，因此會收到日誌，顯示 AWS 服務擔任該角色。type 為 AWSService。

userName

發出呼叫之身分的易記名稱。出現在 userName 中的值取決於 type 中的值。下表顯示 type 與 userName 之間的關係：

type	userName	描述
Root (未設定別名)	不存在	如果您尚未設定別名 AWS 帳戶，則不會顯示該userName欄位。如需有關帳戶別名的詳細資訊，請參閱您的 AWS 帳戶 ID 及其別名。請注意，userName 欄位不能包含 Root，因為 Root 是身分類型，不是使用者名稱。

type	userName	描述
Root (已設定別名)	帳戶別名	如需 AWS 帳戶 別名的詳細資訊，請參閱您的 AWS 帳戶 ID 及其別名。
IAMUser	IAM 使用者的使用者名稱	
AssumedRole	不存在	針對 AssumedRole 類型，您可以在 sessionContext 中找到屬於 **sessionIssuer** 元素一部分的 userName 欄位。如需範例項目，請參閱「範例」。
Role	使用者定義	sessionContext 和 sessionIssuer 區段包含替角色發起工作階段之身分的相關資訊。
FederatedUser	不存在	sessionContext 和 sessionIssuer 區段包含替聯合身分使用者發出工作階段之身分的相關資訊。
Directory	可以存在	例如，值可以是帳戶別名或相關聯 AWS 帳戶 ID 的電郵地址。
AWSService	不存在	
AWSAccount	不存在	
IdentityCenterUser	不存在	onBehalfOf 區段包含呼叫的 IAM Identity Center 使用者 ID 和身分存放區 ARN 的相關資訊。如需 IAM Identity Center 的詳細資訊，請參閱《AWS IAM Identity Center 使用者指南》。
Unknown	可以存在	例如，值可以是帳戶別名或相關聯 AWS 帳戶 ID 的電郵地址。

> **Note**
>
> 當記錄的事件是由不正確的使用者名稱輸入所造成的主控台登入失敗時，userName 欄位會包含字串 HIDDEN_DUE_TO_SECURITY_REASONS。CloudTrail 在此情況下不會記錄內容，因為文字可能包含敏感資訊，如下列範例所示：
>
> - 使用者不小心在使用者名稱欄位中輸入密碼。
> - 使用者按一下某個 AWS 帳戶登入頁面的連結，然後輸入另一個帳戶的帳號。
> - 使用者不小心輸入個人電子郵件帳戶的帳戶名稱、銀行登入識別符或其他一些私有 ID。

選用：True

principalId

發出呼叫之實體的唯一識別符。針對使用暫時性安全登入資料提出的請求，這個值會包含傳遞到 AssumeRole、AssumeRoleWithWebIdentity 或 GetFederationToken API 呼叫的工作階段名稱。

選用：True

arn

發出呼叫之主體的 Amazon Resource Name (ARN)。ARN 的最後一個部分包含發出呼叫的使用者或角色。

選用：True

accountId

擁有授予許可給請求之實體的帳戶。如果使用暫時性安全登入資料提出請求，則此為擁有用來取得登入資料之 IAM 使用者或角色的帳戶。

若使用 IAM Identity Center 授權存取權杖提出請求，則這是擁有 IAM Identity Center 執行個體的帳戶。

選用：True

accessKeyId

用來簽署請求的存取金鑰 ID。如果使用暫時性安全登入資料提出請求，則此為暫時性登入資料的存取金鑰 ID。基於安全理由，accessKeyId 可能不存在，或者可能顯示為空字符串。

選用：True

sessionContext

如果使用暫時性安全登入資料提出請求，sessionContext 會提供為這些登入資料所建立之工作階段的相關資訊。呼叫任何 API 以傳回暫時性登入資料時，您會建立工作階段。當使用者在主控台中工作，並且使用包含多重驗證的 API 提出請求時，也會建立工作階段。此元素具有下列屬性：

- creationDate - 發出暫時性安全登入資料的日期和時間。以 ISO 8601 基本表示法來表示。
- mfaAuthenticated - 如果其登入資料用於請求的根使用者或 IAM 使用者也會向 MFA 裝置進行身分驗證，則此值為 true；否則為 false。
- sourceIdentity – 參閱此主題中的 AWS STS 來源身份。在使用者擔任 IAM 角色執行動作時，sourceIdentity 欄位會出現在事件中。sourceIdentity 識別提出請求的原始使用者身分，無論該使用者身分是 IAM 使用者、IAM 角色、使用 SAML 型聯合驗證的使用者，還是使用 OpenID Connect (OIDC) 相容的網頁聯合身分驗證的使用者。如需有關設定 AWS STS 以收集來源身分資訊的詳細資訊，請參閱《IAM 使用者指南》中的監控和控制假定角色所採取的動作。
- ec2RoleDelivery – 如果憑證由 Amazon EC2 Instance Metadata Service Version 1 (IMDSv1) 提供，此值為 1.0。如果使用新的 IMDS 結構描述提供憑證，此值為 2.0。

  AWS Amazon EC2 執行個體中繼資料服務 (IMDS) 提供的登入資料包含 ec2: RoleDelivery IAM 內容金鑰。透過使用內容金鑰做為 IAM 政策、資源政策 service-by-service 或服務控制政策中的條件，此內容金鑰可讓您輕鬆強制執行新配置的使 AWS Organizations 用或 resource-by-resource 基礎。如需詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的執行個體中繼資料和使用者資料。

選用：True

invokedBy

發出請求 AWS 服務 的名稱，當請求是由 AWS 服務 如 Amazon EC2 Auto Scaling 或 AWS Elastic Beanstalk. 此欄位僅在由 AWS 服務. 這包括服務使用轉寄存取工作階段 (FAS)、 AWS 服務 主參與者、服務連結角色或. AWS 服務

選用：True

sessionIssuer

如果使用者使用暫時性安全登入資料提出請求，sessionIssuer 會提供該使用者如何取得登入資料的相關資訊。例如，如果他們透過擔任角色取得暫時性安全登入資料，此元素會提供所擔任角色的相關資訊。如果他們使用根或 IAM 使用者登入資料呼叫 AWS STS GetFederationToken 而取得登入資料，此元素會提供根帳戶或 IAM 使用者的相關資訊。此元素具有下列屬性：

- type - 暫時性安全登入資料的來源，例如 Root、IAMUser 或 Role。

- userName - 發出工作階段之使用者或角色的易記名稱。出現的值取決於 sessionIssuer 身分 type。下表顯示 sessionIssuer type 與 userName 之間的關係：

sessionIssuer 類型	userName	描述
Root (未設定別名)	不存在	如果您尚未設定帳戶的別名，則不會顯示 userName 欄位。如需 AWS 帳戶 別名的詳細資訊，請參閱您的 AWS 帳戶 ID 及其別名。請注意，userName 欄位不能包含 Root，因為 Root 是身分類型，不是使用者名稱。
Root (已設定別名)	帳戶別名	如需 AWS 帳戶 別名的詳細資訊，請參閱您的 AWS 帳戶 ID 及其別名。
IAMUser	IAM 使用者的使用者名稱	這也適用於聯合身分使用者使用 IAMUser 所發出之工作階段的情況。
Role	角色名稱	由 IAM 使用者或 Web 身分聯合身分使用者在角色工作階段中所承擔的角色。 AWS 服務

- principalId - 用來取得登入資料之實體的內部 ID。
- arn - 用來取得暫時性安全登入資料之來源 (帳戶、IAM 使用者或角色) 的 ARN。
- accountId - 擁有用來取得登入資料之實體的帳戶。

選用：True

onBehalfOf

如果由 IAM Identity Center 呼叫者提出請求，onBehalfOf 會提供呼叫的 IAM Identity Center 使用者 ID 和身分存放區 ARN 的相關資訊。此元素具有下列屬性：

- userId— 被代表執行呼叫之 IAM Identity Center 使用者的 ID。
- identityStoreArn— 被代表執行呼叫之 IAM Identity Center 身分存放區的 ARN。

選用：True

credentialId

用於請求的登入資料 ID。只有當呼叫者使用持有人權杖時，例如 IAM Identity Center 授權存取權杖，才會執行此設定。

選用：True

webIdFederationData

如果使用由網頁聯合身分取得的暫時性安全登入資料提出請求，webIdFederationData 會列出身分提供者的相關資訊。

此元素具有下列屬性：

- federatedProvider - 身分提供者的主體名稱 (例如 Login with Amazon 的 www.amazon.com 或 Google 的 accounts.google.com)。
- attributes - 供應商所回報的應用程式 ID 和使用者 ID (例如 Login with Amazon 的 www.amazon.com:app_id 和 www.amazon.com:user_id)。

> **Note**
>
> 遺漏此欄位或此欄位的值為空白，表示沒有身分識別提供者的相關資訊。

選用：True

具有 SAML 和網路身分聯盟的 AWS STS API 的值

AWS CloudTrail 支援使用安全性宣告標記語言 AWS Security Token Service (SAML AWS STS) 和 Web 身分聯合進行的記錄 () API 呼叫。當使用者呼叫AssumeRoleWithSAML和AssumeRoleWithWebIdentityAPI 時，會 CloudTrail 記錄呼叫，並將事件傳送到您的 Amazon S3 儲存貯體。

這些 API 的 userIdentity 元素包含下列值。

type

身分類型。

- SAMLUser - 使用 SAML 聲明提出請求。
- WebIdentityUser - 由 Web 聯合身分提供者提出請求。

principalId

發出呼叫之實體的唯一識別符。

- 針對 SAMLUser，這是 saml:namequalifier 和 saml:sub 金鑰的組合。

- 針對 WebIdentityUser，這是發行者、應用程式 ID 和使用者 ID 的組合。

userName

發出呼叫之身分的名稱。

- 針對 SAMLUser，這是 saml:sub 金鑰。
- 針對 WebIdentityUser，這是使用者 ID。

identityProvider

外部身分提供者的主體名稱。只有 SAMLUser 或 WebIdentityUser 類型會顯示此欄位。

- 針對 SAMLUser，這是 SAML 聲明的 saml:namequalifier 金鑰。
- 針對 WebIdentityUser，這是 Web 聯合身分提供者的發行者名稱。這可以是您設定的供應商，例如：
  - cognito-identity.amazon.com 適用於 Amazon Cognito
  - Login with Amazon 的 www.amazon.com
  - Google 的 accounts.google.com
  - Facebook 的 graph.facebook.com

以下是 AssumeRoleWithWebIdentity 動作的範例 userIdentity 元素。

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

有關userIdentity元素如何顯示SAMLUser和WebIdentityUser類型的示例日誌，請參閱使用記錄 IAM 和 AWS STS API 呼叫 AWS CloudTrail。

AWS STS 來源身份

IAM 管理員可以設定 AWS Security Token Service 為在使用臨時登入資料擔任角色時，要求使用者指定其身分。使用者擔任 IAM 角色或使用所擔任角色執行任何動作時，sourceIdentity 欄位會出現在事件中。

sourceIdentity 欄位識別提出請求的原始使用者身分，無論該使用者身分是 IAM 使用者、IAM 角色、使用 SAML 型聯合驗證的使用者，還是使用 OpenID Connect (OIDC) 相容的網頁聯合身分驗證的使用者。IAM 管理員設定完成後 AWS STS，在事件 CloudTrail 記錄中的下列事件和位置記錄sourceIdentity資訊：

- 使用者身分在 AWS STS AssumeRole擔任角色時所進行的AssumeRoleWithSAML、或AssumeRoleWithWebIdentity呼叫。 sourceIdentity在 AWS STS 呼叫的requestParameters塊中找到。
- 如果使用者身分使用角色來承擔另一個角色 (稱為角色鏈結)，則會進行、或AssumeRoleWithWebIdentity呼叫。 AWS STS AssumeRole AssumeRoleWithSAML sourceIdentity在 AWS STS 呼叫的requestParameters塊中找到。
- AWS 服務 API 會在擔任角色並使用由指派的臨時憑證時呼叫使用者身分所做的 AWS STS。在服務 API 事件中，sessionContext 區塊中找到 sourceIdentity。例如，如果使用者身分識別建立新的 S3 儲存貯體，則 CreateBucket 事件的 sessionContext 區塊中會發生 sourceIdentity。

如需有關如何設定以收集 AWS STS 來源身分資訊的詳細資訊，請參閱《IAM 使用者指南》中的監控和控制假定角色所採取的動作。如需有關記錄到的 AWS STS 事件的詳細資訊 CloudTrail，請參閱 IAM 使用者指南 AWS CloudTrail中的記錄 IAM 和 AWS STS API 呼叫。

以下是事件的範例片段，其中顯示 sourceIdentity 欄位。

範例 **requestParameters** 區段

在下列範例事件片段中，使用者 AWS STS AssumeRole提出要求，並設定來源識別，此處以表示*source-identity-value-set*。使用者承擔由角色 ARN arn:aws:iam::123456789012:role/Assumed_Role 表示的角色。sourceIdentity 欄位位於事件的 requestParameters 區塊。

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
    },
```

範例 **responseElements** 區段

在下列範例事件片段中，使用者提出 AWS STS AssumeRole要求假設名為的角色Developer_Role，並設定來源識別Admin。使用者承擔由角色 ARN arn:aws:iam::111122223333:role/Developer_Role 表示的角色。sourceIdentity 欄位會顯示在事件的 requestParameters 和 responseElements 區塊。用來擔任角色、工作階段 Token 字串以及擔任的角色 ID、工作階段名稱和工作階段 ARN 的臨時憑證會與來源身分一起顯示在 responseElements 區塊。

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                            EXAMPLE_SESSION_TOKEN
                            XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

範例 **sessionContext** 區段

在下列範例事件片段中，使用者假設名DevRole為呼叫 AWS 服務 API 的角色。使用者設定來源身分，此處以表示*source-identity-value-set*。sourceIdentity 欄位位於 sessionContext 區塊，在事件的 userIdentity 區塊內。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

CloudTrail 見解**insightDetails**元素

AWS CloudTrail 見解事件記錄包含與其 JSON 結構中的其他 CloudTrail 事件不同的欄位，有時稱為裝載。 CloudTrail Insights 事件記錄包含一個insightDetails區塊，其中包含 Insights 事件基礎觸發器的相關資訊，例如事件來源、使用者身分識別、使用者代理程式、歷史平均值或基準線、統計資料、API 名稱，以及事件是否為 Insights 事件的開始或結束。insightDetails 區塊包含下列資訊：

- **state** - 活動是否為開始或結束 Insights 事件。此值可以為 Start 或 End。

  自：1.07

選用：False

- **eventSource**-作為異常活動來源的 AWS 服務端點，例如ec2.amazonaws.com。

  自：1.07

  選用：False

- **eventName** - Insight 事件的名稱，通常是異常活動來源的 API 名稱。

  自：1.07

  選用：False

- **insightType** - Insights 事件的類型。此值可以為 ApiCallRateInsight 或 ApiErrorRateInsight (或兩者)。

  自：1.07

  選用：False

- **insightContext** -

  AWS 工具 (稱為使用者代理程式)、IAM 使用者和角色 (稱為使用者身分)，以及與 CloudTrail 分析以產生 Insights 事件的事件相關聯的錯誤代碼的相關資訊。此元素也包含統計資料，顯示 Insights 事件中的異常活動與基準或正常活動的比較。

  自：1.07

  選用：False

  - **statistics** - 包括有關基準的資料，或在基準期間衡量的帳戶對主旨 API 的一般平均呼叫率或錯誤率、Insights 事件在 Insights 事件第一分鐘觸發 Insights 事件的平均呼叫率或錯誤率、Insights 事件持續時間 (以分鐘為單位)，以及基準衡量期間的持續時間 (以分鐘為單位)。

    自：1.07

    選用：False

    - **baseline** - 針對帳戶的 Insights 事件主旨 API 基準持續時間內，每分鐘平均 API 呼叫或錯誤次數 (在 Insights 事件開始前七天計算)。

      自：1.07

      選用：False

- **insight** -

  針對起始 Insights 事件，此值是異常活動開始期間每分鐘平均 API 呼叫或錯誤次數。針對結束 Insights 事件，此值是異常活動期間每分鐘平均 API 呼叫或錯誤次數。

  自：1.07

  選用：False

- **insightDuration** - Insights 事件的持續時間 (以分鐘為單位) (從主旨 API 上異常活動開始到結束的期間)。開始和結束 Insights 事件中均會出現 `insightDuration`。

  自：1.07

  選用：False

- **baselineDuration** - 基準期間的持續時間 (以分鐘為單位) (主旨 API 上衡量一般活動的時段)。`baselineDuration`是 Insights 事件前的最少七天 (10080 分鐘)。此欄位會出現在開始和結束 Insights 事件中。`baselineDuration` 測量的結束時間永遠是 Insights 事件的開始。

  自：1.07

  選用：False

- **attributions** - 此區塊包括有關使用者身分、使用者代理程式和錯誤碼與異常和基準活動相關的資訊。Insights 事件中最多會擷取五個使用者身分、五個使用者代理程式和五個錯誤碼`attributions`區塊，按活動計數的平均值按從高到低的降序排列。

  自：1.07

  選用：True

  - **attribute** - 包含屬性類型。此值可以是 `userIdentityArn`、`userAgent` 或 `errorCode`。
    - **userIdentityArn**-最多顯示前五名 AWS 使用者或 IAM 角色的區塊，這些角色在異常活動和基準期間導致 API 呼叫或錯誤。另請參閱 `userIdentity` 中的 CloudTrail 記錄內容。

      自：1.07

      選用：False

      - **insight** - 一個區塊，顯示最多五個使用者身分 ARN，這些 ARN 促成了在異常活動期間進行的 API 呼叫，從最大數量的 API 呼叫到最小數量的降序排列。它也會顯示使用者身分在異常活動期間進行的 API 呼叫平均數目。

自：1.07

選用：False

- **value** - 導致在異常活動期間進行的 API 呼叫的前五名使用者身分之一的 ARN。

  自：1.07

  選用：False

- **average** - value 欄位中，使用者身分在異常活動期間每分鐘 API 呼叫或錯誤的次數。

  自：1.07

  選用：False

- **baseline** - 一個區塊，顯示在正常活動期間最常導致 API 呼叫或錯誤的最多前五名使用者身分 ARN。同時也會顯示使用者身分在正常活動期間記錄的平均 API 呼叫或錯誤次數。

  自：1.07

  選用：False

  - **value** - 在正常活動期間導致 API 呼叫或錯誤的前五名使用者身分之一的 ARN。

    自：1.07

    選用：False

  - **average** - value 欄位中，使用者身分在 Insights 活動開始時間前七天內，每分鐘 API 呼叫或錯誤的歷史平均值。

    自：1.07

    選用：False

- **userAgent**-顯示最多前五個 AWS 工具的區塊，使用者身分在異常活動和基準期間對 API 呼叫做出貢獻。這些工具包括 AWS Management Console AWS CLI、或 AWS SDK。另請參閱 userAgent 中的 CloudTrail 記錄內容。

  自：1.07

  選用：False

- **insight** - 一顯示最多五個使用者代理程式的區塊，這些代理程式促成了在異常活動期間進行的 API 呼叫，從最大數量的 API 呼叫到最小數量的降序排列。同時也會顯示使用者代理程式在異常活動期間記錄的平均 API 呼叫或錯誤次數。

  自：1.07

  選用：False

  - **value** - 導致在異常活動期間進行的 API 呼叫的前五個使用者代理程式之一。

    自：1.07

    選用：False

  - **average** - `value` 欄位中，使用者代理程式在異常活動期間每分鐘記錄的 API 呼叫或錯誤的數量。

    自：1.07

    選用：False

- **baseline** - 最多顯示前五名使用者代理程式的區塊，這些區塊對正常活動期間所做的 API 呼叫做出貢獻最多。同時也會顯示使用者代理程式在正常活動期間記錄的平均 API 呼叫或錯誤次數。

  自：1.07

  選用：False

  - **value** - 在正常活動期間記錄的導致 API 呼叫或錯誤的前五名使用者代理程式之一。

    自：1.07

    選用：False

  - **average** - `value` 欄位中，使用者代理程式在 Insights 活動開始時間前七天內，每分鐘 API 呼叫或錯誤的歷史平均值。

    自：1.07

    選用：False

- **errorCode** - 最多顯示在異常活動和基準期間 API 呼叫上發生的前五個錯誤碼的區塊，按從 API 呼叫次數最多到最少的降序排列。另請參閱 `errorCode` 中的 CloudTrail 記錄內容。

自：1.07

選用：False

- **insight** - 最多顯示在異常活動期間 API 呼叫上發生的前五個錯誤碼的區塊，按從 API 呼叫次數最多到最少的降序排列。它也會顯示在異常活動期間進行的 API 呼叫的平均數目。

  自：1.07

  選用：False

  - **value** - 在異常活動期間進行的 API 呼叫上發生的前五個錯誤碼之一，例如 `AccessDeniedException`。

    如果觸發 Insights 事件的呼叫都不會產生錯誤，則此值為 `null`。

    自：1.07

    選用：False

  - **average** - `value` 欄位中，在異常活動期間錯誤碼每分鐘 API 呼叫的數量。

    如果錯誤碼值為 `null`，並且 `insight` 區塊中沒有其他錯誤碼，`average` 中的值與 Insights 事件的 `statistics` 區塊中的值整體相同。

    自：1.07

    選用：False

- **baseline** - 最多顯示前五個錯誤碼的區塊，這些區塊對正常活動期間所做的 API 呼叫做出貢獻最多。它也會顯示使用者代理程式在正常活動期間進行的 API 呼叫平均數目。

  自：1.07

  選用：False

  - **value** - 在正常活動期間進行的 API 呼叫上發生的前五個錯誤碼之一，例如 `AccessDeniedException`。

    自：1.07

    選用：False

  - **average** - `value` 欄位中，錯誤代碼在 Insights 活動開始時間前七天內，每分鐘 API 呼叫或錯誤的歷史平均值。

自：1.07

選用：False

範例 insightDetails 區塊

以下為 Application Auto Scaling API CompleteLifecycleAction 被呼叫異常次數時發生的 Insights 事件的 Insights 事件 insightDetails 區塊的範例。如需完整 Insights 事件的範例，請參閱洞察活動。

此範例來自開始 Insights 事件，由 "state": "Start" 指示。呼叫與 Insights 事件、CodeDeployRole1、CodeDeployRole2，以及 CodeDeployRole3 相關聯之 API 的主要使用者身分，以及此 Insights 事件的平均 API 呼叫率，以及 attributions 角色 基準會顯示在 CodeDeployRole1 區塊。該attributions塊還顯示用戶代理是codedeploy.amazonaws.com，這意味著使用 AWS CodeDeploy 控制台運行 API 調用的頂級用戶身份。

因為沒有與已分析以產生 Insight 事件的事件相關聯的錯誤碼 (值為 null)，錯誤碼的 insight 平均值與整個 Insights 事件的整體 insight 的平均值相同 (顯示在 statistics 區塊。

```
        "insightDetails": {
          "state": "Start",
          "eventSource": "autoscaling.amazonaws.com",
          "eventName": "CompleteLifecycleAction",
          "insightType": "ApiCallRateInsight",
          "insightContext": {
            "statistics": {
              "baseline": {
                "average": 0.0000882145
              },
              "insight": {
                "average": 0.6
              },
              "insightDuration": 5,
              "baselineDuration": 11336
            },
            "attributions": [
              {
                "attribute": "userIdentityArn",
                "insight": [
                  {
```

```
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                    "average": 0.2
                  }
                ],
                "baseline": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
```

```
                }
              ],
              "baseline": [
                {
                  "value": "null",
                  "average": 0.0000882145
                }
              ]
            }
          ]
        }
      }
```

擷取的非 API 事件 CloudTrail

除了記錄 AWS API 呼叫之外，還可 CloudTrail 擷取其他相關事件，這些事件可能對您的 AWS 帳戶產生安全性或合規性影響，或可能協助您疑難排解作業問題。

主題

- AWS 服務事件
- AWS Management Console 登入事件

AWS 服務事件

CloudTrail 支援記錄非 API 服務事件。這些事件是由 AWS 服務所建立，但不會直接由公 AWS 用 API 的要求觸發。對於這些事件，`eventType` 欄位是 `AwsServiceEvent`。

以下是在 AWS Key Management Service (AWS KMS) 中自動輪換客戶管理的金鑰時， AWS 服務事件的範例案例。如需有關轉換 KMS 金鑰的詳細資訊，請參閱 轉換 KMS 金鑰。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
```

```
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```


AWS Management Console 登入事件

CloudTrail 記錄嘗試登入 AWS Management Console、 AWS 論壇和 Sup AWS port 中心。所有 IAM 使用者和 root 使用者登入事件，以及所有聯合使用者登入事件，都會在記錄檔中 CloudTrail 產生記錄。如需有關尋找與檢視日誌的資訊，請參閱 尋找您的 CloudTrail 記錄檔 和 下載您的 CloudTrail 記錄檔。

> **Note**
>
> `ConsoleLogin`事件中記錄的區域會因使用者類型以及您使用全域或地區端點登入而有所不同。
>
> - 如果您以根使用者身分登入，則會在 us-east-1 中 CloudTrail 記錄事件。
> - 如果您使用 IAM 使用者登入並使用全域端點，則會 CloudTrail 記錄`ConsoleLogin`事件的「區域」，如下所示：
>   - 如果瀏覽器中存在帳戶別名 Cookie，則會在下列其中一個區域中 CloudTrail 記錄`ConsoleLogin`事件：US-east-2、eu-north-1 或 AP-東南 -2。這是因為主控台 Proxy 會根據使用者登入位置的延遲重新導向使用者。
>   - 如果瀏覽器中沒有帳戶別名 cookie，則會在 us-east-1 中 CloudTrail 記錄該`ConsoleLogin`事件。這是因為控制台代理重定向回全局登錄。

- 如果您使用 IAM 使用者登入並使用區域端點，則會在端點的適當區域中 CloudTrail 記錄ConsoleLogin事件。如需有關 AWS 登入 端點的詳細資訊，請參閱AWS 登入 端點和配額。

主題

IAM 使用者的範例事件記錄

下列範例顯示數個 IAM 使用者登入案例的事件記錄。

主題

IAM 使用者，在沒有 MFA 的情況下成功登入

下列記錄顯示名為的使用者Anaya已成功登入， AWS Management Console 但不使用多重要素驗證 (MFA)。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
```

```
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


IAM 使用者，在使用 MFA 的情況下成功登入

下列記錄顯示名為的 IAM 使用者Anaya已成功登入 AWS Management Console 使用多重要素驗證 (MFA)。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 使用者，登入失敗

下列記錄顯示名為 Paulo 的 IAM 使用者的失敗登入嘗試。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 使用者，登入程序檢查 MFA (單一 MFA 裝置類型)

以下顯示登入程序檢查 IAM 使用者登入時是否需要多重要素驗證 (MFA)。在此範例中，mfaType 值為 U2F MFA，表示 IAM 使用者已啟用單一 MFA 裝置或多台相同類型的 MFA 裝置 (U2F MFA)。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
```

```
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM 使用者，登入程序檢查 MFA (多個 MFA 裝置類型)

以下顯示登入程序檢查 IAM 使用者登入時是否需要多重要素驗證 (MFA)。在此範例中，mfaType 值為 Multiple MFA Devices，表示 IAM 使用者已啟用多個 MFA 裝置類型。

```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Mary"
    },
    "eventTime": "2023-07-19T23:10:09Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Multiple MFA Devices"
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

根使用者的範例事件紀錄

下列範例顯示多種 root 使用者登入案例的事件記錄。當您使用根使用者登入時，會在 us-east-1 中 CloudTrail 記錄ConsoleLogin事件。

主題

- 根使用者，在沒有 MFA 的情況下成功登入
- 根使用者，在使用 MFA 的情況下成功登入
- 根使用者，登入失敗
- 根使用者，MFA 已變更
- 根使用者，密碼已變更

根使用者，在沒有 MFA 的情況下成功登入

以下顯示根使用者的成功登入事件並未使用多重要素驗證 (MFA)。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

根使用者，在使用 MFA 的情況下成功登入

以下顯示根使用者的成功登入事件使用了多重要素驗證 (MFA)。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
```

```
}
```

根使用者，登入失敗

以下顯示根使用者的登入失敗事件並未使用 MFA。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
```

```
}
```

根使用者，MFA 已變更

下列顯示根使用者變更多重要素驗證 (MFA) 設定的範例事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
```

```
}
```

根使用者，密碼已變更

下列顯示根使用者變更其密碼的範例事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
}
```

聯合身分使用者的範例事件紀錄

下列範例顯示聯合身分使用者的事件記錄。聯合使用者會獲得暫時的安全登入資料，以透過AssumeRole要求存取 AWS 資源。

下列顯示聯合身分加密請求的範例事件。原始存取金鑰 ID 會在 userIdentity 元素的 accessKeyId 欄位中提供。如果請求的 sessionDuration 在加密請求中傳遞，則 responseElements 中的 accessKeyId 欄位將包含一個新的存取金鑰 ID，否則它將包含原始存取金鑰 ID 的值。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
```

```
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

以下顯示聯合身分使用者未使用多重要素驗證 (MFA) 而成功登入的事件。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

使用 CloudTrail 記錄檔

您可以對 CloudTrail 檔案執行更進階的工作。

- 為每個區域建立多個追蹤。
- 通過將日 CloudTrail 誌文件發送到 CloudWatch 日誌來監視它們。
- 在帳戶之間共享日誌檔案。
- 使用 AWS CloudTrail 處理程式庫以 Java 撰寫記錄處理應用程式。
- 驗證您的記錄檔，以確認它們在遞送之後並未變更 CloudTrail。

當您的帳戶中發生事件時，會 CloudTrail 評估事件是否符合追蹤的設定。只有符合追蹤設定的事件才會傳送到 Amazon S3 儲存貯體和 Amazon CloudWatch 日誌日誌群組。

您可以分別設定多筆追蹤，以便追蹤只處理和記錄您指定的事件。例如，一筆追蹤可以記錄唯讀資料和管理事件，以便所有的唯讀事件交付到一個 S3 儲存貯體。另一筆追蹤可以只記錄唯寫資料和管理事件，以便所有的唯寫事件交付到另一個 S3 儲存貯體。

您也可以設定您的追蹤，其中一筆追蹤記錄所有管理事件並交付到一個 S3 儲存貯體，並設定另一筆追蹤記錄所有資料事件並交付到另一個 S3 儲存貯體。

您可以設定您的追蹤記錄下列事項：

- 資料事件：這些事件可讓您深入了解對資源執行或在資源中執行的資源操作。這些也稱為資料平面操作。
- 管理事件：管理事件可讓您查看對 AWS 帳戶中資源執行的管理作業。這些也稱為控制平面操作。管理事件也可以包含您帳戶中發生的非 API 事件。例如，當使用者登入您的帳戶時，會 CloudTrail 記錄`ConsoleLogin`事件。如需詳細資訊，請參閱 擷取的非 API 事件 CloudTrail。
- Insights 事件：Insights 事件會擷取在您的帳戶中偵測到的異常活動。如果您啟用了 Insights 事件並 CloudTrail 偵測到異常活動，Insights 事件會記錄到您追蹤的目的地 S3 儲存貯體，但會記錄在不同的資料夾中。您也可以在 CloudTrail 主控台上檢視 Insights 事件時，查看 Insights 事件的類型和事件期間。與 CloudTrail 追蹤中擷取的其他類型事件不同，Insights 事件只有在 CloudTrail 偵測到帳戶 API 使用量與帳戶的典型使用模式明顯不同時，才會記錄 Insights 事件。

  僅針對管理 API 產生 Insights 事件。如需詳細資訊，請參閱 記錄 Insights 事件。

> **Note**
>
> CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內提供記錄檔。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
> 如果您錯誤設定追蹤 (例如，無法連線 S3 儲存貯體)， CloudTrail 將嘗試將日誌檔重新傳送到 S3 儲存貯體 30 天，而且這些 attempted-to-deliver 事件將收取標準費用。 CloudTrail 若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

主題

從多個區域接收 CloudTrail 記錄檔

您可以設定 CloudTrail 將日誌檔從多個區域傳遞到單一帳戶的單一 S3 儲存貯體。例如，您在美國西部 (奧勒岡) 區域中有一個追蹤，設定為將日誌檔傳遞到 S3 儲存貯體和 CloudWatch 日誌記錄群組。當您變更現有的單一區域追蹤以記錄所有區域時，會 CloudTrail 記錄帳戶中單一 AWS 磁碟分割中所有區域的事件。 CloudTrail 將日誌檔傳遞到相同的 S3 儲存貯體和 CloudWatch 日誌記錄群組。只要 CloudTrail 具有寫入 S3 儲存貯體的權限，多區域追蹤的儲存貯體就不必位於追蹤的主區域中。

若要記錄帳戶中所有分割區中所有 AWS 區域的事件，請在每個磁碟分割中建立多區域追蹤。

依預設，當您在主控台中建立追蹤時，該追蹤會記錄您正在使用的 AWS 分割區中所有 AWS 區域 的事件。這是建議的最佳實務。若要記錄單一區域內的事件 (不建議)，請使用 AWS CLI。若要設定現有的單一區域追蹤以記錄所有區域，您必須使用 AWS CLI。

若要變更現有的線索，使該線索套用至所有區域，請新增 `--is-multi-region-trail` 選項至 update-trail 命令。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

若輸出中的 IsMultiRegionTrail 元素顯示 true，即可確定追蹤現會套用至所有區域。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 當新區域在aws分區中啟 CloudTrail 動時，會使用與原始路徑相同的設置自動在新區域中為您創建一個跟踪。

如需詳細資訊，請參閱下列資源：

- 使用 CloudTrail 軌跡
- CloudTrail 常見問

管理資料一致性 CloudTrail

CloudTrail 使用稱為最終一致性的分佈式計算模型。您對 CloudTrail 組態 (或其他 AWS 服務) 所做的任何變更，包括在屬性型存取控制 (ABAC) 中使用的標籤，都需要一些時間才能從所有可能的端點看見。從將資料從伺服器傳送到伺服器、從複製區域傳送到複製區域，以及從區域傳送到全球各地的區域，所花費的某些延遲時間所產生的結果。 CloudTrail 還使用緩存來提高性能，但在某些情況下，這可能會增加時間。直到先前快取的資料逾時後，才能看到變更。

您設計的應用程式必須能夠處理這些可能的延遲問題。確保它們即使在某個位置所做的變更不會立即顯示在另一個位置時，仍能如預期般運作。這類變更包括建立或更新追蹤或事件資料存放區、更新事件選取器，以及開始或停止記錄。建立或更新追蹤或事件資料存放區時，會根據上次已知的組態將日誌傳 CloudTrail 遞至 S3 儲存貯體或事件資料存放區，直到變更傳播到所有位置為止。

如需有關此功能如何影響其他人的詳細資訊 AWS 服務，請參閱下列資源：

- Amazon DynamoDB：DynamoDB 常見問答集中的 DynamoDB 的一致性模式是什麼？以及位於 Amazon DynamoDB 開發人員指南中的讀取一致性。
- Amazon EC2：Amazon Elastic Compute Cloud API 參考中的最終一致性。
- Amazon EMR：確保在AWS 大數據博客中 MapReduce 為 ETL 工作流程使用 Amazon S3 和 Amazon 彈性時的一致性。
- AWS Identity and Access Management (IAM)：我所做的變更並不一定會立即顯示在 IAM 使用者指南中。
- Amazon Redshift：Amazon Redshift 資料庫開發人員指南中的管理資料一致性。
- Amazon S3：Amazon Simple Storage Service 使用者指南中的 Amazon S3 資料一致性模式。

使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔

您可以 CloudTrail 使用 CloudWatch 日誌進行配置，以監控跟踪日誌並在特定活動發生時收到通知。

1. 設定追蹤以將記錄事件傳送至 CloudWatch 記錄檔。
2. 定義 CloudWatch 記錄量度篩選器，以評估記錄事件是否符合字詞、片語或值。例如，您可以監控 `ConsoleLogin` 事件。
3. 將 CloudWatch 量度指派給量度篩選器。
4. 建立根據您指定的臨界值和時間週期觸發的 CloudWatch 警示。您可以設定警示以在觸發警示時傳送通知，讓您可以採取動作。
5. 您也可以設定 CloudWatch 為自動執行動作以回應警示。

Amazon CloudWatch 和 Amazon CloudWatch 日誌適用標準定價。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

如需有關可設定追蹤以將日誌傳送到日誌的區域的詳細資訊，請參閱AWS 一般參考中的 Amazon CloudWatch 日誌區域和配額。 CloudWatch

主題

- 將事件傳送至 CloudWatch 記錄檔
- 建立 CloudTrail 事件 CloudWatch 警示：範例
- 停 CloudTrail 止將事件傳送至 CloudWatch 記錄檔
- CloudWatch 的記錄群組和記錄資料流命名 CloudTrail
- 使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件

將事件傳送至 CloudWatch 記錄檔

當您將追蹤設定為將事件傳送至 CloudWatch 記錄檔時，只 CloudTrail 會傳送符合追蹤設定的事件。例如，如果您將追蹤設定為僅記錄資料事件，則追蹤只會將資料事件傳送至您的 CloudWatch 記錄檔記錄群組。 CloudTrail 支援將資料、見解和管理事件傳送至 CloudWatch 記錄。如需詳細資訊，請參閱使用 CloudTrail 記錄檔。

> **Note**
>
> 只有管理帳戶可以使用主控台為組織追蹤設定 CloudWatch 記錄檔群組。委派的系統管理員可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 作業來設定 CloudWatch 記錄檔群組。

如果要將事件傳送至記 CloudWatch 錄檔記錄群組：

- 請確定您有足夠權限建立或指定 IAM 角色。如需詳細資訊，請參閱 授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限。
- 如果您要使用設定 CloudWatch 記錄檔記錄群組 AWS CLI，請確定您有足夠的權限可在您指定的 CloudWatch 記錄群組中建立記錄資料流，並將 CloudTrail 事件傳遞至該記錄串流。如需詳細資訊，請參閱 建立政策文件。
- 建立新的線索或指定現有的線索。如需詳細資訊，請參閱 使用主控台建立和更新線索。
- 建立日誌群組或指定現有的日誌群組。
- 指定 IAM 角色。如果要修改組織線索的現有 IAM 角色，您必須手動更新政策，以允許組織線索的記錄。如需更多詳細資訊，請參閱這個政策範例與建立組織追蹤。
- 連接角色政策或使用預設值。

內容

- 建立政策文件
- 更新線索
- 限制

使用主控台設定 CloudWatch 記錄監控

您可以使用 AWS Management Console 來設定追蹤，將事件傳送至 CloudWatch 記錄檔以進行監視。

建立日誌群組或指定現有的日誌群組

CloudTrail 使用記 CloudWatch 錄檔記錄群組做為記錄事件的傳遞端點。您可以建立日誌群組或指定現有的日誌群組。

若要為現有的追蹤建立或指定日誌群組

1. 請確定您以具有足夠權限的系統管理使用者或角色登入，以設定 CloudWatch 記錄檔整合。如需詳細資訊，請參閱 授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限。

   > **Note**
   >
   > 只有管理帳戶可以使用主控台為組織追蹤設定 CloudWatch 記錄檔群組。委派的系統管理員可以使用 AWS CLI 或 CloudTrail `CreateTrail`或 `UpdateTrail` API 作業來設定 CloudWatch 記錄檔群組。

2. 請在以下位置開啟 CloudTrail 主控台。 https://console.aws.amazon.com/cloudtrail/
3. 選擇線索名稱。如果您選擇套用到所有區域的追蹤，系統會將您重新導向到建立該追蹤的區域。您可以在與追蹤相同的區域中建立日誌群組或選擇現有的日誌群組。

   > **Note**
   >
   > 套用至所有區域的追蹤會將所有區域的記錄檔傳送至您指定的 CloudWatch 記錄日誌群組。

4. 在CloudWatch 記錄檔中，選擇編輯。
5. 針對CloudWatch 記錄檔，選擇已啟動。
6. 對於日誌群組名稱，選擇新增以建立新的日誌群組，或選擇現有以使用現有的日誌群組。如果選擇 [新增]，請為您 CloudTrail 指定新記錄群組的名稱，或者輸入名稱。如需有關命名的詳細資訊，請參閱 CloudWatch 的記錄群組和記錄資料流命名 CloudTrail。

7. 如果選擇 Existing (現有)，請從下拉式清單中選擇日誌群組。
8. 對於 [角色名稱]，選擇 [新增]，為許可建立新的 IAM 角色，以將記錄傳送至 CloudWatch 記錄。選擇 Existing (現有) 從下拉式功能表中選擇現有的 IAM 角色。新角色或現有角色的政策陳述式會在您展開政策文件時顯示。如需有關此角色的詳細資訊，請參閱 使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件。

   > **Note**
   >
   > 設定追蹤時，您可以選擇由其他帳戶所屬的 S3 儲存貯體和 SNS 主題。不過，如果您想 CloudTrail 要將事件傳遞至 CloudWatch 記錄檔記錄群組，則必須選擇目前帳戶中存在的記錄群組。

9. 選擇儲存變更。

指定 IAM 角色

您可以指定 CloudTrail 要假設將事件傳遞至記錄串流的角色。

指定角色

1. 預設會為您指定 `CloudTrail_CloudWatchLogs_Role`。預設角色原則具有在您指定的 CloudWatch 記錄群組中建立記錄資料流的必要權限，並將 CloudTrail 事件傳遞至該記錄資料流。

   > **Note**
   >
   > 如果希望此角色用於組織線索的日誌群組，您必須在角色建立之後手動修改該政策。如需更多詳細資訊，請參閱這個政策範例與建立組織追蹤。

   a. 若要驗證角色，請前往 https://console.aws.amazon.com/iam/ 的 AWS Identity and Access Management 主控台。
   b. 選擇 [角色]，然後選擇 [CloudTrailCloudWatchLogs_ 角色]。
   c. 在許可索引標籤中，展開政策以檢視其內容。
2. 您可以指定其他角色，但如果您想要使用該角色將事件傳送至 CloudWatch 記錄檔，則必須將必要的角色原則附加至現有角色。如需詳細資訊，請參閱 使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件。

在 CloudWatch 主控台中檢視事件

將追蹤設定為將事件傳送至 CloudWatch 記錄檔記錄群組後，您可以在 CloudWatch 主控台中檢視事件。 CloudTrail 通常會在 API 呼叫後平均約 5 分鐘內將事件傳遞至您的記錄群組。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。

若要在 CloudWatch 主控台中檢視事件

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在左側導覽窗格中，選擇日誌下方的日誌群組。
3. 選擇您為線索指定的日誌群組。
4. 選擇您要檢視的日誌串流。
5. 若要查看線索所記錄的事件詳細資訊，請選擇事件。

> **Note**
>
> CloudWatch 主控台中的 [時間 (UTC)] 欄會顯示事件傳遞至記錄群組的時間。若要查看事件記錄的實際時間 CloudTrail，請參閱`eventTime`欄位。

設定 CloudWatch 記錄監控 AWS CLI

您可以使用 AWS CLI 來設定將事件傳送 CloudTrail 至 CloudWatch 記錄檔以進行監視。

建立日誌群組

1. 如果您沒有現有的記錄群組，請使用 [CloudWatch 記錄檔] `create-log-group` 命令建立記錄檔群組做為 CloudWatch 記錄事件的傳遞端點。

   ```
   aws logs create-log-group --log-group-name name
   ```

   下列範例會建立名為 `CloudTrail/logs` 的日誌群組：

   ```
   aws logs create-log-group --log-group-name CloudTrail/logs
   ```

2. 擷取日誌群組的 Amazon Resource Name (ARN)。

   ```
   aws logs describe-log-groups
   ```

建立角色

建立可讓其將事件傳送至 CloudWatch 記錄檔記錄群組的角色。 CloudTrail IAM `create-role` 命令需要兩個參數：角色名稱及 JSON 格式之擔任角色政策文件的檔案路徑。您使用的政策文件會授與`AssumeRole`權限 CloudTrail。`create-role` 命令會建立具備必要許可的角色。

若要建立包含政策文件的 JSON 檔案，請開啟文字編輯器，然後將下列政策內容儲存在名為 `assume_role_policy_document.json` 的檔案中。

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

執行下列命令以建立具有`AssumeRole`權限的角色 CloudTrail。

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

當命令完成時，記下輸出中的角色 ARN。

建立政策文件

建立的下列角色原則文件 CloudTrail。本文件授與 CloudTrail 在您指定的 CloudWatch 記錄群組中建立記錄資料流所需的權限，並將 CloudTrail 事件傳遞至該記錄串流。

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
```

```
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

將政策文件儲存在名為 role-policy-document.json 的檔案中。

如果您正在建立也可用於組織線索的政策，您將需要做出稍微有些差異的設定。*######### CloudTrail ############## CloudWatch ################## 111111111111 ######## ## 111111111111 AWS ########## (ID # o-exampleorgid) ###### CloudTrail ############## AWS Organizations*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
```

```
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

如需組織線索的詳細資訊，請參閱建立組織追蹤。

執行下列命令將政策套用到角色。

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

更新線索

使用 CloudTrailupdate-trail命令更新記錄檔群組和角色資訊。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

若要取得有關 AWS CLI 指令的更多資訊，請參閱〈指AWS CloudTrail 令行參考〉。

限制

CloudWatch 記錄檔和 EventBridge 每個記錄檔都允許 256 KB 的事件大小上限。雖然大多數服務事件的大小上限為 256 KB，但有些服務仍有較大的事件。 CloudTrail 不會將這些事件傳送至 CloudWatch 記錄檔或 EventBridge。

從 CloudTrail 事件版本 1.05 開始，事件的大小上限為 256 KB。這是為了防止惡意行為者利用，並允許其他 AWS 服務（例如 CloudWatch Logs 和 EventBridge.

建立 CloudTrail 事件 CloudWatch 警示：範例

本主題說明如何設定 CloudTrail 事件警示，並包含範例。

主題

必要條件

您必須執行下列作業，才能使用此主題中的範例：

- 使用主控台或 CLI 建立追蹤記錄。
- 建立日誌群組，您可以在建立線索的過程中執行此動作。如需建立線索的詳細資訊，請參閱 建立追蹤。
- 指定或建立 IAM 角色，以授 CloudTrail 與權限，以便在您指定的CloudWatch 日誌群組中建立日誌記錄串流，並將 CloudTrail 事件傳遞至該日誌串流。預設 `CloudTrail_CloudWatchLogs_Role` 會為您妥善處理。

如需詳細資訊，請參閱 將事件傳送至 CloudWatch 記錄檔。本節中的範例會在 Amazon CloudWatch 日誌主控台中執行。有關如何建立指標篩選器和警示的詳細資訊，請參閱 Amazon 使用者指南中的使用篩選器從日誌事件建立指標和使 CloudWatch 用 Amazon CloudWatch 警示。

建立指標篩選條件並建立警示

若要建立警示，您必須先建立指標篩選條件，然後根據篩選條件來設定警示。所有範例都會顯示此程序。如需有關日誌事件指標篩選器和模式語法的詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的篩選器和模式語法 JSON 相關章節。 CloudTrail

範例：安全群組組態變更

遵循此程序建立 Amazon CloudWatch 警示，該警示會在安全群組上發生組態變更時觸發。

建立指標篩選條件

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇日誌下方的日誌群組。
3. 在日誌群組清單中，選擇您針對追蹤所建立之日誌群組。
4. 在指標篩選條件或動作選單中，選擇建立指標篩選條件。
5. 在 Define pattern (定義陣列) 頁面的 建立篩選條件模式，請針對篩選條件模式輸入以下內容。

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. 在 Test pattern (測試模式)，保留預設值。選擇 Next (下一步)。
7. 在指派指標頁面的篩選條件名稱中，輸入 **SecurityGroupEvents**。
8. 在指標詳細資訊中，開啟建立新的，然後針對指標命名空間輸入 **CloudTrailMetrics**。
9. 在指標名稱中，輸入 **SecurityGroupEventCount**。
10. 在指標值中，輸入 **1**。
11. 保留 Default value (預設值) 空白。
12. 選擇 Next (下一步)。
13. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Create metric filter (建立指標篩選條件) 以建立篩選條件，或選擇 Edit (編輯) 返回並變更值。

建立警示

建立量度篩選後，會開啟 CloudTrail 追蹤 CloudWatch 記錄群組的「記錄檔群組詳細資料」頁面。請依照此程序來建立警示。

1. 在指標篩選條件索引標籤上，尋找您在 the section called “建立指標篩選條件” 中建立的指標篩選條件。填入指標篩選條件的核取方塊。在 Metric filters (指標篩選條件) 列，選擇 Create alarm (建立警示)。

2. 在指定指標和條件中，輸入以下內容。

   a. 針對 Graph (圖形)，根據您在建立警示時所做的其他設定，該行被設置為 **1**。

   b. 針對 Metric name (指標名稱)，請保留目前的指標名稱**SecurityGroupEventCount**。

   c. 針對 Statistic (統計數字)，保留預設值。**Sum**。

   d. 針對 Period (期間)，保留預設值。**5 minutes**。

   e. 在 Conditions (條件) 中，針對 Threshold type (閾值類型)，選擇 Static (靜態)。

   f. 針對無論何時 ***metric_name*** 為 ，選擇 Greater/Equal (大於/等於)。

   g. 對於閾值，輸入 **1**。

   h. 在 Additional configuration (其他組態) 中，保留預設值。選擇 Next (下一步)。

3. 在 [設定動作] 頁面上，選擇 [通知]，然後選擇 [在警示中]，這表示當超過 5 分鐘內 1 個變更事件的臨界值且SecurityGroupEventCount處於警示狀態時，會採取動作。

   a. 對於將通知傳送至下列 SNS 主題，選擇建立新主題。

   b. 輸入 **SecurityGroupChanges_CloudWatch_Alarms_Topic** 作為新 Amazon SNS 主題的名稱。

   c. 在將接收通知的電子郵件端點中，輸入您要在發出此警示時接收通知的使用者電子郵件地址。以逗號分隔電子郵件地址。

      每個電子郵件收件者會收到電子郵件，要求他們確認是否要訂閱 Amazon SNS 主題。

   d. 請選擇建立主題。

4. 在此範例中，略過其他動作類型。選擇 Next (下一步)。

5. 在 Add name and description (新增名稱和說明) 頁面中，輸入警示的易記名稱和說明。在此範例中，請輸入 **Security group configuration changes** 作為名稱，**Raises alarms if security group configuration changes occur** 作為說明。選擇 Next (下一步)。

6. 在 Preview and create (預覽和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 來進行變更，或者選擇 Create alarm (建立警示) 來建立警示。

   建立鬧鐘後， CloudWatch 開啟 [警示] 頁面。警示 Actions (動作) 欄位顯示 Pending confirmation (等待確認)，直到 SNS 主題上的所有電子郵件收件者都確認他們想要訂閱 SNS 通知。

AWS Management Console 登入失敗範例

依照此程序建立 Amazon CloudWatch 警示，該警示會在五分鐘內發生三次以上 AWS Management Console 登入失敗時觸發。

建立指標篩選條件

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇日誌下方的日誌群組。
3. 在日誌群組清單中，選擇您針對追蹤所建立之日誌群組。
4. 在指標篩選條件或動作選單中，選擇建立指標篩選條件。
5. 在 Define pattern (定義陣列) 頁面的 建立篩選條件模式，請針對篩選條件模式輸入以下內容。

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. 在 Test pattern (測試模式)，保留預設值。選擇 Next (下一步)。
7. 在指派指標頁面的篩選條件名稱中，輸入 **ConsoleSignInFailures**。
8. 在指標詳細資訊中，開啟建立新的，然後針對指標命名空間輸入 **CloudTrailMetrics**。
9. 在指標名稱中，輸入 **ConsoleSigninFailureCount**。
10. 在指標值中，輸入 **1**。
11. 保留 Default value (預設值) 空白。
12. 選擇 Next (下一步)。
13. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Create metric filter (建立指標篩選條件) 以建立篩選條件，或選擇 Edit (編輯) 返回並變更值。

建立警示

建立量度篩選後，會開啟 CloudTrail追蹤 CloudWatch 記錄群組的「記錄檔群組詳細資料」頁面。請依照此程序來建立警示。

1. 在指標篩選條件索引標籤上，尋找您在 the section called “建立指標篩選條件” 中建立的指標篩選條件。填入指標篩選條件的核取方塊。在 Metric filters (指標篩選條件) 列，選擇 Create alarm (建立警示)。
2. 在 Create Alarm (建立警示) 頁面的 Specify metric and conditions (指定指標和條件) 中，輸入下列內容。

   a. 針對 Graph (圖形)，根據您在建立警示時所做的其他設定，該行被設置為 **3**。
   b. 針對 Metric name (指標名稱)，請保留目前的指標名稱**ConsoleSigninFailureCount**。
   c. 針對 Statistic (統計數字)，保留預設值。**Sum**。
   d. 針對 Period (期間)，保留預設值。**5 minutes**。

e. 在 Conditions (條件) 中，針對 Threshold type (閾值類型)，選擇 Static (靜態)。

f. 針對無論何時 ***metric_name*** 為 ，選擇 Greater/Equal (大於/等於)。

g. 對於閾值，輸入 **3**。

h. 在 Additional configuration (其他組態) 中，保留預設值。選擇 Next (下一步)。

3. 在 [設定動作] 頁面上，對於 [通知]，選擇 [在警示中]，這表示當超過 5 分鐘內 3 個變更事件的臨界值且ConsoleSigninFailureCount處於警示狀態時，會採取動作。

   a. 對於將通知傳送至下列 SNS 主題，選擇建立新主題。

   b. 輸入 **ConsoleSignInFailures_CloudWatch_Alarms_Topic** 作為新 Amazon SNS 主題的名稱。

   c. 在將接收通知的電子郵件端點中，輸入您要在發出此警示時接收通知的使用者電子郵件地址。以逗號分隔電子郵件地址。

      每個電子郵件收件者會收到電子郵件，要求他們確認是否要訂閱 Amazon SNS 主題。

   d. 請選擇建立主題。

4. 在此範例中，略過其他動作類型。選擇 Next (下一步)。

5. 在 Add name and description (新增名稱和說明) 頁面中，輸入警示的易記名稱和說明。在此範例中，請輸入 **Console sign-in failures** 作為名稱，**Raises alarms if more than 3 console sign-in failures occur in 5 minutes** 作為說明。選擇 Next (下一步)。

6. 在 Preview and create (預覽和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 來進行變更，或者選擇 Create alarm (建立警示) 來建立警示。

   建立鬧鐘後， CloudWatch 開啟 [警示] 頁面。警示 Actions (動作) 欄位顯示 Pending confirmation (等待確認)，直到 SNS 主題上的所有電子郵件收件者都確認他們想要訂閱 SNS 通知。

範例：IAM 政策變更

按照此程序建立 Amazon CloudWatch 警示，該警示會在進行 API 呼叫以變更 IAM 政策時觸發。

建立指標篩選條件

1. 開啟主 CloudWatch 控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在導覽窗格中，選擇日誌。
3. 在日誌群組清單中，選擇您針對追蹤所建立之日誌群組。
4. 選擇 Actions (動作)，然後選擇 Create metric filter (建立指標篩選條件)。

5. 在 Define pattern (定義陣列) 頁面的 建立篩選條件模式，請針對篩選條件模式輸入以下內容。

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. 在 Test pattern (測試模式)，保留預設值。選擇 Next (下一步)。
7. 在指派指標頁面的篩選條件名稱中，輸入 **IAMPolicyChanges**。
8. 在指標詳細資訊中，開啟建立新的，然後針對指標命名空間輸入 **CloudTrailMetrics**。
9. 在指標名稱中，輸入 **IAMPolicyEventCount**。
10. 在指標值中，輸入 **1**。
11. 保留 Default value (預設值) 空白。
12. 選擇 Next (下一步)。
13. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Create metric filter (建立指標篩選條件) 以建立篩選條件，或選擇 Edit (編輯) 返回並變更值。

建立警示

建立量度篩選後，會開啟 CloudTrail追蹤 CloudWatch 記錄群組的「記錄檔群組詳細資料」頁面。請依照此程序來建立警示。

1. 在指標篩選條件索引標籤上，尋找您在 the section called “建立指標篩選條件” 中建立的指標篩選條件。填入指標篩選條件的核取方塊。在 Metric filters (指標篩選條件) 列，選擇 Create alarm (建立警示)。
2. 在 Create Alarm (建立警示) 頁面的 Specify metric and conditions (指定指標和條件) 中，輸入下列內容。
   a. 針對 Graph (圖形)，根據您在建立警示時所做的其他設定，該行被設置為 **1**。
   b. 針對 Metric name (指標名稱)，請保留目前的指標名稱**IAMPolicyEventCount**。
   c. 針對 Statistic (統計數字)，保留預設值。**Sum**。
   d. 針對 Period (期間)，保留預設值。**5 minutes**。

e. 在 Conditions (條件) 中，針對 Threshold type (閾值類型)，選擇 Static (靜態)。

f. 針對無論何時 ***metric_name*** 為 ，選擇 Greater/Equal (大於/等於)。

g. 對於閾值，輸入 **1**。

h. 在 Additional configuration (其他組態) 中，保留預設值。選擇 Next (下一步)。

i.

3. 在 [設定動作] 頁面上，對於 [通知]，選擇 [在警示中]，這表示當超過 5 分鐘內 1 個變更事件的閾值，且 IAM 處PolicyEventCount於警示狀態時，會採取動作。

   a. 對於將通知傳送至下列 SNS 主題，選擇建立新主題。

   b. 輸入 **IAM_Policy_Changes_CloudWatch_Alarms_Topic** 作為新 Amazon SNS 主題的名稱。

   c. 在將接收通知的電子郵件端點中，輸入您要在發出此警示時接收通知的使用者電子郵件地址。以逗號分隔電子郵件地址。

      每個電子郵件收件者會收到電子郵件，要求他們確認是否要訂閱 Amazon SNS 主題。

   d. 請選擇建立主題。

4. 在此範例中，略過其他動作類型。選擇 Next (下一步)。

5. 在 Add name and description (新增名稱和說明) 頁面中，輸入警示的易記名稱和說明。在此範例中，請輸入 **IAM Policy Changes** 作為名稱，**Raises alarms if IAM policy changes occur** 作為說明。選擇 Next (下一步)。

6. 在 Preview and create (預覽和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 來進行變更，或者選擇 Create alarm (建立警示) 來建立警示。

   建立鬧鐘後， CloudWatch 開啟 [警示] 頁面。警示 Actions (動作) 欄位顯示 Pending confirmation (等待確認)，直到 SNS 主題上的所有電子郵件收件者都確認他們想要訂閱 SNS 通知。

設定 CloudWatch 記錄警示的通知

您可以將 CloudWatch Logs 設定為在觸發警示時傳送通知 CloudTrail。這樣做可讓您快速回應在事件中擷取並由 CloudWatch 記錄偵測到的關鍵操作 CloudTrail事件。 CloudWatch 使用 Amazon Simple Notification Service (SNS) 來傳送電子郵件。如需詳細資訊，請參閱CloudWatch 使用者指南中的設定 Amazon SNS 通知。

停 CloudTrail 止將事件傳送至 CloudWatch 記錄檔

您可以更新追蹤以停用 CloudWatch 日誌設定，以停止將 AWS CloudTrail 事件傳送至 Amazon CloudWatch 日誌。

停止將事件傳送至 CloudWatch 記錄檔（主控台）

停止將 CloudTrail 事件傳送至 CloudWatch 記錄檔

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 在導覽窗格中，選擇 Trails (追蹤記錄)。
3. 選擇您要停用 CloudWatch 記錄檔整合的追蹤名稱。
4. 在CloudWatch 記錄檔中，選擇編輯。
5. 清除 Enabled (已啟用) 核取方塊。
6. 選擇儲存變更。

停止將事件傳送至 CloudWatch 記錄檔 (CLI)

您可以執行update-trail命令，將 CloudWatch 記錄檔記錄群組做為傳遞端點移除。下列命令會將日誌群組 ARN 和 Logs 角色 ARN 的值取代為空白值，以清除追蹤組態中的 CloudWatch 記錄群組和角色。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch 的記錄群組和記錄資料流命名 CloudTrail

Amazon CloudWatch 會顯示您為 CloudTrail 事件建立的日誌群組，以及您在區域中擁有的任何其他日誌群組。建議您使用日誌群組名稱，協助您輕鬆地區別不同的日誌群組。例如 **`CloudTrail/logs`**。

命名日誌群組時，請遵循以下準則：

- 日誌群組的名稱在 AWS 帳戶的區域中必須是唯一的。
- 日誌群組的名稱長度可介於 1 到 512 個字元之間。
- 日誌群組名稱包含下列字元：a-z、A-Z、0-9、'_' (底線)、'-' (連字號)、'/' (斜線)、'.' (句號) 和 '#' (數字符號)。

 # CloudTrail ################################## _ CloudTrail _ trail_ # ##

> **Note**
>
> 如果記 CloudTrail 錄量很大，可能會建立多個記錄串流，將記錄資料傳送至您的記錄群組。*## ################ CloudTrail ############### _ _ trail _ ## CloudTrail _ ###*

如需有關日 CloudWatch 誌群組的詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南和 Amazon 日誌API 參考CreateLogGroup中的使用日誌群組和 CloudWatch 日誌串流。

使用 CloudWatch 記錄進行監視 CloudTrail 的角色原則文件

本節說明將記錄事件傳送至 CloudWatch 記錄檔之 CloudTrail 角色所需的權限原則。當您設定傳送事件時，您可以將原則文件附加 CloudTrail 至角色，如中所述將事件傳送至 CloudWatch 記錄檔。您也可以使用 IAM 建立角色。如需詳細資訊，請參閱建立角色以委派許可給某個 AWS 服務或建立 IAM 角色 (AWS CLI)。

下列範例原則文件包含在您指定的記錄群組中建立 CloudWatch 記錄資料流所需的權限，以及將 CloudTrail 事件傳遞至美國東部 (俄亥俄) 區域的該記錄資料流所需的權限。(這是用於預設 IAM 角色 `CloudTrail_CloudWatchLogs_Role` 的預設政策。)

> **Note**
>
> 混淆副預防不適用於 CloudWatch 記錄監視的角色策略。角色原則不支援使用`aws:SourceArn`和`aws:SourceAccount`。

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
```

```
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

如果您建立可能也會用於組織線索的政策，則您將需要從該角色原已建的預設政策中開始修改。*###### #### CloudTrail ###### log_group_name ## CloudWatch ########################## ## 111111111111 ################ 111111111111 AWS ########### CloudTrail## ########## AWS Organizations*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        },
        {
```

```
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

如需組織線索的詳細資訊，請參閱建立組織追蹤。

從多個帳戶接收 CloudTrail 日誌文件

您可以將多個日誌檔 CloudTrail 交付 AWS 帳戶 到單一 Amazon S3 儲存貯體。例如，您有四個 AWS 帳戶 帳戶識別碼 1111111111、2222222222、333333333333 和 4444444444，而且您想要設定為將這四個帳戶的記錄檔傳遞至屬於帳戶 1111111111 的值區。 CloudTrail 為了達成這個目標，請依序完成下列步驟：

1. 在目的地儲存貯體所屬的帳戶 (在此範例中為 111111111111) 中建立追蹤。此時不要為任何其他帳戶建立追蹤。

   如需說明，請參閱在主控台中建立追蹤。

2. 更新目標值區上的儲存貯體政策，以授與跨帳戶權限。 CloudTrail

   如需說明，請參閱設定多帳戶的儲存貯體政策。

3. 在您想要記錄其活動的其他帳戶 (在此範例中為 222222222222、333333333333 和 444444444444) 中建立追蹤。當在每個帳戶中建立追蹤時，請指定屬於您在步驟 1 中指定之帳戶 (在此範例中為 111111111111) 的 Amazon S3 儲存貯體。如需說明，請參閱在其他帳戶中建立追蹤。

> **Note**
>
> 如果您選擇啟用 SSE-KMS 加密，KMS 金鑰原則必須允許 CloudTrail 使用金鑰來加密記錄檔，並允許您指定的使用者以未加密格式讀取記錄檔。如需手動編輯金鑰政策的資訊，請參閱「設定 AWS KMS 金鑰原則 CloudTrail」。

編輯其他帳戶呼叫之資料事件的儲存貯體擁有者帳戶 ID

從歷史上看，如果在 Amazon S3 CloudTrail 資料事件 API 呼叫者中啟用了資料事件，則會在資料事件中 CloudTrail 顯示 S3 儲存貯體擁有者的帳戶 ID (例如`PutObject`)。 AWS 帳戶 即使儲存貯體擁有者帳戶沒有啟用 S3 資料事件，仍會發生此情況。

現在，如果符合下列兩個條件，則 CloudTrail 移除`resources`區塊中 S3 儲存貯體擁有者的帳戶 ID：

- 資料事件 API 呼叫的來自不同 AWS 帳戶 於 Amazon S3 儲存貯體擁有者。
- API 呼叫者收到僅適用於呼叫者帳戶的 `AccessDenied` 錯誤。

進行 API 呼叫的資源的擁有者仍然收到完整的事件。

以下事件記錄片段為預期行為的範例。在 `Historic` 片段中，S3 儲存貯體擁有者的帳戶 ID 123456789012 顯示給來自不同帳戶 API 呼叫者。在當前行為範例中，並未顯示儲存貯體擁有者的帳戶 ID。

```
# Historic

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

以下為當前行為。

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

主題

設定多帳戶的儲存貯體政策

若要讓值區從多個帳號接收記錄檔，其值區政策必須 CloudTrail 授與從您指定的所有帳號寫入記錄檔的權限。這表示您必須修改目標儲存貯體上的儲存貯體政策，以 CloudTrail 授與從每個指定帳戶寫入記錄檔的權限。

> **Note**
>
> 基於安全理由，未經授權的使用者無法建立包含 `AWSLogs/` 作為 `S3KeyPrefix` 參數的追蹤。

修改儲存貯體許可，以便從多個帳戶接收檔案

1. AWS Management Console 使用擁有儲存貯體的帳戶登入 (本範例中為 1111111111)，然後開啟 Amazon S3 主控台。
2. 選擇提 CloudTrail 供記錄檔的值區，然後選擇 [權限]。
3. 對於 Bucket policy (儲存貯體政策)，選擇 Edit (編輯)。
4. 修改現有的政策，為每個想要將其日誌檔案交付到這個儲存貯體的其他帳戶新增程式碼。請參閱下列範例政策，並注意指定第二個帳戶 ID 加底線的 `Resource` 行。安全最佳實務是將

aws:SourceArn 條件金鑰新增至 Amazon S3 儲存貯體政策。這有助於防止未經授權存取您的 S3 儲存貯體。如果您具有現有的線索，請務必新增一或多個條件金鑰。

> **Note**
>
> AWS 帳戶 ID 是十二位數字，包括前導零。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
              "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
            ]
          }
       }
    },
    {
      "Sid": "AWSCloudTrailWrite20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
        "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": [
```

```
            "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
            "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
          ],
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

在其他帳戶中建立追蹤

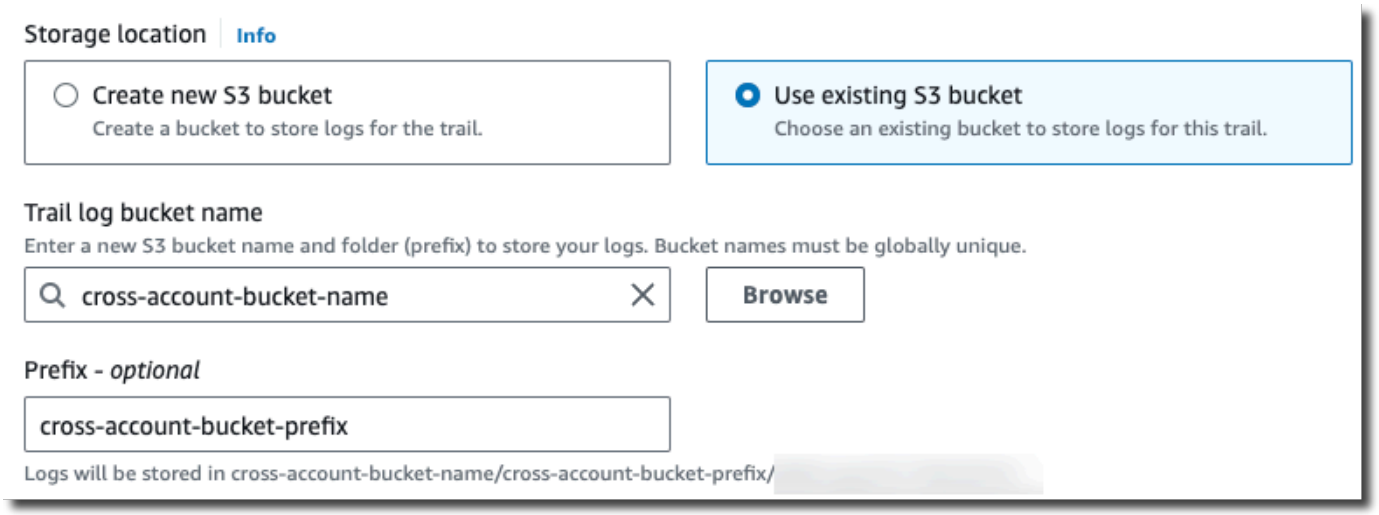
您可以使用主控台或在其他地 AWS CLI 方建立追蹤， AWS 帳戶 並將其日誌檔彙總到一個 Amazon S3 儲存貯體。或者，您可以建立組織追蹤來記錄中組織的所有 AWS 帳戶 組織 AWS Organizations。如需詳細資訊，請參閱 建立組織追蹤。

使用控制台在其他 AWS 帳戶中創建跟踪

您可以使用 CloudTrail 控制台在其他帳戶中創建跟踪。

1. AWS Management Console 使用您要為其建立追蹤的帳戶登入。遵循 在主控台中建立追蹤 中的步驟，使用主控台建立追蹤。
2. 對於 Storage location (儲存位置)，選擇 Use existing S3 bucket (使用現有的 S3 儲存貯體)。使用文字方塊，輸入您用於儲存不同帳戶日誌檔案的儲存貯體的名稱。

> **Note**
>
> 值區政策必須授 CloudTrail 予寫入權限。如需手動編輯儲存貯體政策的資訊，請參閱「設定多帳戶的儲存貯體政策」。



3. 在字首中，輸入您用來儲存不同帳戶日誌檔案的字首。如果您選擇使用與儲存貯體政策中指定的前置詞不同，則必須編輯目的地值區上的值區政策， CloudTrail 以允許使用此新前置詞將記錄檔寫入值區。

使用 CLI 在其他 AWS 帳戶中建立追蹤

您可以使用命 AWS 令列工具在其他帳戶中建立追蹤，並將其日誌檔彙總到一個 Amazon S3 儲存貯體。如需這些工具的詳細資訊，請參閱《AWS CLI 命令參考》中的 cloudtrail。

使用 create-trail 命令建立追蹤，並指定下列內容：

- `--name` 指定線索的名稱。
- `--s3-bucket-name` 指定您用來儲存不同帳戶日誌檔案的 Amazon S3 儲存貯體。
- `--s3-prefix` 指定日誌檔案交付路徑的前綴 (選用)。
- `--is-multi-region-trail`指定此追蹤將記錄您正在使用之分割 AWS 區中所有區域中的事件。

您可以為執行帳號 AWS 資源的每個區域建立一個追蹤。

下列範例命令顯示如何使用 AWS CLI建立其他帳戶的線索。若要將這些帳戶的日誌檔案交付至您在第一個帳戶 (此範例為 111111111111) 中所建立的儲存貯體，請在 `--s3-bucket-name` 選項指定儲存貯體名稱。Amazon S3 儲存貯體名稱是全域唯一的。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail
```

當您執行此命令時，會看到類似下方的輸出：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

若要取得有關使用 AWS 指令行 CloudTrail 工具的更多資訊，請參閱CloudTrail 指令行參考。

在 AWS 帳戶之間共用 CloudTrail 記錄檔

本節說明如何在多個 AWS 帳戶之間共用 CloudTrail 記錄檔。您用來共用日誌的方法 AWS 帳戶 取決於 S3 儲存貯體的組態。共享日誌檔案的選項如下：

- 強制執行的儲存貯體擁有者 – S3 物件擁有權是一項 Amazon S3 儲存貯體層級設定，您可以用來控制上傳至儲存貯體之物件的擁有權，以及停用或啟用存取控制清單 (ACL)。根據預設，物件擁有權設定為強制執行的儲存貯體擁有者設定，而且所有 ACL 都會停用。停用 ACL 時，儲存貯體擁有者會擁有儲存貯體中的所有物件，並使用存取管理政策專門管理對資料的存取。設定強制執行的儲存貯體擁有者選項時，系統會透過儲存貯體政策管理存取權，免除使用者擔任角色的需求。
- 擔任角色以共享日誌檔案 – 如果您尚未選擇強制執行的儲存貯體擁有者設定，使用者將需要擔任角色，才能存取您 S3 儲存貯體中的日誌檔案。

擔任角色以在帳戶之間共享日誌

> **Note**
>
> 本節僅適用於未使用強制執行的儲存貯體擁有者設定的 Amazon S3 儲存貯體。

本節說明如何 AWS 帳戶 透過假定角色在多個 CloudTrail 記錄檔之間共用記錄檔，並說明共用記錄檔的案例。

- 案例 1：將唯讀存取權授予產生日誌檔案 (放置在 Amazon S3 儲存貯體中) 的帳戶。

- 案例 2：將您 Amazon S3 儲存貯體中所有日誌檔案的存取權，授予可為您分析日誌檔案的第三方帳戶。

若要授與 Amazon S3 儲存貯體中日誌檔案的唯讀存取權

1. 為每個要共享日誌檔案的帳戶建立 IAM 角色。您必須是管理員才能授予許可。

   當您建立角色時，請執行下列操作：

   - 選擇其他 AWS 帳戶選項。
   - 輸入要授予存取權之帳戶的 12 位數帳戶 ID。
   - 如果您希望使用者先提供多重要素驗證再擔任角色，請勾選 Require MFA (要求 MFA) 核取方塊。
   - 選擇亞馬遜 S3 政策ReadOnlyAccess。

   > **Note**
   >
   > 根據預設，AmazonS3 ReadOnlyAccess 政策會授予您帳戶內所有 Amazon S3 儲存貯體的擷取和清單權限。

   如需 IAM 角色之許可管理的詳細資訊，請參閱 IAM 使用者指南中的 IAM 角色。
2. 建立存取政策，以將唯讀存取權授予您要共享日誌檔案的帳戶。
3. 指示每個帳戶擔任角色以擷取日誌檔案。

若要將日誌檔案的唯讀存取權授予第三方帳戶

1. 為每個要共享日誌檔案的第三方帳戶建立 IAM 角色。您必須是管理員才能授予許可。

   當您建立角色時，請執行下列操作：

   - 選擇其他 AWS 帳戶選項。
   - 輸入要授予存取權之帳戶的 12 位數帳戶 ID。
   - 輸入外部 ID，提供誰可以擔任該角色的額外控制。如需詳細資訊，請參閱 IAM 使用者指南中的將 AWS 資源存取權授予第三方時如何使用外部 ID。
   - 選擇亞馬遜 S3 政策ReadOnlyAccess。

> **Note**
>
> 根據預設，AmazonS3 ReadOnlyAccess 政策會授予您帳戶內所有 Amazon S3 儲存貯體的擷取和清單權限。

2. 建立存取政策，以將唯讀存取權授予您要共享日誌檔案的第三方帳戶。
3. 指示第三方帳戶擔任角色以擷取日誌檔案。

下列各節將詳細說明這些步驟。

主題

- 建立存取政策將存取權授予您擁有的帳戶
- 建立存取政策將存取權授予第三方
- 擔任角色
- 停止在 AWS 帳戶之間共用 CloudTrail 記錄檔

建立存取政策將存取權授予您擁有的帳戶

身為 Amazon S3 儲存貯體擁有者，您可以完全控制為其他帳戶 CloudTrail 寫入日誌檔的 Amazon S3 儲存貯體。您想將每個業務單位的日誌檔案與建立這些檔案的業務單位共享。但是，您不希望某個單位能夠讀取任何其他單位的日誌檔案。

例如，若要將帳戶 B 的日誌檔案與帳戶 B 共享，但不與帳戶 C 共享，您必須在您的帳戶中建立新的 IAM 角色，指定帳戶 B 是信任帳戶。這個角色信任政策會指定帳戶 B 受到信任，可擔任您帳戶建立的角色，並應類似下列範例所示。如果您使用主控台建立角色，系統會自動建立信任政策。如果您使用開發套件建立角色，您必須將信任政策做為參數提供給 `CreateRole` API。如果您使用 CLI 建立角色，您必須在 `create-role` CLI 命令中指定信任政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
```

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

您還必須建立存取政策，指定帳戶 B 只能從 B 寫入其日誌檔案的位置讀取。存取政策會類似下列內容所示。請注意，當您在 CloudTrail 彙總過程中為帳號 B 開啟時，資源 ARN 包含帳號 B 的十二位數帳號 ID，以及您指定的首碼 (如果有的話)。如需指定前綴的詳細資訊，請參閱「在其他帳戶中建立追蹤」。

> **Important**
>
> 您必須確保存取政策中的前置碼與您為帳戶 B 開啟時指定的前置詞完全相同。如果不是，則必須編輯帳戶中的 IAM 角色存取政策，以納入帳戶 B 的實際前置詞。如果角色存取政策中的前置詞與您在 B CloudTrail 中開啟時指定的前置詞不完全相同，則帳戶 B 將無法存取其記錄檔。CloudTrail

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

為任何其他帳戶執行上述程序。

在您為每個帳戶建立角色並指定適當的信任和存取政策之後，以及在該帳戶的管理員為每個帳戶的 IAM 使用者授予存取權之後，帳戶 B 或 C 中的 IAM 使用者就可以透過程式設計方式擔任此角色。

如需詳細資訊，請參閱 擔任角色。

建立存取政策將存取權授予第三方

您必須為第三方帳戶建立個別的 IAM 角色。當您建立角色時， AWS 會自動建立信任關係，該關係指定第三方帳戶受到信任，可以擔任該角色。角色的存取政策指定該帳戶可採取的動作。如需建立角色的詳細資訊，請參閱建立 IAM 角色。

例如，由建立的信任關係 AWS 指定第三方帳戶 (在此範例中為帳戶 Z) 受信任，以承擔您所建立的角色。信任政策範例如下：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole"
    }]
}
```

如果為第三方帳戶建立角色時指定了外部 ID，您的存取政策會包含新增的 Condition 元素，用於測試該帳戶指派的唯一 ID。此測試會在擔任角色時執行。下列範例存取政策具有 Condition 元素。

如需詳細資訊，請參閱 IAM 使用者指南中的將 AWS 資源存取權授予第三方時如何使用外部 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-
account-Z"}}
```

```
    }]
}
```

您也必須為自己的帳戶建立存取政策，以指定第三方帳戶可以從 Amazon S3 儲存貯體讀取所有日誌。存取政策應該會類似下列範例。Resource 值結尾的萬用字元 (*) 表示第三方帳戶可以存取 S3 儲存貯體中已授予存取權的任何日誌檔案。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

在您為第三方帳戶建立角色並指定適當的信任關係和存取政策之後，第三方帳戶中的 IAM 使用者必須透過程式設計方式擔任該角色，才能從儲存貯體讀取日誌檔案。如需詳細資訊，請參閱 擔任角色。

擔任角色

您必須指定單獨的 IAM 使用者來擔任您在每個帳戶中建立的每個角色。然後，您必須確定每個 IAM 使用者均有適當許可。

IAM 使用者和角色

建立必要的角色和政策後，您必須在每個要共享檔案的帳戶中指定 IAM 使用者。每個 IAM 使用者透過編寫程式的方式擔任適當角色，藉此存取日誌檔案。當使用者擔任角色時， AWS 會將暫時安全憑證傳

回給該使用者。然後，他們可以提出請求以根據透過與該角色相關聯的存取政策所授予的許可來列出、擷取、複製或刪除日誌檔案。

如需有關使用 IAM 身分的詳細資訊，請參閱 IAM 身分 (使用者、使用者群組和角色)。

主要差異在於針對每個案例中各個 IAM 角色所建立的存取政策。

- 在案例 1 中，存取政策會限制每個帳戶只能讀取其專屬日誌檔案。如需詳細資訊，請參閱 建立存取政策將存取權授予您擁有的帳戶。
- 在案例 2 中，存取政策可讓第三方讀取 Amazon S3 儲存貯體中彙整的所有日誌檔案。如需詳細資訊，請參閱 建立存取政策將存取權授予第三方。

建立 IAM 使用者的許可政策

若要執行角色允許的動作，IAM 使用者必須具有呼叫 AWS STS `AssumeRole`API 的權限。您必須編輯每個使用者的政策，以將適當的許可授予他們。為此，您在連接至 IAM 使用者的政策中設定資源元素。下列範例顯示另一個帳戶中 IAM 使用者的政策，可讓使用者擔任帳戶 A 先前所建立且名為 `Test` 的角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

編輯客戶受管政策 (主控台)

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇 Policies (政策)。
3. 在政策清單中，選擇要編輯的政策的政策名稱。您可以使用搜尋方塊來篩選政策清單。
4. 選擇許可索引標籤，然後選擇編輯。
5. 執行以下任意一項：

- 選擇視覺化選項可變更政策，且無需了解 JSON 語法。您可以變更政策中每個許可區塊的服務、動作、資源或可選條件。您也可以匯入政策以在政策底部新增其他許可。完成變更後，選擇下一步以繼續。
- 選擇 JSON 選項，可透過在 JSON 文字方塊中輸入或貼上文字來修改政策。您也可以匯入政策以在政策底部新增其他許可。解決政策驗證期間產生的任何安全性警告、錯誤或一般性警告，然後選擇 Next (下一步)。

> **Note**
>
> 您可以隨時切換視覺化與 JSON 編輯器選項。不過，如果您進行變更或在視覺化編輯器中選擇下一步，IAM 就可能會調整您的政策結構，以便針對視覺化編輯器進行最佳化。如需詳細資訊，請參閱 IAM 使用者指南中的調整政策結構。

6. 在檢視與儲存頁面上，檢視此政策中定義的許可，然後選擇儲存變更以儲存工作。
7. 如果受管政策有最多五個版本，選擇儲存變更可顯示一個對話方塊。若要儲存新版本，該政策的最舊非預設版本會遭到移除，並以此新版本取代之。您也可以將新版本設定為預設的政策版本。

   選擇儲存變更，可儲存新的政策版本。

呼叫 AssumeRole

使用者可以透過建立呼叫 AWS STS `AssumeRole`API 並傳遞角色工作階段名稱的應用程式、要承擔的 Amazon 資源編號 (ARN) 以及選用的外部 ID 來擔任角色。角色工作階段名稱是由建立要擔任之角色的帳戶所定義。外部 ID (如果有的話) 是由第三方帳戶所定義，並在建立角色期間傳遞至擁有帳戶以進行併入。如需詳細資訊，請參閱 IAM 使用者指南中的將 AWS 資源存取權授予第三方時如何使用外部 ID。您可以開啟 IAM 主控台，從帳戶 A 擷取 ARN。

使用 IAM 主控台尋找帳戶 A 中的 ARN 值

1. 選擇 Roles (角色)
2. 選擇您想要檢查的角色。
3. 在 Summary (摘要) 區段中，尋找 Role ARN (角色 ARN)。

AssumeRole API 會傳回用來存取擁有帳戶中資源的臨時登入資料。在此範例中，您想存取的資源是 Amazon S3 儲存貯體，以及儲存貯體中包含的日誌檔案。暫時登入資料具有您在角色存取政策中定義的許可。

下列 Python 範例 (使用 AWS SDK for Python (Boto)) 顯示如何呼叫 AssumeRole 以及如何使用所傳回的暫時安全登入資料列出帳戶 A 所控制的所有 Amazon S3 儲存貯體。

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
```

```
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

停止在 AWS 帳戶之間共用 CloudTrail 記錄檔

若要停止與其他人共用記錄檔 AWS 帳戶，請刪除您為該帳號建立的角色。如需關於刪除角色的資訊，請參閱刪除角色或執行個體設定檔。

驗證 CloudTrail 記錄檔完整性

若要判斷記錄檔在 CloudTrail 傳送之後是否已修改、刪除或未變更，您可以使用 CloudTrail 記錄檔完整性驗證。此功能以產業標準演算法建置：SHA-256 適用於進行雜湊，而含 RSA 的 SHA-256 適用於進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail 日誌文件而不進行檢測。您可以使用 AWS CLI 來驗證傳 CloudTrail 送檔案的位置中的檔案。

為什麼使用它？

驗證過的日誌檔案對於安全和鑑識調查十分重要。例如，驗證過的日誌檔案可讓您積極宣告日誌檔案本身尚未變更，或該特定使用者登入資料已執行特定 API 活動。記 CloudTrail 錄檔完整性驗證程序也會讓您知道記錄檔是否已遭刪除或變更，或是確定在指定期間內未傳送任何記錄檔到您的帳戶。

運作方式

當您啟用記錄檔完整性驗證時， CloudTrail 會為其提供的每個記錄檔建立雜湊。每小時 CloudTrail 也會建立並傳送參照最後一小時記錄檔的檔案，並包含每個記錄檔的雜湊值。這個檔案稱為摘要檔案。CloudTrail 使用公開金鑰和私密 key pair 的私密金鑰來簽署每個摘要檔案。傳送後，您可以使用公開金鑰來驗證摘要檔案。 CloudTrail 每個密鑰對使用不同的密鑰對 AWS 區域。

摘要檔案會傳送至與您的追蹤相關聯的 Amazon S3 儲存貯體，做為 CloudTrail 日誌檔案。如果您的日誌檔是從所有區域或從多個帳戶傳送到單一 Amazon S3 儲存貯體，則 CloudTrail 會將這些區域和帳戶的摘要檔傳送到同一個儲存貯體。

摘要檔案和日誌檔案會分別放入不同的資料夾。將摘要檔案和日誌檔案區隔可讓您強制執行精細的安全政策，以及允許現有日誌處理解決方案來持續操作，而無需修改。每個摘要檔案也會包含先前摘要檔案

的數位簽章 (如果有的話)。目前摘要檔案的簽章位在摘要檔案 Amazon S3 物件的中繼資料屬性中。如需摘要檔案內容的詳細資訊，請參閱「CloudTrail 摘要檔案結構」。

存放日誌檔案和摘要檔案

您可以將 CloudTrail 日誌檔和摘要檔案安全、持久且經濟實惠地存放在 Amazon S3 或 S3 Glacier 中，無限期。若要強化存放在 Amazon S3 中之摘要檔案的安全性，您可以使用 Amazon S3 MFA Delete。

啟用驗證並驗證檔案

若要啟用記錄檔完整性驗證 AWS Management Console，您可以使用 AWS CLI、或 CloudTrail API。啟用日誌檔完整性驗證允許 CloudTrail 將摘要日誌檔傳遞到 Amazon S3 儲存貯體，但不會驗證檔案的完整性。如需詳細資訊，請參閱 啟用記錄檔完整性驗證 CloudTrail。

若要驗證記 CloudTrail 錄檔的完整性，您可以使用 AWS CLI 或建立自己的解決方案。 AWS CLI 將驗證 CloudTrail 傳送檔案的位置中的檔案。如果您想要驗證已移至不同位置的日誌 (在 Amazon S3 或其他位置中)，則可建立自己的驗證工具。

如需使用驗證記錄檔的資訊 AWS CLI，請參閱驗證 CloudTrail 記錄檔完整性 AWS CLI。如需有關開發 CloudTrail 記錄檔驗證自訂實作的資訊，請參閱 CloudTrail 記錄檔完整性驗證的自訂實作。

啟用記錄檔完整性驗證 CloudTrail

您可以使用 AWS 命令列介面 (AWS CLI) 或 CloudTrail API 來啟用記錄檔完整性驗證。 AWS Management Console CloudTrail 在大約一小時內開始傳遞摘要檔案。

AWS Management Console

若要透過 CloudTrail 主控台啟用記錄檔完整性驗證，請在建立或更新追蹤時，針對 [啟用記錄檔驗證] 選項選擇 [是]。預設會為新的線索啟用這項功能。如需詳細資訊，請參閱 使用主控台建立和更新線索。

AWS CLI

若要啟用記錄檔完整性驗證 AWS CLI，請搭配建立軌跡或更新追蹤命令使用`--enable-log-file-validation`此選項。若要停用日誌檔案完整性驗證，請使用 `--no-enable-log-file-validation` 選項。

範例

下列 update-trail 命令會啟用日誌檔案驗證，並開始將摘要檔案交付到指定線索的 Amazon S3 儲存貯體。

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

若要透過 CloudTrail API 啟用記錄檔完整性驗證，EnableLogFileValidation請在呼叫CreateTrail或true時將要求參數設定為UpdateTrail。

如需詳細資訊，請參閱 AWS CloudTrail API 參考UpdateTrail中的CreateTrail和。

驗證 CloudTrail 記錄檔完整性 AWS CLI

若要使用驗證記錄檔 AWS Command Line Interface，請使用 CloudTrail validate-logs指令。此命令會使用交付至您 Amazon S3 儲存貯體的摘要檔案來執行驗證。如需摘要檔案的資訊，請參閱「CloudTrail 摘要檔案結構」。

AWS CLI 可讓您偵測下列類型的變更：

- 修改或刪除 CloudTrail 記錄檔
- 修改或刪除 CloudTrail 摘要文件
- 修改或刪除上述兩者

> **Note**
>
> 只會 AWS CLI 驗證摘要檔所參考的記錄檔。如需詳細資訊，請參閱 檢查特定檔案是否由 CloudTrail。

必要條件

若要使用驗證記錄檔完整性 AWS CLI，必須符合下列條件：

- 您必須具有的線上連線 AWS。
- 您必須具有包含摘要和日誌檔案之 Amazon S3 儲存貯體的讀取存取。
- 摘要檔和日誌檔不得從 CloudTrail 交付它們的原始 Amazon S3 位置移動。

> **Note**
>
> 無法使用 AWS CLI驗證已下載至本機磁碟的日誌檔案。如需建立您自己的工具進行驗證的指導方針，請參閱「CloudTrail 記錄檔完整性驗證的自訂實作」。

validate-logs

語法

下列是 validate-logs 的語法。選用參數會以中括號顯示。

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> validate-logs 命令限特定區域使用。您必須指定--region全域選項，以驗證特定記錄檔 AWS 區域。

選項

下列是 validate-logs 的命令列選項。--trail-arn 和 --start-time 選項是必要的。組織追蹤額外需要 --account-id 選項。

--start-time

指定將會驗證在指定的 UTC 時間戳記值或此值之後交付的日誌檔案。範例：2015-01-08T05:21:42Z。

--end-time

選擇性指定將會驗證在指定的 UTC 時間戳記值或此值之前交付的日誌檔案。預設值是目前 UTC 時間 (Date.now())。範例：2015-01-08T12:31:41Z。

> **Note**
>
> 對於指定的時間範圍，validate-logs 命令只會檢查其對應摘要檔案中所參考的日誌檔案。不會檢查 Amazon S3 儲存貯體中的其他日誌檔案。如需詳細資訊，請參閱 檢查特定檔案是否由 CloudTrail。

--s3-bucket

選擇性指定摘要檔案要存放的 Amazon S3 儲存貯體。如果未指定值區名稱，則 AWS CLI 會透過呼叫來擷取值區名稱DescribeTrails()。

--s3-prefix

選擇性指定摘要檔案要存放的 Amazon S3 前綴。如果未指定， AWS CLI 將透過呼叫擷取它DescribeTrails()。

> **Note**
>
> 只有在目前的前綴與您所指定之時間範圍期間使用的前綴不同時，才應該使用此選項。

--account-id

可選擇指定用於驗證日誌的帳戶。組織追蹤需要此參數，以驗證組織內特定帳戶的日誌。

--trail-arn

指定要驗證之線索的 Amazon Resource Name (ARN)。線索 ARN 的格式如下。

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> 若要取得線索的線索 ARN，您可以在執行 describe-trails 之前使用 validate-logs 命令。
> 如果日誌檔案已在所指定時間範圍內交付至多個儲存貯體，而且您要限制只驗證其中一個儲存貯體中的日誌檔案，則除了線索 ARN 之外，還建議您指定儲存貯體名稱和前綴。

`--verbose`

選擇性地輸出所指定時間範圍內每個日誌或摘要檔案的驗證資訊。該輸出會指出檔案保持不變還是已進行修改或刪除。在非詳細資訊模式下 (預設)，僅於驗證失敗時才會傳回資訊。

範例

下列範例會驗證自指定的時間開始到現在的日誌檔案，並使用針對目前線索所設定的 Amazon S3 儲存貯體，及指定詳細資訊輸出。

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

validate-logs 的運作方式

`validate-logs` 命令始於驗證所指定之時間範圍內的最新摘要檔案。首先，命令會驗證已從宣告的所屬位置下載的摘要檔案。換言之，如果 CLI 從 S3 位置 `df1` 下載摘要檔案 `p1`，則 validate-logs 會驗證 `p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`。

如果摘要檔案的簽章有效，則會檢查摘要檔案中所參考之每個日誌的雜湊值。此命令接著會回復，並連續驗證先前的摘要檔案和其參考的日誌檔案。它會持續直到到達指定的 `start-time` 值，或直到摘要鏈結束。如果摘要檔案遺失或無效，則會在輸出中指出無法驗證的時間範圍。

驗證結果

驗證結果會以摘要標頭開始，格式如下：

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

主要輸出的每列都包含單一摘要或日誌檔案的驗證結果，格式如下：

```
<Digest file | Log file> <S3 path> <Validation Message>
```

下表說明日誌和摘要檔案的可能驗證訊息。

檔案類型	驗證訊息	描述
Digest file	valid	摘要檔案簽章有效。可以檢查其參考的日誌檔案。此訊息只會包含在詳細資訊模式。

檔案類型	驗證訊息	描述
Digest file	INVALID: has been moved from its original location	從中擷取摘要檔案的 S3 儲存貯體或 S3 物件不符合摘要檔案本身所記錄的 S3 儲存貯體或 S3 物件位置。
Digest file	INVALID: invalid format	摘要檔案的格式無效。無法驗證對應至摘要檔案所代表之時間範圍的日誌檔案。
Digest file	INVALID: not found	找不到摘要檔案。無法驗證對應至摘要檔案所代表之時間範圍的日誌檔案。
Digest file	INVALID: public key not found for fingerprint *fingerprint*	找不到對應至摘要檔案中所記錄之指紋的公有金鑰。無法驗證摘要檔案。
Digest file	INVALID: signature verification failed	摘要檔案簽章無效。因為摘要檔案無效，所以無法驗證其參考的日誌檔案，而且不會宣告其中的 API 活動。
Digest file	INVALID: Unable to load PKCS #1 key with fingerprint *fingerprint*	因為無法載入 PKCS #1 格式且具有指定之指紋的 DER 編碼公有金鑰，所以無法驗證摘要檔案。
Log file	valid	日誌檔案已驗證，且自交付之後未經修改。此訊息只會包含在詳細資訊模式。
Log file	INVALID: hash value doesn't match	日誌檔案的雜湊不符。記錄檔在遞送之後已修改 CloudTrail。
Log file	INVALID: invalid format	日誌檔案的格式無效。無法驗證日誌檔案。
Log file	INVALID: not found	找不到且無法驗證日誌檔案。

輸出會包含所傳回結果的摘要資訊。

範例輸出

詳細資訊

下列範例 validate-logs 指令使用 --verbose 標記並產生接下來的範例輸出。[...] 表示縮寫的範例輸出。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid
```

```
Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

非詳細資訊

下列範例 validate-logs 命令未使用 --verbose 旗標。在下面的範例輸出中，發現一個錯誤。只會傳回標頭、錯誤和摘要資訊。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

檢查特定檔案是否由 CloudTrail

若要檢查儲存貯體中的特定檔案是否已由傳送 CloudTrail，請validate-logs在包含檔案的期間以詳細模式執行。如果檔案出現在的輸出中validate-logs，則檔案由遞送 CloudTrail。

CloudTrail 摘要檔案結構

每個摘要檔案包含上個小時交付至您 Amazon S3 儲存貯體的日誌檔案名稱、這些日誌檔案的雜湊值，以及前一個摘要檔的數位簽章。目前的摘要檔案簽章存放在摘要檔案物件的中繼資料屬性中。數位簽章和雜湊是用於驗證日誌檔案和摘要檔案本身的完整性。

摘要檔案位置

摘要檔案會交付到遵循此語法的 Amazon S3 儲存貯體位置。

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> 對於組織追蹤，儲存貯體的位置也包含組織單位 ID，如下所示：
>
> ```
> s3://s3-bucket-name/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

範例摘要檔案內容

下列範例摘要檔包含 CloudTrail 記錄的資訊。

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
```

```
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```

摘要檔案欄位說明

以下是摘要檔案中每個欄位的說明：

`awsAccountId`

摘要檔案已傳遞的 AWS 帳號 ID。

`digestStartTime`

摘要檔案涵蓋的 UTC 起始時間範圍，作為記錄檔傳送時間的參考 CloudTrail。這表示如果時間範圍是 [Ta, Tb]，摘要會包含從 Ta 到 Tb 這段時間內交付給客戶的所有日誌檔案。

`digestEndTime`

摘要檔涵蓋的結束 UTC 時間範圍，作為記錄檔傳送時間的參考 CloudTrail。這表示如果時間範圍是 [Ta, Tb]，摘要會包含從 Ta 到 Tb 這段時間內交付給客戶的所有日誌檔案。

`digestS3Bucket`

目前摘要檔案已交付的 Amazon S3 儲存貯體名稱。

`digestS3Object`

目前摘要檔案的 Amazon S3 物件金鑰 (也就是 Amazon S3 儲存貯體位置)。字串中的前兩個區域，會顯示摘要檔案傳遞來源的區域。最後一個區域 (在 `your-trail-name` 的後面) 是追蹤的主區域。主區域是建立追蹤的所在區域。在多區域追蹤的案例中，這不同於摘要檔案傳遞來源的區域。

`newestEventTime`

摘要日誌檔案中所有事件的最近事件 UTC 時間。

`oldestEventTime`

摘要日誌檔案中所有事件的最舊事件 UTC 時間。

> **Note**
>
> 如果摘要檔案交付延遲，則 `oldestEventTime` 值會早於 `digestStartTime` 值。

`previousDigestS3Bucket`

前一個摘要檔案的交付 Amazon S3 儲存貯體。

`previousDigestS3Object`

前一個摘要檔案的 Amazon S3 物件金鑰 (也就是 Amazon S3 儲存貯體位置)。

`previousDigestHashValue`

前一個摘要檔案的未壓縮內容十六進位編碼雜湊值。

`previousDigestHashAlgorithm`

用來雜湊前一個摘要檔案的雜湊演算法名稱。

`publicKeyFingerprint`

符合簽署此摘要檔案所用私有金鑰的公有金鑰十六進位編碼指紋。您可以使用 AWS CLI 或 API 擷取摘要檔案對應時間範圍的公開金 CloudTrail 鑰。屬於傳回的公有金鑰，其指紋符合此值，可用

於驗證摘要檔案。如需擷取摘要檔案之公開金鑰的相關資訊，請參閱 AWS CLI `list-public-keys`命令或 CloudTrail `ListPublicKeys`API。

> **Note**
>
> CloudTrail 每個區域使用不同的私鑰/公鑰對。每個摘要檔案都是使用對其區域而言唯一的私有金鑰來簽署。因此，當您驗證來自特定區域的摘要檔案時，您必須在同一個區域中查詢其對應的公有金鑰。

`digestSignatureAlgorithm`

簽署摘要檔案所用的演算法。

`logFiles.s3Bucket`

日誌檔案的 Amazon S3 儲存貯體名稱。

`logFiles.s3Object`

目前日誌檔案的 Amazon S3 物件金鑰。

`logFiles.newestEventTime`

日誌檔案中最近事件的 UTC 時間。此時間也對應到日誌檔案本身的時間戳記。

`logFiles.oldestEventTime`

日誌檔案中最舊事件的 UTC 時間。

`logFiles.hashValue`

未壓縮日誌檔案內容的十六進位編碼雜湊值。

`logFiles.hashAlgorithm`

雜湊日誌檔案所用的雜湊演算法。

起始的摘要檔案

當日誌檔案完整性驗證開始時，會產生起始的摘要檔案。當日誌檔案完整性驗證重新開始時，也會產生起始的摘要檔案 (透過停用再重新啟動日誌檔案完整性驗證，或停止記錄再於啟用驗證的情況下重新開始記錄)。在起始的摘要檔案中，與前一個摘要檔案有關的下列欄位都會是 null：

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

「空」的摘要檔案

CloudTrail 即使摘要檔案所代表的一小時內，您的帳戶中沒有任何 API 活動，仍會傳送摘要檔案。當您需要主張摘要檔案回報的一小時內沒有任何日誌檔案交付時，這很有幫助。

以下範例顯示的摘要檔案內容，記錄的一小時內沒有任何 API 活動。請注意，摘要檔案內容結尾處的 `logFiles:[ ]` 欄位是空的。

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
```

```
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```

摘要檔案的簽章

摘要檔案簽章資訊位在 Amazon S3 摘要檔案物件的兩個物件中繼資料屬性中。每個摘要檔案都有下列中繼資料項目：

- `x-amz-meta-signature`

  摘要檔案簽章的十六進位編碼值。以下為範例簽章：

  ```
  3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
  28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
  05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
  ```

- `x-amz-meta-signature-algorithm`

  以下所示為產生摘要簽章所使用的演算法範例值：

  `SHA256withRSA`

摘要檔案鏈結

事實上，每個摘要檔都包含其先前摘要檔案的參考會啟用「鏈結」，以允許驗證工具 (例如偵測摘要檔案是否已刪除)。 AWS CLI 它還可以成功檢查指定時間範圍內的摘要檔案，從最近的第一個檔案開始。

> **Note**
>
> 當您停用記錄檔完整性驗證時，摘要檔的鏈結會在一小時後中斷。 CloudTrail 不會針對在記錄檔完整性驗證停用的期間內傳送的記錄檔建立摘要檔。例如，如果您在 1 月 1 日中午啟用日誌檔案完整性驗證，並在 1 月 2 日中午停用它，又在 1 月 10 日中午重新啟用，則 1 月 2 日中午到 1 月 10 日中午這段期間交付的日誌檔案不會建立摘要檔案。每當您停止 CloudTrail 記錄或刪除追蹤時，這同樣適用。

如果追蹤的 S3 儲存貯 CloudTrail 體政策設定錯誤或發生非預期的服務中斷，您可能不會收到全部或部分摘要檔案。若要確認追蹤是否有任何摘要傳送錯誤，請執行get-trail-status命令並檢查LatestDigestDeliveryError參數是否有錯誤。解決傳遞問題後 (例如，透過修正儲存貯體政策)， CloudTrail 將嘗試重新傳送任何遺失的摘要檔案。在重新傳遞期間，摘要檔案可能無序遞送，因此鏈結可能會暫時中斷。

如果記錄停止或刪除追蹤， CloudTrail 將會傳送最終摘要檔案。此摘要檔案可以包含任何涵蓋最近事件的剩餘日誌檔案資訊，並包括 StopLogging 事件。

CloudTrail 記錄檔完整性驗證的自訂實作

由於 CloudTrail 使用業界標準、公開可用的密碼編譯演算法和雜湊函數，因此您可以建立自己的工具來驗證 CloudTrail 記錄檔的完整性。啟用日誌檔完整性驗證後，將摘要檔案 CloudTrail 交付到 Amazon S3 儲存貯體。您可以使用這些檔案來實作自己的驗證解決方案。如需摘要檔案的詳細資訊，請參閱「CloudTrail 摘要檔案結構」。

本主題說明如何簽署摘要檔案，並接著詳細說明您必須執行的步驟，以實作解決方案來驗證摘要檔案及其所參考的日誌檔案。

了解 CloudTrail 摘要文件的簽名方式

CloudTrail 摘要檔案會使用 RSA 數位簽章來簽署。對於每個摘要檔案，請 CloudTrail執行下列動作：

1. 根據指定的摘要檔案欄位來建立資料簽署字串 (如下一節所述)。
2. 取得區域唯一的私有金鑰。
3. 將字串和私有金鑰的 SHA-256 雜湊傳遞到 RSA 簽署演算法，以產生數位簽章。
4. 將簽章的位元組碼編碼為十六進位格式。
5. 將數位簽章放在 Amazon S3 摘要檔案物件的 x-amz-meta-signature 中繼資料屬性。

資料簽署字串內容

下列 CloudTrail 物件包含在用於資料簽署的字串中：

- 摘要檔案的結束時間戳記，採用 UTC 延伸格式 (例如 2015-05-08T07:19:37Z)
- 目前摘要檔案的 S3 路徑
- 目前摘要檔案的十六進位編碼 SHA-256 雜湊
- 先前摘要檔案的十六進位編碼簽章

本文件稍後會提供用於計算此字串的格式及範例字串。

自訂驗證實作步驟

實作自訂驗證解決方案時，您需要先驗證摘要檔案，再驗證其所參考的日誌檔案。

驗證摘要檔案

若要驗證摘要檔案，您需要其簽章、其私有金鑰已用來簽署的公有金鑰，以及用來運算的資料簽署字串。

1. 取得摘要檔案。
2. 確認已從其原始位置擷取摘要檔案。
3. 取得摘要檔案的十六進位編碼簽章。
4. 取得其私有金鑰已用來簽署摘要檔案之公有金鑰的十六進位編碼指紋。
5. 擷取摘要檔案對應時間範圍內的公有金鑰。
6. 從所擷取的公有金鑰，選擇其指紋符合摘要檔案中指紋的公有金鑰。
7. 使用摘要檔案雜湊及其他摘要檔案欄位，重新建立用來驗證摘要檔案簽章的資料簽署字串。
8. 傳遞字串、公有金鑰和簽章的 SHA-256 雜湊做為 RSA 簽章驗證演算法的參數，來驗證簽章。如果結果為 true，則摘要檔案有效。

驗證日誌檔案

如果摘要檔案有效，請驗證摘要檔案所參考的每個日誌檔案。

1. 若要驗證日誌檔案的完整性，請在其未壓縮的內容上計算其 SHA-256 雜湊值，並將結果與摘要中以十六進位記錄之日誌檔案的雜湊進行比較。如果雜湊相符，則日誌檔案有效。
2. 使用包含在目前摘要檔案中之先前摘要檔案的相關資訊，先驗證先前摘要檔案，再驗證其對應的日誌檔案。

下列各節將詳細說明這些步驟。

A. 取得摘要檔案

第一個步驟是取得最新摘要檔案、確認您已從其原始位置擷取該檔案、確認其數位簽章，並取得公有金鑰的指紋。

1. 使用 S3 GetObject或 Amazons3 用戶端類別 (例如)，從 Amazon S3 儲存貯體取得您想要驗證的時間範圍內的最新摘要檔案。
2. 確認用來擷取檔案的 S3 儲存貯體和 S3 物件符合摘要檔案本身所記錄的 S3 儲存貯體 S3 物件位置。
3. 接下來，從 Amazon S3 中摘要檔案物件的 x-amz-meta-signature 中繼資料屬性，取得摘要檔案的數位簽章。
4. 在摘要檔案中，從 digestPublicKeyFingerprint 欄位取得其私有金鑰已用來簽署摘要檔案之公有金鑰的指紋。

B. 擷取用於驗證摘要檔案的公有金鑰

若要取得公開金鑰以驗證摘要檔案，您可以使用 AWS CLI 或 CloudTrail API。在這兩種情況下，您會為要驗證的摘要檔案指定時間範圍 (即開始時間和結束時間)。您指定的時間範圍內可能會傳回一或多個公有金鑰。傳回的金鑰可能會有重疊的有效時間範圍。

> **Note**
>
> 由於每個區域 CloudTrail 使用不同的私鑰/公鑰對，因此每個摘要文件都使用其區域專有的私鑰進行簽名。因此，當您驗證來自特定區域的摘要檔案時，您必須從同一個區域擷取其公有金鑰。

使用擷 AWS CLI 取公開金鑰

若要使用擷取摘要檔案的公開金鑰 AWS CLI，請使用cloudtrail list-public-keys指令。此命令的格式如下：

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

開始時間和結束時間參數是 UTC 時間戳記，而且是選用的。如果未指定，則會使用目前的時間，並傳回一或多個目前作用中的公有金鑰。

回應範例

回應會是代表所傳回之一或多個金鑰的 JSON 物件清單：

```
{
    "publicKeyList": [
```

```
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

使用 CloudTrail API 擷取公開金鑰

若要使用 CloudTrail API 擷取摘要檔案的公開金鑰，請將開始時間和結束時間值傳遞至 `ListPublicKeys` API。`ListPublicKeys`API 會傳回其私有金鑰已在指定時間範圍內用來簽署摘要檔案的公有金鑰。針對每個公有金鑰，API 也會傳回對應的指紋。

`ListPublicKeys`

本節說明 `ListPublicKeys` API 的請求參數和回應元素。

> **Note**
>
> ListPublicKeys 的二進位欄位編碼可能會有所變更。

請求參數

名稱	描述
StartTime	選擇性地指定時間範圍的開始時間範圍，以查詢 CloudTrail 摘要檔案的公開金鑰。如果 StartTime 未指定，則使用當前時間，並返回當前的公鑰。 類型: DateTime
EndTime	選擇性地指定時間範圍的結束時間範圍，以查詢 CloudTrail 摘要檔案的公開金鑰。如果 EndTime 未指定，則使用目前時間。 類型: DateTime

回應元素

PublicKeyList 是 PublicKey 物件陣列，其中包含：

名稱	描述
Value	PKCS #1 格式的 DER 編碼公有金鑰值。 類型：Blob
ValidityStartTime	公有金鑰的有效開始時間。 類型: DateTime
ValidityEndTime	公有金鑰的有效結束時間。 類型: DateTime
Fingerprint	公有金鑰的指紋。該指紋可用來識別驗證摘要檔案所需使用的公有金鑰。 類型：字串

C. 選擇要用於驗證的公有金鑰

從 `list-public-keys` 或 `ListPublicKeys` 所擷取的公有金鑰，選擇其指紋符合摘要檔案 `digestPublicKeyFingerprint` 欄位中所記錄之指紋的公有金鑰。這是您將用來驗證摘要檔案的公有金鑰。

D. 重新建立資料簽署字串

現在您已擁有摘要檔案的簽章及相關聯的公有金鑰，您需要計算資料簽署字串。計算資料簽署字串之後，您將擁有驗證簽章所需的輸入。

資料簽署字串的格式如下：

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

`Data_To_Sign_String` 範例如下。

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

重新建立此字串之後，您可以驗證摘要檔案。

E. 驗證摘要檔案

將重新建立後的資料簽署字串、數位簽章和公有金鑰的 SHA-256 雜湊傳遞到 RSA 簽章驗證演算法。如果輸出為 true，則摘要檔案的簽章已經過驗證且摘要檔案有效。

F. 驗證日誌檔案

驗證摘要檔案之後，您可以驗證其所參考的日誌檔案。摘要檔案包含日誌檔案的 SHA-256 雜湊。如果其中一個記錄檔在 CloudTrail 傳送之後被修改，SHA-256 雜湊將會變更，且摘要檔的簽章將不符。

以下說明如何驗證日誌檔案：

1. 使用摘要檔案之 S3 Get 和 logFiles.s3Bucket 欄位中的 S3 位置資訊，對日誌檔案執行 logFiles.s3Object。
2. 如果 S3 Get 操作成功，請使用下列步驟逐一查看摘要檔案 logFiles 陣列中所列的日誌檔案：
   a. 從摘要檔案中對應日誌的 logFiles.hashValue 欄位，擷取檔案的原始雜湊。
   b. 使用 logFiles.hashAlgorithm 中指定的雜湊演算法，將日誌檔案的未壓縮內容進行雜湊。
   c. 將所產生的雜湊值與摘要檔案中日誌的雜湊值進行比較。如果雜湊相符，則日誌檔案有效。

G. 驗證其他摘要和日誌檔案

在每個摘要檔案中，下列欄位提供先前摘要檔案的位置和簽章：

- previousDigestS3Bucket
- previousDigestS3Object
- previousDigestSignature

使用這項資訊循序瀏覽先前摘要檔案，並使用先前章節中的步驟來驗證每個摘要檔案的簽章及其所參考的日誌檔案。唯一的差別是，針對先前的摘要檔案，您不需要從摘要檔案物件的 Amazon S3 中繼資料屬性擷取數位簽章。previousDigestSignature 欄位中會為您提供先前摘要檔案的簽章。

您可以回到摘要檔案一開始，或直到摘要檔案鏈結中斷為止，以兩者之中先到者為準。

離線驗證摘要和日誌檔案

離線驗證摘要和日誌檔案時，您通常可以遵循先前章節中所述的程序。不過，您必須考慮下列幾個部分：

處理最新摘要檔案

最新 (即「目前」) 摘要檔案的數位簽章位在摘要檔案物件的 Amazon S3 中繼資料屬性中。在離線案例中，目前摘要檔案的數位簽章將無法使用。

有兩個方法可處理此問題：

- 由於上一個摘要檔案的數位簽章位於目前摘要檔案中，因此請從 next-to-last 摘要檔案開始驗證。使用此方法，就不會驗證最新摘要檔案。

- 在所有步驟之前，先從摘要檔案物件的中繼資料屬性取得目前摘要檔案的簽章，然號將它存放在安全的離線位置。如此除了鏈結中的先前檔案，還能驗證目前摘要檔案。

路徑解析

已下載摘要檔案中的欄位 (例如 `s3Object` 和 `previousDigestS3Object`) 仍會指向日誌檔案和摘要檔案的 Amazon S3 線上位置。離線解決方案必須設法將這些位置，重新路由到已下載日誌和摘要檔案的目前路徑。

公有金鑰

若要離線驗證，您必須先在線上取得在指定時間範圍內驗證日誌檔案所需的所有公有金鑰 (例如藉由呼叫 `ListPublicKeys`)，然後存放在安全的離線位置。每當您想要在指定的初始時間範圍外驗證其他檔案時，都必須重複此步驟。

範例驗證程式碼片段

下列範例程式碼片段提供了用於驗證 CloudTrail 摘要和記錄檔的基礎架構程式碼。此骨架程式碼線上/離線皆可使用；也就是說，您可以決定是否要線上連線到 AWS來實作它。建議的實作使用 Java Cryptography Extension (JCE) 和 Bouncy Castle 做為安全供應商。

此範例程式碼片段說明：

- 如何建立用來驗證摘要檔案簽章的資料簽署字串。
- 如何驗證摘要檔案簽章。
- 如何驗證日誌檔案雜湊。
- 驗證摘要檔案鏈結的程式碼結構。

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;
```

```
public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
as part of the data to sign
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
 ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:
```

```
                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
                    messageDigest.update(logFileContent);
```

```
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
 Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
 match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
 Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail 記錄檔範例

CloudTrail 監控您帳戶的事件。如果您建立追蹤，其會將這些事件做為日誌檔案交付至您的 Amazon S3 儲存貯體。如果您在 CloudTrail Lake 中建立事件資料倉庫，則會將事件記錄到您的事件資料倉庫中。事件資料存放區不會使用 S3 儲存貯體。

主題

CloudTrail 記錄檔名稱格式

CloudTrail 將下列檔案名稱格式用於傳送至 Amazon S3 儲存貯體的日誌檔物件：

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYY、MM、DD、HH 和 mm 是交付日誌檔案之年、月、日、時和分的數字。小時為 24 小時格式。Z 指出時間為 UTC 時間。

  > **Note**
  >
  > 在特定時間交付的日誌檔案，會包含該時間之前的任何時間點所寫入之記錄。

- 日誌檔案名稱的 16 字元 UniqueString 元件是為了避免覆寫檔案。它沒有任何意義，所以日誌處理軟體應會忽略它。
- FileNameFormat 是檔案的編碼。目前，這是 json.gz，即壓縮 gzip 格式的 JSON 文字檔。

範例 CloudTrail 記錄檔名稱

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

日誌檔案範例

日誌檔案包含一或多筆記錄。下列範例是日誌的程式碼片段，可顯示開始建立日誌檔案之動作的記錄。

如需 CloudTrail 事件記錄欄位的資訊，請參閱CloudTrail 記錄內容。

內容

Amazon EC2 日誌範例

Amazon Elastic Compute Cloud (Amazon EC2) 在 AWS 雲端中提供可調整大小的運算容量。您可以啟動虛擬伺服器、設定安全和聯網功能，以及管理儲存。Amazon EC2 也可以迅速擴展與縮減規模，以處理需求或熱門高峰的變更，從而降低您預測伺服器流量的需求。如需詳細資訊，請參閱《Linux 執行個體 Amazon EC2 使用者指南》。

下列範例顯示名為 Mateo 的 IAM 使用者執行 aws ec2 start-instances 命令，為執行個體 i-EXAMPLE56126103cb 和 i-EXAMPLEaff4840c22 呼叫 Amazon EC2 StartInstances 動作。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
```

```
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

下列範例顯示名為 Nikki 的 IAM 使用者執行 aws ec2 stop-instances 命令，呼叫 Amazon EC2 StopInstances 動作以停止兩個執行個體。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
```

```
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

下列範例顯示名為 Arnav 的 IAM 使用者執行 aws ec2 create-key-pair 命令，以呼叫 CreateKeyPair 動作。請注意，responseElements包含 key pair 的散列並 AWS 刪除了密鑰材料。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
```

```
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

IAM 日誌範例

AWS Identity and Access Management (IAM) 是可協助您安全地控制 AWS 資源存取的 Web 服務。使用 IAM，您可以集中管理控制使用者可以存取哪些 AWS 資源的許可。您可以使用 IAM 來控制能通過身分驗證 (登入) 和授權使用資源的 (具有許可) 的人員。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/。

下列範例顯示名為 `Mary` 的 IAM 使用者執行 aws iam create-user 命令，呼叫 `CreateUser` 動作以建立名為 `Richard` 的新使用者。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
```

```
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
```

```
}]}
```

下列範例顯示名為 Paulo 的 IAM 使用者執行 aws iam add-user-to-group 命令，呼叫 AddUserToGroup 動作以新增名為 Jane 的使用者至 Admin 群組。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
```

```
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

下列範例顯示名為 Saanvi 的 IAM 使用者執行 aws iam create-role 命令，呼叫 CreateRole 動作以建立一個角色。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
```

```
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

錯誤代碼和訊息日誌範例

下列範例顯示名為 Terry 的 IAM 使用者執行 aws cloudtrail update-trail 命令來呼叫 UpdateTrail 動作以更新名為 myTrail2 的追蹤，但找不到該追蹤名稱。日誌會顯示 errorCode 和 errorMessage 元素中的這個錯誤。

```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
```

```
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail 洞察事件記錄範例

下列範例顯示 CloudTrail 深入解析事件記錄檔。Insights 事件實際上是一組事件，標記異常寫入管理 API 活動或錯誤回應活動的一段時間的開始和結束。`state` 欄位會顯示事件是在異常活動期間的開始還是結束時記錄的。事件名稱與 CloudTrail 分析管理事件的 AWS Systems Manager API 名稱相同`UpdateInstanceInformation`，以判斷發生異常活動。雖然開始和結束事件具有唯一的 `eventID` 值，但它們也具有由該組使用的 `sharedEventID` 值。Insights 事件會顯示 `baseline`

(活動的正常模式)、insight (觸發開始 Insights 事件的或平均異常活動)，以及在結束事件中，顯示 Insights 事件期間平均異常活動的 insight 值。如需 CloudTrail 深入解析的詳細資訊，請參閱記錄 Insights 事件。


```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
```

```
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

使用 CloudTrail 處理程式庫

CloudTrail 處理庫是一個 Java 庫，提供了一種簡單的方法來處理 AWS CloudTrail 日誌。您可以提供 CloudTrail SQS 佇列的組態詳細資料，並撰寫程式碼來處理事件。 CloudTrail 處理庫完成剩下的工作。它會輪詢您的 Amazon SQS 佇列、讀取和剖析佇列訊息、下載 CloudTrail 記錄檔、剖析日誌檔中的事件，以及將事件作為 Java 物件傳遞至程式碼。

CloudTrail 處理程式庫具有高度擴充性和容錯能力。它會處理日誌檔案的平行處理，讓您可以處理所需數目的日誌。它會處理與網路逾時和無法存取資源相關的網路失敗。

下列主題說明如何使用 CloudTrail 處理程式庫來處理 Java 專案中的 CloudTrail 記錄檔。

該庫作為 APACHE 許可的開源項目提供，可在以下位置獲得：。 GitHub https://github.com/aws/aws-cloudtrail-processing-library此程式庫來源包括可用作您自己專案基礎的範本程式碼。

主題

- 最低需求
- 處理 CloudTrail 記錄
- 進階主題
- 其他資源

最低需求

若要使用「 CloudTrail 處理程式庫」，您必須具備下列項目：

- AWS SDK for Java 1.11.830
- Java 1.8 (Java SE 8)

處理 CloudTrail 記錄

若要在 Java 應用程式中處理 CloudTrail 記錄檔：

1. 將 CloudTrail 處理程式庫新增至您的專案
2. 配置 CloudTrail 處理程式庫
3. 實作事件處理器
4. 實例化和執行處理執行器

將 CloudTrail 處理程式庫新增至您的專案

要使用 CloudTrail 處理庫，請將其添加到 Java 項目的類路徑中。

內容

- 將程式庫新增至 Apache Ant 專案
- 將程式庫新增至 Apache Maven 專案
- 將程式庫新增至 Eclipse 專案
- 將程式庫新增至 IntelliJ 專案

將程式庫新增至 Apache Ant 專案

若要將 CloudTrail 處理程式庫新增至 Apache Ant 專案

1. 從下列位置下載或複製 CloudTrail 處理程式庫原始程式碼 GitHub：
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 從源程式碼建置 .jar 檔案，如 README 中所述：

```
mvn clean install -Dgpg.skip=true
```

3. 將產生的 .jar 檔案複製至您的專案，並將它新增至您專案的 build.xml 檔案。例如：

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

將程式庫新增至 Apache Maven 專案

CloudTrail 處理庫可用於阿帕奇的 Maven。您可以將它新增至專案，方法是在專案的 pom.xml 檔案中編寫單一相依性。

若要將 CloudTrail 處理程式庫新增至 Maven 專案

- 開啟 Maven 專案的 pom.xml 檔案，並新增下列相依性：

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

將程式庫新增至 Eclipse 專案

若要將 CloudTrail 處理程式庫新增至 Eclipse 專案

1. 從下列位置下載或複製 CloudTrail 處理程式庫原始程式碼 GitHub：
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 從源程式碼建置 .jar 檔案，如 README 中所述：

```
mvn clean install -Dgpg.skip=true
```

3. 將構建的 aws-cloudtrail-processing-library -1.6.1.jar 複製到項目中的目錄（通常）。lib
4. 在 Eclipse Project Explorer (專案瀏覽器) 中，以滑鼠右鍵按一下您專案的名稱，並選擇 Build Path (建置路徑)，然後選擇 Configure (設定)
5. 在 Java Build Path (Java 建置路徑) 視窗中，選擇 Libraries (程式庫) 索引標籤。

6. 選擇添加 JAR... 並導航到您複製 aws-cloudtrail-processing-library -1.6.1.jar 的路徑。
7. 選擇 OK (確定) 完成將 `.jar` 新增至您的專案。

將程式庫新增至 IntelliJ 專案

若要將 CloudTrail 處理程式庫加入 IntelliJ 專案

1. 從下列位置下載或複製 CloudTrail 處理程式庫原始程式碼 GitHub：
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 從源程式碼建置 .jar 檔案，如 README 中所述：

```
mvn clean install -Dgpg.skip=true
```

3. 從 File (檔案) 中，選擇 Project Structure (專案結構)。
4. 選擇 Modules (模組)，然後選擇 Dependencies (相依性)。
5. 選擇 + JARS or Directories (+ JARS 或目錄)，然後前往您建置 `aws-cloudtrail-processing-library-1.6.1.jar` 的路徑。
6. 選擇 Apply (套用)，然後選擇 OK (確定) 完成將 `.jar` 新增至您的專案。

配置 CloudTrail 處理程式庫

您可以建立在執行階段載入的類別路徑屬性檔案，或透過建立`ClientConfiguration`物件並手動設定選項，來設定 CloudTrail 處理程序庫。

提供屬性檔案

您可以編寫 classpath 屬性檔案，以將組態選項提供給您的應用程式。下列範例檔案顯示您可設定的選項：

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url
```

```
# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

下列是必要參數：

- `sqsUrl`— 提供要從中提取 CloudTrail通知的 URL。如果您未指定此值，則 `AWSCloudTrailProcessingExecutor` 會擲出 `IllegalStateException`。
- `accessKey` – 您帳戶的唯一識別符，例如 AKIAIOSFODNN7EXAMPLE。
- `secretKey`— 您帳戶的唯一識別碼，例如：密碼 /K7M登記/CYEXAMPLEKE bPxRfi Y。

`accessKey`和`secretKey`參數會將您的 AWS 認證提供給程式庫，以便程式庫可以代表您存取 AWS 。

其他參數的預設值是透過程式庫所設定。如需詳細資訊，請參閱 AWS CloudTrail Processing Library 參考。

創建一個 ClientConfiguration

您可以初始化和設定 AWSCloudTrailProcessingExecutor 物件的選項，以將選項提供給 ClientConfiguration，而不是在 classpath 屬性中設定選項，如下列範例所示：

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

實作事件處理器

若要處理 CloudTrail 記錄檔，您必須實作EventsProcessor接收記 CloudTrail 錄資料的。下列是範例實作：

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

實施時EventsProcessor，您實現了AWSCloudTrailProcessingExecutor用於向您發送 CloudTrail 事件的process()回調。事件是以 CloudTrailClientEvent 物件清單形式提供。

CloudTrailClientEvent物件提供了CloudTrailEvent和CloudTrailEventMetadata，您可以用來讀取 CloudTrail 事件和遞送資訊。

此簡單範例會列印每個傳遞至 SampleEventsProcessor 之事件的事件資訊。在您自己的實作中，您可以在符合您需求時處理日誌。AWSCloudTrailProcessingExecutor 只要有要傳送的事件且仍在執行，就會持續將事件傳送至 EventsProcessor。

實例化和執行處理執行器

在您為 CloudTrail 處理程式庫撰寫EventsProcessor並設定組態值之後 (無論是在屬性檔案中或使用ClientConfiguration類別)，您就可以使用這些元素來初始化和使用AWSCloudTrailProcessingExecutor.

用於處**AWSCloudTrailProcessingExecutor**理 CloudTrail 事件

1. 實例化 AWSCloudTrailProcessingExecutor.Builder 物件。Builder 的建構函數採用 EventsProcessor 物件和 classpath 屬性檔案名稱。
2. 呼叫 Builder 的 build() 原廠方法來設定和取得 AWSCloudTrailProcessingExecutor 物件。
3. 使用AWSCloudTrailProcessingExecutor的start()和stop()方法來開始和結束 CloudTrail 事件處理。

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

進階主題

主題

- 篩選要處理的事件
- 處理資料事件
- 報告進度
- 處理錯誤

篩選要處理的事件

根據預設，您 Amazon SQS 佇列之 S3 儲存貯體中的所有日誌和其所含的所有事件都會傳送至 EventsProcessor。Process Library 提供選 CloudTrail 用的介面，您可以實作這些介面來篩選用來取得 CloudTrail 記錄檔的來源，以及篩選您有興趣處理的事件。

SourceFilter

您可以實作 SourceFilter 界面，選擇是否要處理所提供來源的日誌。SourceFilter 會宣告可接收 CloudTrailSource 物件的單一回呼方法 filterSource()。若要持續處理來源中的事件，請從 false 傳回 filterSource()。

程式庫會在程filterSource()式庫輪詢 Amazon SQS 佇列上的日誌之後， CloudTrail 處理程式庫會呼叫該方法。這發生在程式庫啟動日誌的事件篩選或處理之前。

下列是範例實作：

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
```

```
  }
}
```

如果您未提供自己的 SourceFilter，則會使用 DefaultSourceFilter，以允許處理所有來源 (一律會傳回 true)。

EventFilter

您可以實現接EventFilter口以選擇是否將 CloudTrail事件發送到您的EventsProcessor. EventFilter宣告接收CloudTrailEvent物件的單一回呼方法。filterEvent()若要持續處理事件，請從 false 傳回 filterEvent()。

程 CloudTrail 式庫會在程filterEvent()式庫輪詢 Amazon SQS 佇列上的日誌之後，以及在來源篩選之後呼叫該方法。這發生在程式庫啟動日誌的事件處理之前。

請參閱下列範例實作：

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

如果您未提供自己的 EventFilter，則會使用 DefaultEventFilter，以允許處理所有事件 (一律會傳回 true)。

處理資料事件

CloudTrail 處理資料事件時，會以原始格式保留數字，無論是整數 (int) 還是 float (包含小數的數字)。在資料事件欄位中具有整數的事件中， CloudTrail 歷史上會將這些數字當作浮點數處理。目前，透過保留原始格式來 CloudTrail 處理這些欄位中的數字。

為了避免中斷自動化作業的最佳作法，請在您用來處理或篩選 CloudTrail 資料事件的任何程`float`式碼或自動化作業中保持彈性，並同時`int`允許和格式化的數字。為獲得最佳結果，請使用 CloudTrail 處理庫的 1.4.0 或更高版本。

下列範例片段顯示 `float` 格式化的數字，`2.0`，適用於資料事件的 `ResponseParameters` 區塊中的 `desiredCount` 參數。

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

下列範例片段顯示 `int` 格式化的數字，`2`，適用於資料事件的 `ResponseParameters` 區塊中的 `desiredCount` 參數。

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

報告進度

實作`ProgressReporter`介面以自訂 CloudTrail 處理程式庫進度報告。 `ProgressReporter`聲明兩種方法：`reportStart()`和`reportEnd()`，它們在以下操作的開始和結束時調用：

- 輪詢 Amazon SQS 中的訊息
- 剖析 Amazon SQS 中的訊息
- 處理日誌的 Amazon SQS 來 CloudTrail 源
- 刪除 Amazon SQS 中的訊息
- 下載記 CloudTrail 錄檔

- 處理記 CloudTrail 錄檔

兩種方法都會收到 ProgressStatus 物件，其中包含所執行操作的資訊。progressState 成員擁有可識別目前操作之 ProgressState 列舉的成員。這個成員可以在 progressInfo 成員中包含其他資訊。此外，您從 reportStart() 傳回的任何物件都會傳遞至 reportEnd()，因此您可以提供內容資訊 (例如開始處理事件的時間)。

下列範例實作提供操作需要多久時間才能完成的資訊：

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

如果您未實作自己的 ProgressReporter，則會改用 DefaultExceptionHandler，以列印所執行狀態的名稱。

處理錯誤

ExceptionHandler 界面可讓您在日誌處理期間發生例外狀況時提供特殊處理。ExceptionHandler 宣告單一回呼方法 handleException()，以接收包含所發生例外狀況之內容的 ProcessingLibraryException 物件。

您可以使用傳入之 ProcessingLibraryException 的 getStatus() 方法，了解發生例外狀況時所執行的操作，並取得操作狀態的其他資訊。ProcessingLibraryException 衍生自 Java 的標準 Exception 類別，因此您也可以呼叫任何例外狀況方法來擷取例外狀況的資訊。

請參閱下列範例實作：

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

如果您未提供自己的 ExceptionHandler，則會改用 DefaultExceptionHandler，以列印標準錯誤訊息。

> **Note**
>
> 如果deleteMessageUponFailure參數為true，則 CloudTrail 處理程式庫不會區分一般例外狀況與處理錯誤，而且可能會刪除佇列訊息。
>
> 1. 例如，您使用 SourceFilter，依時間戳記來篩選訊息。
> 2. 不過，您沒有存取接收 CloudTrail 日誌檔案的 S3 儲存貯體所需的權限。因為您沒有必要許可，所以會擲回 AmazonServiceException。 CloudTrail 處理庫將其包裝在CallBackException.
> 3. DefaultExceptionHandler 會將這個項目記錄為錯誤，但不會識別根本原因，即您沒有必要許可。 CloudTrail 處理程式庫會將此視為處理錯誤，並刪除訊息，即使訊息包含有效的 CloudTrail 記錄檔也一樣。
>
> 如果您想要使用 SourceFilter 來篩選訊息，則請驗證 ExceptionHandler 可以區分服務例外狀況與處理錯誤。

其他資源

如需有關 CloudTrail 處理程式庫的詳細資訊，請參閱下列內容：

- CloudTrail 處理程式庫 GitHub 專案，其中包含示範如何實作 CloudTrail 處理程式庫應用程式的範例程式碼。
- CloudTrail 處理程式庫 Java Package 件文件。

中的安全性 AWS CloudTrail

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS CloudTrail，請參閱合規方案的AWS 服務範圍。
- 雲端中的安全性 — 您的責任取決於您使用的 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時套用共同責任模型 CloudTrail。下列主題說明如何設定 CloudTrail 以符合安全性與合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 CloudTrail 資源。

主題

- 資料保護 AWS CloudTrail
- 的 Identity and Access Management AWS CloudTrail
- 符合性驗證 AWS CloudTrail
- 韌性 AWS CloudTrail
- 基礎結構安全 AWS CloudTrail
- 預防跨服務混淆代理人
- 安全性最佳做法 AWS CloudTrail
- 使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)

資料保護 AWS CloudTrail

AWS 共用責任模型適用於中的資料保護 AWS CloudTrail。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 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，例如名稱欄位。這包括當您使用主控台、API CloudTrail 或 AWS SDK 時 AWS 服務 使用或其他使用時。 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。

依預設， CloudTrail 事件日誌檔會使用 Amazon S3 伺服器端加密 (SSE) 加密。您也可以選擇使用 AWS Key Management Service (AWS KMS) 金鑰加密記錄檔。您可以將日誌檔案存放在 儲存貯體中，沒有時間限制。您也可以定義 Amazon S3 生命週期規則以自動封存或刪除日誌檔案。如果您要日誌檔案交付和驗證的通知，可以設定 Amazon SNS 通知。

下列安全性最佳做法也會解決中的資料保護 CloudTrail：

- 使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)
- Amazon S3 存儲桶政策 CloudTrail
- 驗證 CloudTrail 記錄檔完整性
- 在 AWS 帳戶之間共用 CloudTrail 記錄檔

由於 CloudTrail 日誌檔存放在 Amazon S3 的儲存貯體或儲存貯體中，因此您還應該在 Amazon 簡單儲存服務使用者指南中查看資料保護資訊。如需詳細資訊，請參閱 Amazon S3 中的資料保護。

的 Identity and Access Management AWS CloudTrail

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 CloudTrail 資源。IAM 是您可以使用的 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，具體取決於您在進行的工作 CloudTrail。

服務使用者 — 如果您使用 CloudTrail 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 CloudTrail 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果無法存取中的圖徵 CloudTrail，請參閱疑難排解 AWS CloudTrail 身分和存取。

服務管理員 — 如果您負責公司的 CloudTrail 資源，您可能擁有完整的存取權 CloudTrail。決定您的服務使用者應該存取哪些 CloudTrail 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。若要進一步瞭解貴公司如何搭配使用 IAM CloudTrail，請參閱如何與 IAM AWS CloudTrail 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存取權限的詳細資訊 CloudTrail。若要檢視可在 IAM 中使用的 CloudTrail 基於身分的政策範例，請參閱。以身分識別為基礎的原則範例 AWS CloudTrail

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。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

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

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取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任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳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。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。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。如需使用角色的方法更多相關資訊，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 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。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 (信任的委託人) 存取您帳戶中的資源。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）。若要了解跨帳戶存取權角色和資源型政策間的差異，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。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 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。如需更多資訊，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。如需更多資訊，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。

若要了解是否要使用 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更多相關資訊，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。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該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。若要了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限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。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) 可控制哪些委託人 (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予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政

策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。

- 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。如需組織和 SCP 的更多相關資訊，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。如需更多資訊，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。

如何與 IAM AWS CloudTrail 搭配使用

在您使用 IAM 管理存取權限之前 CloudTrail，請先了解哪些 IAM 功能可搭配使用 CloudTrail。

您可以搭配使用的 IAM 功能 AWS CloudTrail

IAM 功能	CloudTrail 支持
身分型政策	是
資源型政策	部分
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	否
ACL	否
ABAC(政策中的標籤)	部分

IAM 功能	CloudTrail 支持
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	是

若要深入瞭解如何以 CloudTrail 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

以身分識別為基礎的原則 CloudTrail

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。

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

以身分識別為基礎的原則範例 CloudTrail

若要檢視以 CloudTrail 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS CloudTrail

以資源為基礎的政策 CloudTrail

支援以資源基礎的政策	部分

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。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，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。當主體和資源位於不同時 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連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

CloudTrail 針對用於與外部事件來源的 CloudTrail Lake 整合的管道，支援以資源為基礎的 AWS政策。通道的資源型政策會定義哪些主體實體 (帳戶、使用者、角色和聯合身分使用者) 可在通道上呼叫 `PutAuditEvents`，將事件傳送至目的地事件資料存放區。如需有關建立與 CloudTrail Lake 整合的詳細資訊，請參閱建立與事件來源以外的整合 AWS。

範例

若要檢視 CloudTrail 以資源為基礎的政策範例，請參閱AWS CloudTrail 資源型政策範例。

的政策動作 CloudTrail

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。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 CloudTrail 動作清單，請參閱服務授權參考 AWS CloudTrail中的定義動作。

中的策略動作在動作之前 CloudTrail 使用下列前置詞：

```
cloudtrail
```

例如，若要授予某人使用 ListTags API 操作追蹤清單的許可，請在其政策中加入 cloudtrail:ListTags 動作。政策陳述式必須包含 Action 或 NotAction 元素。 CloudTrail 定義了它自己的一組動作，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
      "cloudtrail:RemoveTags
```

您可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Get 文字的所有動作，請包含以下動作：

```
"Action": "cloudtrail:Get*"
```

的政策資源 CloudTrail

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 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 CloudTrail 資源類型及其 ARN 的清單，請參閱服務授權參考資料 AWS CloudTrail中的定義資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS CloudTrail定義的動作。

在中 CloudTrail，有三種資源類型：追蹤、事件資料存放區和通道。每個資源都有一個相關聯的唯一 Amazon Resource Name (ARN)。在策略中，您可以使用 ARN 來識別策略適用的資源。 CloudTrail 目前不支援其他資源類型，有時也稱為子資源。

追 CloudTrail 蹤資源具有下列 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

CloudTrail 事件資料存放區資源具有下列 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

通 CloudTrail 道資源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 服務命名空間。

例如，如果是識別碼為 *123456789012*，若要在陳述式中指定存在於美國東部 (俄亥俄) 區域中名為 *My-Trail* 的追蹤，請 AWS 帳戶 使用下列 ARN：

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

若要指定屬於其中特定帳戶的所有追蹤 AWS 區域，請使用萬用字元 (*)：

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

某些 CloudTrail 動作 (例如用來建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

許多 CloudTrail API 動作涉及多個資源。例如，`CreateTrail` 需要 Amazon S3 儲存貯體來存放日誌檔案，因此使用者必須有寫入儲存貯體的許可。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

```
"Resource": [
```

```
        "resource1",
        "resource2"
```

的政策條件索引鍵 CloudTrail

支援服務特定政策條件金鑰	否

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予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。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。

CloudTrail 不定義自己的條件鍵，但它支持使用一些全局條件鍵。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。

若要查看 CloudTrail 條件索引鍵清單，請參閱服務授權參考 AWS CloudTrail中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱動作定義者 AWS CloudTrail。

ACL 在 CloudTrail

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。

阿巴克與 CloudTrail

支援 ABAC (政策中的標籤)	部分

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 的詳細資訊，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)。

雖然您可以將標籤附加至 CloudTrail 資源，但 CloudTrail 僅支援根據標籤控制對 CloudTrail Lake 事件資料存放區和頻道的存取。您無法按照標籤控制對追蹤的存取權限。

您可以將標籤附加至 CloudTrail 資源，或將要求中的標籤傳遞給 CloudTrail。如需標記 CloudTrail 資源的詳細資訊，請參閱建立追蹤和建立、更新和管理追蹤 AWS CLI。

使用臨時登入資料 CloudTrail

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。如需切換角色的詳細資訊，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。

轉寄存取工作階段 CloudTrail

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。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 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》。

CloudTrail 的服務角色

支援服務角色	是

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。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 CloudTrail 功能。只有在 CloudTrail 提供指引時才編輯服務角色。

服務連結角色 CloudTrail

支援服務連結角色	是

服務連結角色是一種連結至. 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。

CloudTrail 支援與 AWS Organizations整合的服務連結角色。建立組織追蹤或事件資料存放區時需使用此角色。組織追蹤和事件資料會儲存組織 AWS 帳戶 中所有人的記錄事件。如需建立或管理 CloudTrail 服務連結角色的詳細資訊，請參閱使用服務連結角色 AWS CloudTrail。

以身分識別為基礎的原則範例 AWS CloudTrail

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

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。

如需有關由定義的動作和資源類型的詳細資訊 CloudTrail，包括每個資源類型的 ARN 格式，請參閱服務授權參考 AWS CloudTrail中的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 範例：允許和拒絕對於特定追蹤的動作
- 範例：在特定追蹤建立和套用政策的動作
- 範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限
- 使用 CloudTrail 主控台
- 允許使用者檢視他們自己的許可
- 授與使用者的自訂 CloudTrail 權限

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 CloudTrail 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。它們可用在您的 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。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。

- 套用最低許可許可 – 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 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。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。如需更多資訊，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。如需更多資訊，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。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，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。

CloudTrail 沒有您可以在政策陳述式`Condition`元素中使用的服務特定內容索引鍵。

範例：允許和拒絕對於特定追蹤的動作

以下範例示範的政策允許使用此政策的使用者檢視追蹤的狀態和組態，以及開始和停止記錄名為 *My-First-Trail* 的追蹤。此路徑是在美國東部 (俄亥俄) 區域 (其本土區域) 中建立的，ID 為 *123* 456789012。 AWS 帳戶

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
```

```
            ]
        }
    ]
}
```

下列範例示範一項原則，明確拒絕任何未命名為 *My-* First-Trail 之追蹤的 CloudTrail 動作。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

範例：在特定追蹤建立和套用政策的動作

您可以使用權限和策略來控制使用者對 CloudTrail 追蹤執行特定動作的能力。

例如，您不希望公司開發人員群組的使用者開始或停止記錄特定追蹤。不過，您可能想要授予他們對追蹤執行 `DescribeTrails` 和 `GetTrailStatus` 動作的許可。您要開發人員群組使用者在他們管理的追蹤上執行 `StartLogging` 或 `StopLogging` 動作。

您可以建立兩個政策陳述式，然後將其連接至您建立於 IAM 中的開發人員群組。如需 IAM 中群組的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 群組。

在第一個政策中，您拒絕對所指定的追蹤 ARN 執行 `StartLogging` 和 `StopLogging` 動作。在下列範例中，追蹤 ARN 是 `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`。

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

```
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

在第二個策略中，允許對所有 CloudTrail 資源GetTrailStatus執行DescribeTrails和動作：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

如果開發人員群組使用者嘗試開始或停止您在第一個政策中指定的追蹤記錄日誌，該使用者會收到拒絕存取的例外狀況。開發人員群組使用者可以對他們所建立及管理的追蹤予以開始與停止記錄日誌。

以下示例顯示配置的開發人員組在一個名為的配置 AWS CLI 文件中devgroup。首先，devgroup 的使用者執行 describe-trails 命令。

```
$ aws --profile devgroup cloudtrail describe-trails
```

命令成功完成並產生以下輸出：

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
            "S3BucketName": "myS3bucket ",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

使用者接著會對您在第一個政策中指定的追蹤執行 get-trail-status 命令。

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

命令成功完成並產生以下輸出：

```
{
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

接下來，devgroup 群組中的使用者對同一個追蹤執行 stop-logging 命令。

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

命令會傳回拒絕存取的例外狀況，例如下列內容：

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

使用者會對相同的追蹤執行 start-logging 命令。

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

命令再次傳回拒絕存取的例外狀況，例如下列內容：

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限

在以下政策範例中，如果下方條件中至少有一項不符合，使用 CreateEventDataStore 建立事件資料存放區的許可便會被拒絕：

- 事件資料存放區沒有套用至自身之 stage 的標籤索引鍵
- 階段標籤的值不是 alpha、beta、gamma 或 prod。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
```

```
                    ]
                }
            }
        }
    ]
}
```

在以下政策範例中，如果事件資料存放區有值為 prod 的 stage 標籤，則使用 DeleteEventDataStore 刪除事件資料存放區的許可會被拒絕。類似的政策可以協助保護事件資料存放區免遭意外刪除。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

使用 CloudTrail 主控台

若要存取 AWS CloudTrail 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. CloudTrail 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。

授與CloudTrail 管理權限

若要允許 IAM 角色或使用者管理 CloudTrail 資源 (例如追蹤、事件資料存放區或通道)，您必須授與明確許可，才能執行與 CloudTrail 工作相關聯的動作。在大多數情況下，您可以使用包含預先定義權限的 AWS 受管理策略。

> **Note**
>
> 您授予使用者執行 CloudTrail 管理任務的許可與將日誌檔傳送到 Amazon S3 儲存貯體或傳送通知至 Amazon SNS 主題所 CloudTrail 需的許可不同。如需這些許可的詳細資訊，請參閱 Amazon S3 存儲桶政策 CloudTrail。
> 如果您設定與 Amazon CloudWatch 日誌的整合， CloudTrail 還需要一個角色，該角色可將事件傳遞到 Amazon CloudWatch 日誌日誌群組。您必須建立使 CloudTrail 用的角色。如需詳細資訊，請參閱 授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限及 將事件傳送至 CloudWatch 記錄檔。

下列 AWS 受管理的策略適用於 CloudTrail：

- AWSCloudTrail_FullAccess— 此原則提供對 CloudTrail 資源 CloudTrail 動作 (例如追蹤、事件資料存放區和通道) 的完整存取權。此原則提供建立、更新和刪除 CloudTrail 追蹤、事件資料存放區和通道所需的權限。

  此政策還提供管理 Amazon S3 儲存貯體、 CloudWatch 日誌的日誌群組和追蹤的 Amazon SNS 主題的許可。不過，受`AWSCloudTrail_FullAccess`管政策並未提供刪除 Amazon S3 儲存貯體、CloudWatch 日誌的日誌群組或 Amazon SNS 主題的許可。如需其他人的受管理策略的相關資訊 AWS 服務，請參閱受AWS 管理的策略參考指南。

  > **Note**
  >
  > 該AWSCloudTrail_FullAccess政策不打算在您 AWS 帳戶的. 使用此角色的使用者可以在自己的 AWS 帳戶中關閉或重新設定最敏感和重要的稽核功能。因此，您必須僅向帳戶管理員套用此政策。您必須嚴密控制並監視此政策的使用狀況。

- AWSCloudTrail_ReadOnlyAccess— 此原則授與檢視 CloudTrail 主控台的權限，包括最近的事件和事件歷程記錄。此政策還允許您檢視現有的追蹤、事件資料存放區和通道。使用此政策的角色和使用者可以下載事件歷史記錄，但無法建立或更新追蹤、事件資料存放區或通道。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 使用者和群組位於 AWS IAM Identity Center：

  建立權限合集。請按照 AWS IAM Identity Center 使用者指南 中的 建立權限合集 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。請按照 IAM 使用者指南 的 為第三方身分提供者 (聯合) 建立角色 中的指示進行操作。

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照 IAM 使用者指南 的 為 IAM 使用者建立角色 中的指示進行操作。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循 IAM 使用者指南的新增許可到使用者 (主控台)中的指示。

其他資源

若要進一步了解如何使用 IAM 提供身分識別，例如使用者和角色、存取帳戶中的資源，請參閱 IAM 使用者指南中的 AWS 資源設定 IAM 和存取管理。

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，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

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": "*"
        }
    ]
}
```

授與使用者的自訂 CloudTrail 權限

CloudTrail 策略會將權限授與合作的使用者 CloudTrail。如果您需要授與不同的權限給使用者，可以將 CloudTrail 政策附加到 IAM 群組或使用者。您可以編輯政策，藉以包含或排除特定許可。您也可以建立自己的自訂政策。政策是 JSON 文件，可定義允許使用者執行的動作，以及使用者得以執行這些動作的資源。如需具體範例，請參閱 範例：允許和拒絕對於特定追蹤的動作 和 範例：在特定追蹤建立和套用政策的動作。

內容

- 唯讀存取
- 完整 存取
- 授與檢視 CloudTrail 主控台 AWS Config 資訊的權限
- 授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限
- 其他資訊

唯讀存取

下列範例顯示授與 CloudTrail 追蹤唯讀存取權的原則。這相當於受管政策 AWSCloudTrail_ReadOnlyAccess。政策會將查看追蹤資訊的許可授予使用者，但未授予建立或更新追蹤的許可。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:Get*",
                "cloudtrail:Describe*",
                "cloudtrail:List*",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

在政策陳述式中，Effect 元素指定允許或拒絕動作。Action 元素列出允許使用者執行的特定動作。Resource元素會列出允許使用者執行這些動作的 AWS 資源。對於控制 CloudTrail 動作存取權的原則，Resource元素通常會設定為*，萬用字元表示「所有資源」。

Action 元素中的值對應至服務所支援的 API。動作前面會加上，cloudtrail:以指出它們參照 CloudTrail 動作。您可以在 Action 元素中使用 * 萬用字元，如下列範例所示：

- "Action": ["cloudtrail:*Logging"]

  這允許所有以「Logging」(StartLogging,StopLogging) 結尾的 CloudTrail 動作。
- "Action": ["cloudtrail:*"]

  這允許所有 CloudTrail 操作，但不允許其他 AWS 服務的操作。
- "Action": ["*"]

  這允許所有 AWS 操作。此許可適用於身為您帳戶之 AWS 管理員的使用者。

唯讀政策不會將 CreateTrail、UpdateTrail、StartLogging 和 StopLogging 動作的許可授予使用者。不允許具有此政策的使用者建立追蹤、更新追蹤，或是開啟或關閉記錄日誌。有關 CloudTrail 操作列表，請參閱 AWS CloudTrail API 參考。

完整 存取

下列範例顯示授與完整存取權的策略 CloudTrail。這相當於受管政策 AWSCloudTrail_FullAccess。它授予用戶執行所有 CloudTrail 操作的權限。它也可讓使用者在 Amazon S3 記錄資料事件 AWS Lambda，以及管理 Amazon S3 儲存貯體中的檔案、管理 CloudWatch 日 CloudTrail 誌監控日誌事件的方式，以及管理使用者關聯帳戶中的 Amazon SNS 主題。

> **Important**
>
> AWSCloudTrail_FullAccess策略或同等權限不打算在您的 AWS 帳戶中廣泛共享。具有此角色或同等存取權的使用者可以停用或重新設定其 AWS 帳戶中最敏感和最重要的稽核功能。因此，此政策應僅套用於帳戶管理員，並且在嚴密的控制和監控下使用此政策。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

授與檢視 CloudTrail 主控台 AWS Config 資訊的權限

您可以在 CloudTrail 主控台上檢視事件資訊，包括與該事件相關的資源。對於這些資源，您可以選擇 AWS Config 圖示以在 AWS Config 主控台中檢視該資源的時間表。將此原則附加至您的使用者，以授與他們唯讀 AWS Config 存取權。該政策不會將於 AWS Config中變更設定的許可授予他們。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

如需詳細資訊，請參閱 使用 AWS Config檢視所參考的資源。

授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限

如果您有足夠的權限，您可以在 CloudTrail 主控台中檢視和設定事件傳遞至 CloudWatch 記錄檔。這些權限可能超出授予 CloudTrail系統管理員的權限。將此原則附加至將設定及管理與 CloudWatch 記錄 CloudTrail整合的系統管理員。此原則不會直接授與他們記錄檔 CloudTrail 或 CloudWatch 記錄檔中的權限，而是授與建立和設定角色所需的權限， CloudTrail將假設成功將事件傳遞至您的 CloudWatch 記錄群組。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

如需詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。

其他資訊

若要進一步了解如何使用 IAM 提供身分識別，例如使用者和角色、存取帳戶中的資源，請參閱 IAM 使用者指南中的 AWS 資源入門和存取管理。

AWS CloudTrail 資源型政策範例

CloudTrail 支援用於 CloudTrail Lake 整合的 CloudTrail 管道的資源型權限原則。如需有關建立與 CloudTrail Lake 整合的詳細資訊，請參閱建立與事件來源以外的整合 AWS。

政策所需的資訊取決於整合類型。

- 若要進行方向整合， CloudTrail 需要政策包含合作夥伴的 AWS 帳戶 ID，並要求您輸入合作夥伴提供的唯一外部 ID。 CloudTrail 當您使用 CloudTrail 主控台建立整合時，會自動將合作夥伴的 AWS 帳戶 ID 新增至資源策略。請參閱合作夥伴的說明文件，以瞭解如何取得政策所需的 AWS 帳戶 數字。
- 對於解決方案整合，您必須至少指定一個 AWS 帳戶 ID 作為主參與者，並且可以選擇性地輸入外部 ID，以防止混淆副手。

資源型政策的需求如下：

- 政策中定義的資源 ARN 必須與政策所連接的通道 ARN 相符。
- 政策僅包含一個動作：`cloudtrail-data:PutAuditEvents`
- 政策至少包含一個陳述式。政策最多可以有 20 個陳述式。
- 每個陳述式至少包含一個主體。陳述式最多可以有 50 個主體。

通道擁有者可以在通道上呼叫 `PutAuditEvents` API，除非政策拒絕擁有者存取資源。

主題

- 範例：提供通道存取權給主體
- 範例：使用外部 ID 預防混淆代理人

範例：提供通道存取權給主體

下列範例會將權限授與具有 ARN 的主體 `arn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root`，以及`arn:aws:iam::123456789012:root`使用 ARN 呼叫 CloudTrail 頻道上的 PutAuditEventsAPI。`arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
```

```
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

範例：使用外部 ID 預防混淆代理人

下列範例使用外部 ID 來處理和預防混淆代理人。混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。

整合合作夥伴建立要在政策中使用的外部 ID。然後，在建立整合的過程中向您提供該外部 ID。該值可為任何唯一字串，例如密碼短語或帳戶號碼。

此範例會將權限授與具有 ARN 的主體 `arn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root`，並`arn:aws:iam::123456789012:root`在 PutAuditEventsAPI 呼叫包含原則中定義的外部 ID 值時，呼叫 CloudTrail 通道資源上的 `PutAuditEvents` API。

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
```

```
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
                    "cloudtrail:ExternalId": "uniquePartnerExternalID"
                }
            }
        }
    ]
}
```

Amazon S3 存儲桶政策 CloudTrail

根據預設，所有 Amazon S3 儲存貯體和物件皆為私有。只有資源擁有者 (建立儲存貯體的 AWS 帳戶)，可存取儲存貯體及其包含的物件。資源擁有者可藉由編寫存取政策，將存取許可授予其他資源和使用者。

若要建立或修改 Amazon S3 儲存貯體以接收組織追蹤的日誌檔案，則必須變更儲存貯體政策。如需詳細資訊，請參閱 建立組織的追蹤 AWS Command Line Interface。

若要將日誌檔傳遞到 S3 儲存貯體， CloudTrail 必須具有必要的許可，且無法將其設定為要求者付費儲存貯體。

CloudTrail 在政策中為您新增下列欄位：

- 允許的 SID
- 儲存貯體名稱
- 下列項目的服務主要名稱 CloudTrail
- 儲存記錄檔的資料夾名稱，包括值區名稱、前置詞 (如果已指定)，以及您的 AWS 帳戶 ID

安全最佳實務是將 `aws:SourceArn` 條件金鑰新增至 Amazon S3 儲存貯體政策。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對特定追蹤或追蹤 CloudTrail 寫入 S3 儲存貯體。`aws:SourceArn` 的值一律為使用儲存貯體來存放日誌的追蹤 ARN (或追蹤 ARN 陣列)。請務必將 `aws:SourceArn` 條件金鑰新增至現有追蹤的 S3 儲存貯體政策。

以下策略 CloudTrail 允許從支持將日誌文件寫入存儲桶 AWS 區域。使用適合您組態的值取代*myBucketName*、*[#####]/*、「我的*## ID*」、「*##*」和「*####*」。

S3 儲存貯體政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

如需有關的更多資訊 AWS 區域，請參閱CloudTrail 支援的地區。

內容

- 針對 Amazon S3 儲存貯體政策進行故障診斷
  - 常見的 Amazon S3 政策設定錯誤
  - 變更現有儲存貯體的前綴
- 其他資源

指定記 CloudTrail 錄傳送的現有值區

如果您指定現有的 S3 儲存貯體做為日誌檔交付的儲存位置，則必須將政策附加 CloudTrail 到允許寫入儲存貯體的儲存貯體。

> **Note**
>
> 最佳做法是使用專用的 S3 儲存貯體來處理 CloudTrail 日誌。

若要將必要的 CloudTrail 政策新增至 Amazon S3 儲存貯體

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 選擇您要 CloudTrail 傳送記錄檔的值區，然後選擇 [權限]。
3. 選擇編輯。
4. 將 S3 bucket policy 複製到 Bucket Policy Editor (儲存貯體政策編輯器) 視窗。將斜體預留位置取代成您儲存貯體的名稱、前綴和帳號。如果您在建立追蹤時指定了前綴，請在這裡包含它。前綴是 S3 物件金鑰的選用新增項目，可在您的儲存貯體中建立類似資料夾的組織。

   > **Note**
   >
   > 如果現有值區已附加一或多個政策，請新增陳述式以 CloudTrail 存取該政策或政策。請評估所產生的一組許可，以確保它們適用於將存取儲存貯體的使用者。

從其他帳戶接收日誌檔案

您可以設定 CloudTrail 將日誌檔從多個 AWS 帳戶傳遞到單一 S3 儲存貯體。如需詳細資訊，請參閱 從多個帳戶接收 CloudTrail 日誌文件。

建立或更新 Amazon S3 儲存貯體以存放組織追蹤的日誌檔案

您必須指定 Amazon S3 儲存貯體以接收組織追蹤的日誌檔案。此值區必須具有允 CloudTrail 許將組織的記錄檔放入值區的政策。

以下是名為的 Amazon S3 儲存貯體的範例政策 *myOrganizationBucket*，該儲存貯體由組織的管理帳戶擁有。以組織的值取代*myOrganizationBucket*、*##*、*#### ID*、*####*和 *O ###* ID

此儲存貯體政策包含三個陳述式。

- 第一個語句 CloudTrail 允許在 Amazon S3 存儲桶調用 Amazon S3 `GetBucketAcl` 動作。
- 第二個陳述式允許記錄當追蹤從組織追蹤變更成僅限該帳戶使用的事件。
- 第三個陳述式允許組織追蹤記錄。

範例政策會納入 Amazon S3 儲存貯體政策的 `aws:SourceArn` 條件金鑰。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對特定追蹤或追蹤 CloudTrail 寫入 S3 儲存貯體。在組織追蹤中，`aws:SourceArn` 的值必須是管理帳戶所擁有且使用管理帳戶 ID 的追蹤 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

這個範例政策不允許成員帳戶中任何使用者存取為該組織建立的日誌檔案。在預設情況下，只有管理帳戶才能存取組織日誌檔案。如需有關如何允許成員帳戶中 IAM 使用者對於 Amazon S3 儲存貯體的讀取許可，請參閱 [在 AWS 帳戶之間共用 CloudTrail 記錄檔](#)。

針對 Amazon S3 儲存貯體政策進行故障診斷

下列各節說明如何針對 S3 儲存貯體政策進行故障診斷。

常見的 Amazon S3 政策設定錯誤

當您在建立或更新追蹤時建立新值區時，請將必要的權限 CloudTrail附加至值區。儲存貯體政策使用服務主體名稱"cloudtrail.amazonaws.com"，該名稱 CloudTrail 允許傳遞所有區域的記錄檔。

如果 CloudTrail 未提供區域的記錄，則您的儲存貯體可能有較舊的政策，指定每個區域的 CloudTrail 帳戶 ID。此原則 CloudTrail授與僅針對指定區域傳遞記錄檔的權限。

最佳作法是更新原則以使用 CloudTrail 服務主體的權限。若要執行此作業，請將帳戶 ID ARN 取代成服務主體名稱："cloudtrail.amazonaws.com"。這會 CloudTrail 授予傳遞目前和新區域記錄的權限。安全最佳實務是將 aws:SourceArn 或 aws:SourceAccount 條件金鑰新增至 Amazon S3 儲存貯體政策。這有助於防止未經授權的帳戶存取您的 S3 儲存貯體。如果您具有現有的追蹤，請務必新增一或多個條件金鑰。以下範例顯示推薦的政策組態。使用適合您組態的值取代*myBucketName*、*[### ##]/*、「我的*## ID*」、「*##*」和「*####*」。

Example 儲存貯體政策與服務主體名稱範例

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
```

```
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

變更現有儲存貯體的前綴

如果您嘗試為從追蹤接收日誌的 S3 儲存貯體，新增、修改或移除日誌檔案前綴，您可能會看到下列錯誤：There is a problem with the bucket policy (儲存貯體政策發生問題)。前綴不正確的儲存貯體政策可能會使您的追蹤無法將日誌交付到儲存貯體。若要解決此問題，請使用 Amazon S3 主控台更新儲存貯體政策中的前置詞，然後使用 CloudTrail主控台為追蹤中的儲存貯體指定相同的前置詞。

更新 Amazon S3 儲存貯體的日誌檔案前綴

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 選擇您要修改字首的儲存貯體，然後選擇 Permissions (許可)。
3. 選擇編輯。
4. 在儲存貯體政策中，編輯 `s3:PutObject` 動作下的 `Resource` 項目，以視需要新增、修改或移除日誌檔案 *`prefix/`*。

   ```
   "Action": "s3:PutObject",
         "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
   ```

5. 選擇儲存。
6. 開啟主 CloudTrail 控台，網址為 https://console.aws.amazon.com/cloudtrail/。
7. 選擇您的追蹤，然後針對 Storage location (儲存位置)，按一下鉛筆圖示以編輯您的儲存貯體設定。
8. 針對 S3 bucket (S3 儲存貯體)，選擇您要變更前綴的儲存貯體。
9. 針對 Log file prefix (日誌檔案前綴)，更新前綴以符合您在儲存貯體政策中輸入的前綴。
10. 選擇儲存。

其他資源

如需 S3 儲存貯體和政策的詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的使用儲存貯體政策。

CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策

根據預設，所有 Amazon S3 儲存貯體和物件皆為私有。只有資源擁有者 (建立儲存貯體的 AWS 帳戶)，可存取儲存貯體及其包含的物件。資源擁有者可藉由編寫存取政策，將存取許可授予其他資源和使用者。

若要將 CloudTrail Lake 查詢結果傳遞至 S3 儲存貯體， CloudTrail 必須具有必要的許可，且無法將其設定為要求者付費儲存貯體。

CloudTrail 在政策中為您新增下列欄位：

- 允許的 SID
- 儲存貯體名稱
- 下列項目的服務主要名稱 CloudTrail

安全最佳實務是將 `aws:SourceArn` 條件金鑰新增至 Amazon S3 儲存貯體政策。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對事件資料存放區 CloudTrail 寫入 S3 儲存貯體。

下列政策允許 CloudTrail 將查詢結果從支援的值區傳送至值區 AWS 區域。使用適合您組態的值取*myBucketName*代、我的*## ID* 和*myQueryRunning##*。*MyAccountId* 是用於使用的 AWS 帳戶識別碼 CloudTrail，可能與 S3 儲存貯體的 AWS 帳戶識別碼不同。

> **Note**
>
> 如果您的儲存貯體政策包含 KMS 金鑰的陳述式，我們會建議使用完全合格的 KMS 金鑰 ARN。如果您改用 KMS 金鑰別名，請 AWS KMS 解析要求者帳戶內的金鑰。此行為可能會導致資料使用屬於申請者 (而不是儲存貯體擁有者) 的 KMS 金鑰來加密。
> 如果這是組織事件資料存放區，則事件資料存放區 ARN 必須包含管理帳戶的 AWS 帳戶 ID。這是因為管理帳戶會維護所有組織資源的擁有權。

S3 儲存貯體政策

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

內容

- 為 CloudTrail Lake 查詢結果指定現有值區

- 其他資源

為 CloudTrail Lake 查詢結果指定現有值區

如果您指定現有的 S3 儲存貯體做為 CloudTrail Lake 查詢結果交付的儲存位置，則必須將政策附加到允許將查詢結果傳送 CloudTrail 到儲存貯體的儲存貯體。

> **Note**
>
> 最佳做法是針對 CloudTrail Lake 查詢結果使用專用 S3 儲存貯體。

若要將必要的 CloudTrail 政策新增至 Amazon S3 儲存貯體

1. 前往 https://console.aws.amazon.com/s3/ 開啟的 Amazon Simple Storage Service (Amazon S3) 主控台。
2. 選擇您要 CloudTrail 傳送 Lake 查詢結果的值區，然後選擇 [權限]。
3. 選擇編輯。
4. 將 S3 bucket policy for query results 複製到 Bucket Policy Editor (儲存貯體政策編輯器) 視窗。將斜體預留位置取代成您儲存貯體的名稱、區域和帳戶 ID。

> **Note**
>
> 如果現有值區已附加一或多個政策，請新增陳述式以 CloudTrail 存取該政策或政策。請評估所產生的一組許可，以確保它們適用於存取儲存貯體的使用者。

其他資源

如需 S3 儲存貯體和政策的詳細資訊，請參閱 Amazon Simple Storage Service 使用者指南中的使用儲存貯體政策。

Amazon SNS 主題政策 CloudTrail

若要傳送通知至 SNS 主題， CloudTrail 必須具有必要的權限。 CloudTrail當您在主 CloudTrail 控台中建立或更新追蹤時，建立 Amazon SNS 主題時，會自動將必要的許可附加至主題。

> **Important**
>
> 作為安全最佳實務，為了限制對 SNS 主題的存取，我們強烈建議您在建立或更新線索以傳送 SNS 通知之後，手動編輯附加至 SNS 主題的 IAM 政策以新增條件金鑰。如需詳細資訊，請參閱此主題中的the section called “SNS 主題政策的安全最佳實務”。

CloudTrail 為您新增下列陳述式至政策，並包含下列欄位：

- 允許的 SID。
- 的服務主要名稱 CloudTrail。
- SNS 主題，包含區域、帳戶 ID 和主題名稱。

下列原則允許 CloudTrail 從支援的區域傳送有關記錄檔傳遞的通知。如需詳細資訊，請參閱 CloudTrail 支援的地區。這是當您建立或更新追蹤並選擇啟用 SNS 通知時，附加至新的或現有的 SNS 主題政策的預設政策。

SNS 主題政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
        }
    ]
}
```

若要使用 AWS KMS加密的 Amazon SNS 主題傳送通知，您還必須在的政策中新增下列陳述式，以啟用事件來源 (CloudTrail) 和加密主題之間的相容性。 AWS KMS key

KMS 金鑰政策

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

如需詳細資訊，請參閱啟用來自 AWS 服務的事件來源與加密主題之間的相容性。

內容

SNS 主題政策的安全最佳實務

依預設， CloudTrail 附加至 Amazon SNS 主題的 IAM 政策陳述式可讓 CloudTrail 服務主體發佈到以 ARN 識別的 SNS 主題。若要協助防止攻擊者取得您 SNS 主題的存取權，並代表傳送通知 CloudTrail 給主題收件者，請手動編輯您的 CloudTrail SNS 主題原則，將`aws:SourceArn`條件金鑰新增至附加的原則陳述式 CloudTrail。此金鑰的值是線索的 ARN，或是使用 SNS 主題的線索 ARN 陣列。因為其同時包含特定線索 ID 和擁有線索之帳戶的 ID，所以會限制 SNS 主題只能存取那些具有管理線索許可的帳戶。在您將條件金鑰新增至 SNS 主題原則之前，請先從主 CloudTrail 控台的追蹤設定中取得 SNS 主題名稱。

亦支援 `aws:SourceAccount` 條件金鑰，但不建議使用。

新增 **aws:SourceArn** SNS 主題政策的條件金鑰

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇主題。
3. 選擇線索設定中顯示的 SNS 主題，然後選擇 Edit (編輯)。
4. 展開 Access policy (存取政策)。
5. 在存取政策 JSON 編輯器中，尋找類似下列範例的區塊。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. 為條件新增一個新區塊，aws:SourceArn，如下列範例所示。aws:SourceArn 的值是您要向 SNS 發送通知的線索的 ARN。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. 完成編輯 SNS 主題政策後，請選擇 Save changes (儲存變更)。

新增 **aws:SourceAccount** SNS 主題政策的條件金鑰

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 在導覽窗格中，選擇主題。
3. 選擇線索設定中顯示的 SNS 主題，然後選擇 Edit (編輯)。
4. 展開 Access policy (存取政策)。
5. 在存取政策 JSON 編輯器中，尋找類似下列範例的區塊。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. 為條件新增一個新區塊，`aws:SourceAccount`，如下列範例所示。的值`aws:SourceAccount`是擁有 CloudTrail 追蹤之帳戶的識別碼。此範例將 SNS 主題的存取權限制為只有可以登入 AWS 帳戶 123456789012 的使用者。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. 完成編輯 SNS 主題政策後，請選擇 Save changes (儲存變更)。

指定用於傳送通知的現有主題

您可以手動將 Amazon SNS 主題的許可新增至 Amazon SNS 主控台中的主題政策，然後在主控 CloudTrail 台中指定主題。

手動更新 SNS 主題政策

1. 在 https://console.aws.amazon.com/sns/v3/home 開啟 Amazon SNS 主控台。
2. 選擇 Topics (主題)，然後選擇主題。
3. 選擇 [編輯]，然後向下捲動至 [存取原則]。
4. 新增來自SNS topic policy的陳述式，並為地區、帳戶 ID 和主題名稱的適當值。
5. 如果您的主題是加密主題，則必須 CloudTrail 允許擁有`kms:GenerateDataKey*`和`kms:Decrypt`權限。如需詳細資訊，請參閱 Encrypted SNS topic KMS key policy。
6. 選擇 Save changes (儲存變更)。
7. 返回主 CloudTrail 控台並指定追蹤的主題。

針對 SNS 主題政策進行故障診斷

下列各節說明如何針對 SNS 主題政策進行故障診斷。

案例：

- CloudTrail 沒有傳送區域的通知
- CloudTrail 未傳送組織中成員帳戶的通知

CloudTrail 沒有傳送區域的通知

當您建立新主題作為建立或更新追蹤的一部分時，會將必要的權限 CloudTrail 附加至您的主題。主題原則會使用服務主體名稱`"cloudtrail.amazonaws.com"`，此名稱可 CloudTrail 讓您傳送所有區域的通知。

如果沒 CloudTrail 有傳送區域的通知，您的主題可能有較舊的政策，指定每個區域的 CloudTrail 帳號 ID。此原則 CloudTrail 授予僅針對指定區域傳送通知的權限。

下列主題原則只 CloudTrail 允許傳送指定九個區域的通知：

Example 主題政策與帳戶 ID

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

此原則會根據個別 CloudTrail 帳號 ID 使用權限。若要傳送新區域的記錄檔，您必須手動更新政策以包含該區域的 CloudTrail帳戶 ID。例如，由於已新 CloudTrail 增對美國東部 (俄亥俄) 區域的支援，因此您必須更新政策以新增該區域的帳戶 ID ARN: `"arn:aws:iam::475085895292:root"`。

最佳作法是更新原則以使用 CloudTrail 服務主體的權限。若要執行此作業，請將帳戶 ID ARN 取代成服務主體名稱：`"cloudtrail.amazonaws.com"`。

這會 CloudTrail 授予傳送目前和新區域通知的權限。以下是上述政策的更新版本：

Example 主題政策與服務主體名稱

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
```

```
    }]
}
```

驗證政策具有正確的值：

- 在 `Resource` 欄位中，指定主題擁有者的帳戶號碼。對於您建立的主題，指定您的帳戶號碼。
- 為區域和 SNS 主題名稱指定適當的值。

CloudTrail 未傳送組織中成員帳戶的通知

具有 AWS Organizations 組織追蹤的成員帳戶未傳送 Amazon SNS 通知時，SNS 主題政策的組態可能發生問題。 CloudTrail 即使資源驗證失敗，也會在成員帳戶中建立組織追蹤，例如組織軌跡的 SNS 主題不包含所有成員帳號 ID。如果 SNS 主題原則不正確，就會發生授權失敗。

若要檢查追蹤的 SNS 主題原則是否有授權失敗：

- 從 CloudTrail 主控台，檢查軌跡的詳細資訊頁面。如果授權失敗，詳細資料頁面會包含警告，SNS `authorization failed`並指示要修正 SNS 主題原則。
- 從中 AWS CLI，執行命get-trail-status令。如果授權失敗，命令輸出會包含值為的`LastNotificationError`欄位`AuthorizationError`。

其他資源

如需有關 SNS 主題及訂閱方式的詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》。

疑難排解 AWS CloudTrail 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 CloudTrail 常見問題。

主題

- 我沒有執行操作的授權 CloudTrail
- 我未獲得執行 iam:PassRole 的授權
- 我想允許我以外的人訪 AWS 帳戶 問我的 CloudTrail 資源
- 我未獲得執行 iam:PassRole 的授權
- 當我嘗試建立組織追蹤或事件資料存放區時遇到 NoManagementAccountSLRExistsException 例外狀況

我沒有執行操作的授權 CloudTrail

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 cloudtrail:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 cloudtrail:*GetWidget* 動作存取 *my-example-widget* 資源。

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簽署憑證。

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。

當 mateojackson IAM 使用者嘗試使用主控台檢視追蹤的詳細資料，但沒有適當的 CloudTrail 受管政策 (AWSCloudTrail_FullAccess或 AWSCloudTrail_ReadOnlyAccess) 或對等權限套用至其帳戶時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

在這種情況下，Mateo 會要求管理員更新其政策，以允許該使用者在主控台中存取追蹤資訊和狀態。

如果您使用具有AWSCloudTrail_FullAccess受管政策或同等許可的 IAM 使用者或角色登入，且無法設定 AWS Config 或 Amazon CloudWatch Logs 與追蹤整合，則可能會遺漏與這些服務整合所需的許可。如需詳細資訊，請參閱 授與檢視 CloudTrail 主控台 AWS Config 資訊的權限 及 授與在主控台上檢視和設定 Amazon CloudWatch 日誌資 CloudTrail 訊的權限。

我未獲得執行 **iam:PassRole** 的授權

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給 CloudTrail。

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嘗試使用主控台執行中的動作時，會發生下列範例錯誤 CloudTrail。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 CloudTrail 資源

您可以建立角色，並在多個角色之間共用 CloudTrail 資訊 AWS 帳戶。如需詳細資訊，請參閱 在 AWS 帳戶之間共用 CloudTrail 記錄檔。

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 CloudTrail 支援這些功能，請參閱如何與 IAM AWS CloudTrail 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。
- 若要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。

我未獲得執行 `iam:PassRole` 的授權

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給 CloudTrail。

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`嘗試使用主控台執行中的動作時，會發生下列範例錯誤 CloudTrail。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

當我嘗試建立組織追蹤或事件資料存放區時遇到 **NoManagementAccountSLRExistsException** 例外狀況

`NoManagementAccountSLRExistsException` 例外狀況會在管理帳戶沒有服務連結角色時擲出。當您使用 AWS Organizations AWS CLI 或 API 作業新增委派的系統管理員時，如果服務連結角色不存在，就不會建立該角色。

當您使用組織的管理帳戶新增委派的管理員，或在 CloudTrail 主控台中建立組織追蹤或事件資料存放區時，或使用 AWS CLI 或 CloudTrail API 時，如果您的管理帳戶尚未存在，則會 CloudTrail 自動為您的管理帳戶建立服務連結角色。

如果您尚未新增委派管理員，請使用 CloudTrail 主控台 AWS CLI 或 CloudTrail API 新增委派的管理員。如需有關新增委派管理員的詳細資訊，請參閱新增 CloudTrail 委派管理員和 RegisterOrganizationDelegatedAdmin(API)。

如果您已新增委派管理員，請使用管理帳戶在 CloudTrail 主控台中建立組織追蹤或事件資料存放區，或使用 AWS CLI 或 CloudTrail API。如需有關建立組織軌跡的詳細資訊 使用主控台建立組織追蹤建立組織的追蹤 AWS Command Line Interface，請參閱、和 CreateTrail(API)。

使用服務連結角色 AWS CloudTrail

AWS CloudTrail 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 CloudTrail的唯一 IAM 角色類型。服務連結角色由預先定義， CloudTrail 並包含服務代表您呼叫其他人所需 AWS 服務 的所有權限。

服務連結角色可讓您 CloudTrail 更輕鬆地設定，因為您不需要手動新增必要的權限。 CloudTrail 定義其服務連結角色的權限，除非另有定義，否則只 CloudTrail 能擔任其角色。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。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

服務連結角色權限 CloudTrail

CloudTrail 使用名為的服務連結角色 AWSServiceRoleForCloudTrail— 此服務連結角色用於支援組織追蹤和組織事件資料存放區。

服 AWSServiceRoleForCloudTrail 務連結角色會信任下列服務擔任該角色：

- `cloudtrail.amazonaws.com`

此角色用於支援在中建立和管理 CloudTrail 組織追蹤和 CloudTrail Lake 組織事件資料存放區 CloudTrail。如需詳細資訊，請參閱 建立組織追蹤。

附加到角色的CloudTrailServiceRolePolicy策略允許 CloudTrail 對指定的資源完成以下動作：

- 對所有 CloudTrail 資源執行的動作：
  - `All`
- 對所有 AWS Organizations 資源執行的動作：
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- 針對 CloudTrail 服務主參與者的所有「組織」資源執行動作，Organizations 列出組織的委派管理員：
  - `organizations:ListDelegatedAdministrators`
- 組織事件資料存放區上的停用 Lake 聯合動作：
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

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。

建立服務連結角色 CloudTrail

您不需要手動建立一個服務連結角色。當您建立組織追蹤或組織事件資料存放區，或在 CloudTrail 主控台中新增委派的管理員，或使用 AWS CLI 或 API 作業時，如果服務連結角色尚未存在，則會為您建 CloudTrail立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立組織追蹤或組織事件資料存放區，或新增委派的管理員時， CloudTrail 會再次為您建立服務連結角色。

編輯下列項目的服務連結角色 CloudTrail

CloudTrail 不允許您編輯AWSServiceRoleForCloudTrail服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除下列項目的服務連結角色 CloudTrail

您不需要手動刪除 AWSServiceRoleForCloudTrail 角色。如果從「組織」組 Organizations 中移除AWSServiceRoleForCloudTrail角色，則會自動從該組織中移除角色 AWS 帳戶。 AWS 帳戶 您必須先從組織中移除帳戶，才能從組織管理帳戶的 AWSServiceRoleForCloudTrail 服務連結角色中斷連結或移除政策。

您也可以使用 IAM 主控台 AWS CLI 或 AWS API 手動刪除服務連結角色。若要執行此操作，您必須先手動清除服務連結角色的資源，然後才能手動刪除它。

> **Note**
>
> 當您嘗試刪除資源時，如果 CloudTrail 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

若要移除 AWSServiceRoleForCloudTrail 角色正在使用的資源，您可以執行下列其中一項：

- 從「組織」 AWS 帳戶 中的組 Organizations 中移除。
- 更新追蹤，因此不再是組織追蹤。如需詳細資訊，請參閱 更新追蹤。
- 更新事件資料存放區，使其不再作為組織事件資料存放區。如需詳細資訊，請參閱 使用主控台更新事件資料存放區。
- 刪除追蹤。如需詳細資訊，請參閱 刪除追蹤。
- 刪除事件資料存放區。如需詳細資訊，請參閱 使用主控台刪除事件資料存放區。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除AWSServiceRoleForCloudTrail服務連結角色。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

支援 CloudTrail 服務連結角色的區域

CloudTrail 支援在所有「Organizations」可用的 AWS 區域 位置 CloudTrail 中使用服務連結角色。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 服務 端點。

AWS 受管理的政策 AWS CloudTrail

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

AWS 受管理的策略：**AWSCloudTrail_ReadOnlyAccess**

將AWSCloudTrail_ReadOnlyAccess原則附加至其角色的使用者身分識別可以在中執行唯讀動作 CloudTrail，例如`Get*`、`List*`，以及對追蹤、 CloudTrail Lake 事件資料存放區或 Lake 查詢執行`Describe*`動作。

AWS 受管理的策略：**AWSServiceRoleForCloudTrail**

此CloudTrailServiceRolePolicy原則 AWS CloudTrail 允許代表您對組織追蹤和組織事件資料存放區執行動作。該策略包括描述和列出組織帳戶和委派管理員在組 AWS Organizations 織中的必要 AWS Organizations 權限。

此原則還包含在組織事件資料存放區上停用 Lake 聯盟的必要 AWS Lake Formation 權限 AWS Glue 和權限。

此原則會附加至AWSServiceRoleForCloudTrail服務連結角色，可 CloudTrail 讓您代表執行動作。您無法將此政策連接至使用者、群組或角色。

CloudTrail AWS 受管理策略的更新

檢視有關的 AWS 受管理策略更新的詳細資訊 CloudTrail。如需有關此頁面變更的自動警示，請訂閱 CloudTrail 文件歷史紀錄頁面上的 RSS 摘要。

變更	描述	日期
CloudTrailServiceRolePolicy – 更新現有政策	已更新政策，允許在停用聯合時於組織事件資料存放區中執行以下動作： • glue:DeleteTable • lakeformation:DeregisterResource	2023 年 11 月 26 日
AWSCloudTrail_ReadOnlyAccess – 更新現有政策	CloudTrail 將AWSCloudTrailReadOnlyAccess 策略的名稱變更為AWSCloudTrail_ReadOnlyAccess 。此外，原則中的權限範圍已縮減為 CloudTrail 動作。它不再包含 Amazon S3 或 AWS KMS動 AWS Lambda 作許可。	2022 年 6 月 6 日
CloudTrail 開始追蹤變更	CloudTrail 開始追蹤其 AWS 受管理策略的變更。	2022 年 6 月 6 日

符合性驗證 AWS CloudTrail

協力廠商稽核員會評估其安全性與合規性， AWS CloudTrail 做為多個 AWS 合規計畫的一部分。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 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AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 AWS CloudTrail

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。 AWS 區域提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠在可用區域之間自動容錯移轉，而不會發生中斷。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。如果您特別需要在更遠的地理距離複寫 CloudTrail 日誌檔案，可以針對追蹤 Amazon S3 儲存貯體使用跨區域複寫，以便在不同區 AWS 域中的儲存貯體之間自動異步複製物件。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎架構之外，還 CloudTrail 提供多種功能，協助支援您的資料恢復能力和備份需求。

記錄所有 AWS 區域中事件的追蹤和事件資料儲存

當您將追蹤套用至所有 AWS 區域時， CloudTrail 會在您正在使用的AWS 分割區中的所有其他設定 AWS 區域 中建立具有相同組態的追蹤。新 AWS 增區域時，系統會在新的「區域」中自動建立該軌跡組態。

當您建立多區域事件資料存放區時，會 CloudTrail 收集帳戶中全部發生 AWS 區域 的事件。

CloudTrail 日誌資料的版本控制、生命週期組態和物件鎖定保護

由於 CloudTrail 使用 Amazon S3 儲存貯體存放日誌檔，因此您也可以使用 Amazon S3 提供的功能來協助支援您的資料彈性和備份需求。如需詳細資訊，請參閱 Amazon S3 的恢復能力。

基礎結構安全 AWS CloudTrail

作為託管服務， AWS CloudTrail 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透 CloudTrail 過網路進行存取。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

下列安全性最佳做法也解決了中的基礎結構安全性 CloudTrail：

- 考慮 Amazon VPC 端點存取的線索。
- 考慮 Amazon S3 儲存貯體存取的 Amazon VPC 端點 如需詳細資訊，請參閱使用儲存貯體策略控制來自 VPC 端點的存取。
- 識別和稽核包含 CloudTrail 日誌檔的所有 Amazon S3 儲存貯體。請考慮使用標籤來協助識別追 CloudTrail 蹤和包含 CloudTrail日誌檔的 Amazon S3 儲存貯體。然後，您可以將資源群組用於資 CloudTrail 源。如需更多詳細資訊，請參閱 AWS Resource Groups。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源策略中使用aws:SourceArn和aws:SourceAccount全域條件前後關聯索引鍵，以限制將其他服務 AWS CloudTrail 提供給資源的權限。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 aws:SourceArn。如果您想要允許該帳戶中的任何資源與跨服務使用相關聯，請使用 aws:SourceAccount。

防範混淆代理人問題最有效的方法，是使用 aws:SourceArn 全域條件內容金鑰，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 aws:SourceArn 全域條件內容金鑰，同時使用萬用字元 (*) 表示 ARN 的未知部分。例如 "arn:aws:cloudtrail:*:*AccountID*:trail/*"。如果包含萬用字元，您還必須使用 StringLike 條件運算子。

aws:SourceArn 的值必須是追蹤的 ARN、事件資料存放區或使用資源的通道。

下列範例顯示如何在中使用aws:SourceArn和aws:SourceAccount全域條件前後關聯鍵字 CloudTrail 來避免混淆的副問 CloudTrail 湖泊查詢結果的 Amazon S3 儲存貯體政策題：

安全性最佳做法 AWS CloudTrail

AWS CloudTrail 在您開發和實作自己的安全性原則時，提供許多安全性功能供您考量。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

主題

- CloudTrail 偵探安全最佳實踐
- CloudTrail 預防性安全性最佳做法

CloudTrail 偵探安全最佳實踐

建立線索

若要在 AWS 帳戶中持續記錄事件，您必須建立追蹤。雖然在 CloudTrail 主控台中為管理事件 CloudTrail 提供 90 天的事件歷程記錄資訊，但它不是永久記錄，也不會提供所有可能事件類型的相關資訊。針對持續記錄，以及記錄包含所有您指定的事件類型，您必須建立線索，將日誌檔案傳遞到指定的 Amazon S3 儲存貯體。

若要協助管理您的資 CloudTrail 料，請考慮建立一個記錄所有管理事件的追蹤 AWS 區域，然後建立其他追蹤來記錄資源的特定事件類型，例如 Amazon S3 儲存貯體活動或 AWS Lambda 函數。

以下是您可進行的一些步驟：

- 為您的 AWS 帳戶建立線索。
- 為組織建立線索。

將系統線套用至所有 AWS 區域

若要取得 IAM 身分或 AWS 帳戶中服務所採取的事件的完整記錄，應將每個追蹤設定為全部記錄事件 AWS 區域。藉由記錄 all 中的事件 AWS 區域，您可以確保 AWS 帳戶中發生的所有事件都會記錄下來，而不論事件發生在哪個 AWS 區域。這包括記錄全域服務事件，這些事件會記錄到該服務特定的 AWS 區域。當您建立適用於所有區域的追蹤時，會 CloudTrail 記錄每個區域中的事件，並將 CloudTrail 事件日誌檔傳遞至您指定的 S3 儲存貯體。如果在您建立套用至所有區域的追蹤之後新增 AWS 區域，則會自動包含新的區域，並記錄該區域中的事件。這是您在 CloudTrail 主控台中建立追蹤時的預設選項。

以下是您可進行的一些步驟：

- 為您的 AWS 帳戶建立線索。
- 更新現有線索來記錄所有 AWS 區域中的事件。
- 實作進行中的偵探控制項，以協助確保建立的所有追蹤都會在中使 AWS 區域 用multi-region-cloud-trail已啟用的規則記錄事件 AWS Config。

啟用 CloudTrail 記錄檔完整性

驗證過的日誌檔案對於安全和鑑識調查尤其重要。例如，驗證過的日誌檔案可讓您積極宣告日誌檔案本身尚未變更，或該特定 IAM 身分登入資料已執行特定 API 活動。記 CloudTrail 錄檔完整性驗證程序也會讓您知道記錄檔是否已遭刪除或變更，或是確定在指定期間內未傳送任何記錄檔到您的帳戶。CloudTrail 記錄檔完整性驗證使用業界標準演算法：用於雜湊的 SHA-256 和 SHA-256 搭配 RSA 進行數位簽署。這使得在計算上不可行修改，刪除或偽造 CloudTrail日誌文件而不進行檢測。如需詳細資訊，請參閱 啟用驗證並驗證檔案。

與 Amazon CloudWatch 日誌集成

CloudWatch 記錄可讓您監視和接收由擷取之特定事件的警示 CloudTrail。傳送至 CloudWatch 記錄的事件是設定為由追蹤記錄的事件，因此請確定您已設定追蹤或追蹤，以記錄您感興趣監視的事件類型 (管理事件和/或資料事件)。

例如，您可以監視金鑰安全性和網路相關的管理事件，例如失敗的 AWS Management Console 登入事件。

以下是您可進行的一些步驟：

- 檢閱的範例CloudWatch記錄檔整合 CloudTrail。
- 配置您的跟踪以將事件發送到 CloudWatch 日誌。
- 請考慮實作進行中的偵測控制項，以協助確保所有追蹤都將事件傳送至 CloudWatch 記錄檔進行監視，方法是使用中的 cloud-trail-cloud-watch-logs 啟用規則。 AWS Config

使用 Amazon GuardDuty

Amazon GuardDuty 是一種威脅偵測服務，可協助您保護 AWS 環境中的帳戶、容器、工作負載和資料。透過使用機器學習 (ML) 模型，以及異常和威脅偵測功能， GuardDuty 持續監控不同的記錄檔來源，以識別環境中潛在的安全風險和惡意活動，並排定優先順序。

例如，如果偵測到透過執行個體啟動角色專為 Amazon EC2 執行個體建立的登入資料，但正在從其他帳戶使用的登入資料，則 GuardDuty 會偵測潛在的登入資料洩漏。 AWS如需詳細資訊，請參閱 Amazon GuardDuty 使用者指南。

使用 AWS Security Hub

監視您的使用， CloudTrail 因為它與安全性最佳做法相關的使用方式使用AWS Security Hub。Security Hub 會透過偵測性安全控制來評估資源組態和安全標準，協助您遵守各種合規架構。如需有關使用 Security Hub 評估 CloudTrail 資源的詳細資訊，請參閱使用AWS Security Hub 者指南中的AWS CloudTrail 控制項。

CloudTrail 預防性安全性最佳做法

下列的最佳作法 CloudTrail 可協助防止安全性事件發生。

記錄到專用和集中式的 Amazon S3 儲存貯體

CloudTrail 記錄檔是 IAM 身分或 AWS 服務所採取之動作的稽核記錄。這些日誌的完整性、完成度和可用性對於趨勢的增長和稽核目的相當重要。透過記錄到專用和集中式的 Amazon S3 儲存貯體，您可以強制執行嚴格的安全控制、存取和職責劃分。

以下是您可進行的一些步驟：

- 創建一個單獨的 AWS 帳戶作為日誌存檔帳戶。如果您使用 AWS Organizations，請在組織中註冊此帳戶，並考慮建立組織追蹤記錄組織中所有 AWS 帳戶的資料。
- 如果您不使用「Organizations」，但想要記錄多個 AWS 帳戶的資料，請建立追蹤，以便在此記錄封存帳戶中記錄活動。限制存取此帳戶為信任的管理使用者，具備帳戶和稽核資料的存取權。
- 在建立追蹤的過程中，無論是組織追蹤還是單一 AWS 帳戶的追蹤，都可以建立專用的 Amazon S3 儲存貯體來存放此追蹤的日誌檔。
- 如果您想要記錄多個 AWS 帳戶的活動，請修改值區政策，以允許記錄您想要記錄帳 AWS 戶活動的所有 AWS 帳戶記錄和儲存記錄檔。
- 如果您不是使用組織線索、為您所有 AWS 帳戶建立線索，從日誌存檔帳戶中指定 Amazon S3 儲存貯體。

將伺服器端加密與 AWS KMS 受管理金鑰

根據預設，傳送 CloudTrail 到 S3 儲存貯體的記錄檔會使用具有 KMS 金鑰 (SSE-KMS) 的伺服器端加密來加密。若要搭配使用 SSE-KMS CloudTrail，您可以建立和管理 AWS KMS key，也稱為 KMS 金鑰。

> **Note**
>
> 如果您使用 SSE-KMS 和日誌檔案驗證，而您修改 Amazon S3 儲存貯體政策僅允許 SSE-KMS 加密檔案，您將無法建立利用儲存貯體的線索，除非您修改儲存貯體政策為允許 AES256 加密，如下列範例政策所示。
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

以下是您可進行的一些步驟：

- 檢閱使用 SSE-KMS 加密日誌檔案的優勢。
- 建立用於加密日誌檔案的 KMS 金鑰。
- 設定日誌檔案加密您的線索。

- 請考慮實作持續的偵探控制項，以協助確保所有追蹤都使用中cloud-trail-encryption-enabled的規則，透過 SSE-KMS 加密記錄檔。 AWS Config

將條件索引鍵新增至預設的 Amazon SNS 主題政策

當您設定追蹤以傳送通知至 Amazon SNS 時，會將政策聲明 CloudTrail 新增至 SNS 主題存取政策，以 CloudTrail 便將內容傳送至 SNS 主題。為了安全性最佳作法，我們建議您在 CloudTrail 原則陳述式中新增 `aws:SourceArn` (或選擇性`aws:SourceAccount`) 條件金鑰。這有助於防止未經授權的帳戶存取您的 SNS 主題。如需詳細資訊，請參閱 Amazon SNS 主題政策 CloudTrail。

實作最低權限存取到 Amazon S3 儲存貯體，就是存放日誌檔案的位置

CloudTrail 追蹤將事件記錄到您指定的 Amazon S3 儲存貯體。這些記錄檔包含 IAM 身分識別和 AWS 服務所採取之動作的稽核記錄。這些日誌檔案的完整性和完程度對於稽核和鑑定目的相當重要。為了確保完整性，您在建立或修改用於存放 CloudTrail 日誌檔的任何 Amazon S3 儲存貯體的存取時，應遵守最低權限原則。

採取下列步驟：

- 檢閱 Amazon S3 儲存貯體政策 任何存放日誌檔案的儲存貯體，並調整其在必要時移除任何不必要的存取。如果您使用 CloudTrail 主控台建立追蹤，系統會為您產生此儲存貯體政策，但也可以手動建立和管理。
- 安全最佳實務是務必手動將 `aws:SourceArn` 條件金鑰新增至儲存貯體政策。如需詳細資訊，請參閱 Amazon S3 存儲桶政策 CloudTrail。
- 如果您使用相同的 Amazon S3 儲存貯體來存放多個 AWS 帳戶的日誌檔，請遵循接收多個帳戶的日誌檔的指引。
- 如果您使用組織線索，確保您遵循組織線索，並檢閱 建立組織的追蹤 AWS Command Line Interface 中組織線索 Amazon S3 儲存貯體的範例政策。
- 檢閱 Amazon S3 安全文件和逐步解說保護儲存貯體的範例。

在您儲存日誌檔案的 Amazon S3 儲存貯體上啟用 MFA Delete

在設定多重要素驗證 (MFA) 時，嘗試變更儲存貯體的版本控制狀態或刪除某個儲存貯體中的物件版本需要額外的身分驗證。如此一來，即時使用者取得具有永久刪除 Amazon S3 物件許可之 IAM 使用者的密碼，您仍然可以防止可能損壞您的日誌檔案的操作。

以下是您可進行的一些步驟：

- 檢閱《Amazon Simple Storage Service 使用者指南》中的 MFA Delete 指引。
- 新增 Amazon S3 儲存貯體政策需要 MFA。

> **Note**
>
> 您無法搭配使用 MFA 刪除與生命週期組態。如需有關生命週期組態以及它們如何與其他組態互動的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的生命週期與其他儲存貯體。

設定 Amazon S3 儲存貯體上的物件生命週期，也就是存放日誌檔案的地方

CloudTrail 追蹤預設值是無限期地將日誌檔存放在針對追蹤設定的 Amazon S3 儲存貯體中。您可以使用 Amazon S3 物件生命週期管理規則 來定義自己的保留政策，以便更能滿足您的業務和稽核需求。例如，您可能想要存檔一年以上的日誌檔案到 Amazon Glacier，或刪除超過特定時間的日誌檔案。

> **Note**
>
> 已啟用 Multi-Factor Authentication (MFA) 之儲存貯體上不支援生命週期組態。

限制對 AWSCloudTrail_FullAccess策略的存取

具有該AWSCloudTrail_FullAccess策略的使用者可以停用或重新設定其 AWS 帳戶中最敏感和最重要的稽核功能。此政策不適用於共用或廣泛套用至您 AWS 帳戶中的 IAM 身分。將此政策的應用限制在盡可能少的個人，以及您希望擔任 AWS 帳戶管理員的人員。

使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)

根據預設，傳送 CloudTrail 至儲存貯體的記錄檔會使用具有 KMS 金鑰 (SSE-KMS) 的伺服器端加密來加密。如果您未啟用 SSE-KMS 加密，您的記錄會使用 SSE-S3 加密加密。

> **Note**
>
> 啟用伺服器端加密可加密日誌檔案，但未使用 SSE-KMS 加密摘要檔案。摘要檔案是使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。

如果您將現有 S3 儲存貯體與 S3 儲存貯體金鑰搭配使用，則 CloudTrail 必須獲得金鑰政策中的許可，才能使用 AWS KMS 動作`GenerateDataKey`和`DescribeKey`。如果 `cloudtrail.amazonaws.com` 未授與金鑰政策中的這些許可，則無法建立或更新追蹤。

若要搭配使用 SSE-KMS CloudTrail，您可以建立和管理 KMS 金鑰，也稱為. AWS KMS key 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 CloudTrail 記錄檔。解密是透過 S3 無縫進行。當獲得授權的金鑰使用者讀取 CloudTrail 日誌檔時，S3 會管理解密，授權的使用者能夠以未加密的形式讀取日誌檔。

這種方法具有下列優勢：

- 您可以自行建立和管理 KMS 加密金鑰。
- 您可以使用單一 KMS 金鑰來加密和解密所有區域之多個帳戶的日誌檔案。
- 您可以控制誰可以使用您的密鑰來加密和解密 CloudTrail 日誌文件。您可以根據需求將金鑰的許可指派給組織中的使用者。
- 您可以增強安全性。若要使用此功能讀取日誌檔案，則需要以下許可：
  - 針對包含日誌檔案的儲存貯體，使用者必須擁有 S3 讀取許可。
  - 使用者還必須套用允許 KMS 金鑰政策解密許可的政策或角色。
- 由於 S3 會自動解密授權使用 KMS 金鑰之使用者請求的記錄檔，因此 CloudTrail 記錄檔的 SSE-KMS 加密與讀取記錄資料的應用程式向後相容。 CloudTrail

Note

您選擇的 KMS 金鑰必須建立在與接收日誌檔的 Amazon S3 儲存貯體相同的 AWS 區域中。例如，如果該日誌檔案將存放在美國東部 (俄亥俄) 區域中的儲存貯體，則您必須建立或選擇該區域中建立的 KMS 金鑰。若要驗證 Amazon S3 儲存貯體的區域，請在 Amazon S3 主控台中檢查其屬性。

啟用日誌檔案加密

> **Note**
>
> 如果您在 CloudTrail 主控台中建立 KMS 金鑰，請為您 CloudTrail 新增必要的 KMS 金鑰原則區段。如果您在 IAM 主控台中建立金鑰，或者 AWS CLI 需要手動新增必要的政策區段，請遵循下列程序。

若要為 CloudTrail 記錄檔啟用 SSE-KMS 加密，請執行下列高階步驟：

1. 建立 KMS 金鑰。

   - 如需使用建立 KMS 金鑰的相關資訊 AWS Management Console，請參閱AWS Key Management Service 開發人員指南中的建立金鑰。
   - 如需使用建立 KMS 金鑰的相關資訊 AWS CLI，請參閱建立金鑰。

   > **Note**
   >
   > 您選擇的 KMS 金鑰必須與接收您日誌檔案之 S3 儲存貯體位在相同的區域中。若要驗證 S3 儲存貯體的區域，請在 S3 主控台中檢查儲存貯體的屬性。

2. 將原則區段新增至可加密的金鑰， CloudTrail 以及使用者解密記錄檔。

   - 如需政策中所含項目的資訊，請參閱「設定 AWS KMS 金鑰原則 CloudTrail」。

     > **Warning**
     >
     > 請務必在所有需要讀取日誌檔案之使用者的政策中包含解密許可。如果您在將金鑰新增至線索組態之前未先執行此步驟，則沒有解密許可的使用者就無法讀取加密檔案；除非您授與他們那些許可。

   - 如需使用 IAM 主控台編輯政策的資訊，請參閱《AWS Key Management Service 開發人員指南》中的編輯金鑰政策。
   - 如需使用將原則附加至 KMS 金鑰的相關資訊 AWS CLI，請參閱put-key-policy。

3. 更新追蹤以使用您修改其原則的 KMS 金鑰 CloudTrail。

   - 若要使用 CloudTrail 主控台更新追蹤組態，請參閱更新資源以使用您的 KMS 金鑰。

- 若要使用更新軌跡組態 AWS CLI，請參閱啟用和停用 CloudTrail 記錄檔加密 AWS CLI。

CloudTrail 還支持 AWS KMS 多區域鍵。如需多區域金鑰的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的使用多區域金鑰。

下一節說明 KMS 金鑰原則與搭配使用所需的原則區段 CloudTrail。

授與建立 KMS 金鑰的許可

您可以授與使用者使用`AWSKeyManagementServicePowerUser`原則建立 AWS KMS key 的權限。

准許建立 KMS 金鑰的許可

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 選擇您要授予許可的群組或使用者。
3. 選擇 Permissions (許可)，然後選擇 Attach Policy (連接政策)。
4. 搜尋 AWSKeyManagementServicePowerUser，選擇政策，然後選擇 Attach Policy (連接政策)。

   使用者現在具備建立 KMS 金鑰的許可。如需有關建立政策的詳細資訊，請參閱 IAM 使用者指南中的建立 IAM 政策。

設定 AWS KMS 金鑰原則 CloudTrail

您可以通過三種方式創建： AWS KMS key

- CloudTrail 控制台
- AWS 管理主控台
- 該 AWS CLI

> **Note**
>
> 如果您在 CloudTrail 主控台中建立 KMS 金鑰，請為您 CloudTrail 新增必要的 KMS 金鑰原則。您不需要手動新增政策陳述式。請參閱在 CloudTrail 主控台中建立預設 KMS 金鑰原則。

如果您在 AWS 管理或建立 KMS 金鑰 AWS CLI，則必須將原則區段新增至金鑰，以便您可以搭配使用 CloudTrail。此原則必須允許 CloudTrail 使用金鑰來加密您的記錄檔和事件資料存放區，並允許您指定的使用者以未加密的形式讀取記錄檔。

請參閱下列資源：

- 若要使用建立 KMS 金鑰 AWS CLI，請參閱建立金鑰。
- 若要編輯的 KMS 金鑰原則 CloudTrail，請參閱AWS Key Management Service 開發人員指南中的編輯金鑰原則。
- 如需 CloudTrail 使用方式的技術詳細資訊 AWS KMS，請參閱AWS Key Management Service 開發人員指南 AWS KMS中的 AWS CloudTrail 使用方式。

與搭配使用的必要 KMS 金鑰原則區段 CloudTrail

如果您使用 AWS 管理主控台或建立 KMS 金鑰 AWS CLI，則至少必須將下列陳述式新增至 KMS 金鑰原則，才能使用 CloudTrail。

主題

- 適用於追蹤的必要 KMS 金鑰政策
- 適用於事件資料存放區的必要 KMS 金鑰政策

適用於追蹤的必要 KMS 金鑰政策

1. 啟用 CloudTrail 記錄檔加密權限。請參閱授予加密許可。
2. 啟用 CloudTrail 記錄檔解密權限。請參閱授予解密許可。如果您使用帶有 S3 儲存貯體金鑰的現有 S3 儲存貯體，則需要 `kms:Decrypt` 許可才能建立或更新啟用 SSE-KMS 加密的追蹤。
3. 啟用 CloudTrail 此選項可描述 KMS 金鑰屬性。請參閱啟用 CloudTrail 以說明 KMS 金鑰屬性。

安全最佳實務是將 `aws:SourceArn` 條件金鑰新增至 KMS 金鑰政策。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對特定追蹤或追蹤 CloudTrail 使用 KMS 金鑰。`aws:SourceArn` 的值一律為使用 KMS 金鑰的追蹤 ARN (或追蹤 ARN 陣列)。請務必將 `aws:SourceArn` 條件金鑰新增至現有追蹤的 KMS 金鑰政策。

亦支援 `aws:SourceAccount` 條件金鑰，但不建議使用。`aws:SourceAccount` 的值是追蹤擁有者的帳戶 ID，或是組織追蹤的管理帳戶 ID。

> **Important**
>
> 當您為 KMS 金鑰政策新增區段時，請勿變更政策中任何現有的區段。
> 如果追蹤已啟用加密，且 KMS 金鑰已停用，或 KMS 金鑰原則未正確設定 CloudTrail，則 CloudTrail 無法傳遞記錄。

適用於事件資料存放區的必要 KMS 金鑰政策

1. 啟用 CloudTrail 記錄檔加密權限。請參閱授予加密許可。
2. 啟用 CloudTrail 記錄檔解密權限。請參閱授予解密許可。
3. 授予使用者和角色使用 KMS 金鑰加密和解密事件資料存放區的許可。

   當您建立事件資料存放區並使用 KMS 金鑰加密，或在使用 KMS 金鑰加密的事件資料存放區上執行查詢時，您應該擁有 KMS 金鑰的寫入存取權。KMS 金鑰原則必須具有存取權 CloudTrail，而且 KMS 金鑰應由在事件資料存放區上執行作業 (例如查詢) 的使用者來管理。
4. 啟用 CloudTrail 此選項可描述 KMS 金鑰屬性。請參閱啟用 CloudTrail 以說明 KMS 金鑰屬性。

事件資料存放區的 KMS 金鑰政策中不支援 `aws:SourceArn` 和 `aws:SourceAccount` 條件金鑰。

> **Important**
>
> 當您為 KMS 金鑰政策新增區段時，請勿變更政策中任何現有的區段。
> 如果在事件資料存放區上啟用了加密，且 KMS 金鑰已停用或刪除，或 KMS 金鑰原則未正確設定 CloudTrail，則 CloudTrail無法將事件傳遞至您的事件資料存放區。

授予加密許可

Example 允 CloudTrail 許代表特定帳號加密記錄

CloudTrail 需要明確的權限，才能使用 KMS 金鑰代表特定帳戶加密記錄。若要指定帳戶，請將下列必要陳述式新增至您的 KMS 金鑰政策，並將 *`account-id`*、*`region`* 和 *`trailName`* 替換為適當的組態值。您可以在`EncryptionContext`區段中新增其他帳戶 ID，以便讓這些帳戶用 CloudTrail 來使用 KMS 金鑰來加密記錄檔。

安全最佳實務是將 `aws:SourceArn` 條件金鑰新增至追蹤的 KMS 金鑰政策。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對特定追蹤或追蹤 CloudTrail 使用 KMS 金鑰。

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
         "StringLike": {
             "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
         }
    }
}
```

用於加密 CloudTrail Lake 事件資料存放區記錄的 KMS 金鑰政策無法使用條件金鑰`aws:SourceArn`或`aws:SourceAccount`。以下是事件資料存放區的 KMS 金鑰政策範例。

```
{
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

下列範例原則陳述式說明其他帳戶如何使用您的 KMS 金鑰來加密 CloudTrail 記錄檔。

案例

- 您的 KMS 金鑰在帳戶 *111111111111* 中。

- 您和帳戶 *222222222222* 都要加密日誌。

在策略中，您可以將一個或多個使用您的金鑰加密的帳戶新增至 CloudTrail EncryptionContext. 這會限制只 CloudTrail 使用您指定之帳戶的金鑰來加密記錄。當您授予帳號根 *222222222222* 加密記錄檔的權限時，它會將必要權限委派給帳戶管理員，以便將必要權限加密給該帳戶中的其他使用者。帳戶管理員透過變更與這些 IAM 使用者相關聯的政策來執行此操作。

安全最佳實務是將 `aws:SourceArn` 條件金鑰新增至 KMS 金鑰政策。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對指定的追蹤 CloudTrail 使用 KMS 金鑰。事件資料存放區的 KMS 金鑰政策中不支援此條件。

KMS 金鑰政策聲明：

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

如需有關編輯與搭配使用的 KMS 金鑰原則的詳細資訊 CloudTrail，請參閱 AWS Key Management Service 開發人員指南中的編輯金鑰原則。

授予解密許可

在您將 KMS 金鑰新增至 CloudTrail 設定之前，請務必將解密權限授予所有需要這些權限的使用者。具加密許可但不具解密許可的使用者無法讀取加密的日誌。如果您使用帶有 S3 儲存貯體金鑰的現有 S3 儲存貯體，則需要 `kms:Decrypt` 許可才能建立或更新啟用 SSE-KMS 加密的追蹤。

啟用 CloudTrail 記錄檔解密權限

您的金鑰使用者必須獲得明確的權限，才能讀取 CloudTrail 已加密的記錄檔。若要允許使用者讀取加密的日誌，請將下列必要陳述式新增至您的 KMS 金鑰政策，並修改 `Principal` 區段，為您希望可以使用您 KMS 金鑰解密的每個主體 (角色或使用者) 新增程式碼。

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

以下是允許 CloudTrail 服務主體解密追蹤記錄所需的範例原則。

```
{
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

與 CloudTrail Lake 事件資料存放區搭配使用的 KMS 金鑰的解密政策類似於以下內容。值指定為 `Principal` 的使用者或角色 ARN 需要解密許可，才能建立或更新事件資料存放區、執行查詢或取得查詢結果。

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

以下是允許 CloudTrail 服務主體解密事件資料存放區記錄檔所需的範例原則。

```
{
      "Sid": "Allow CloudTrail to decrypt an event data store",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

允許您帳戶中的使用者使用您的 KMS 金鑰解密追蹤日誌

範例

此政策陳述式示範如何允許您帳戶中的使用者或角色，使用您的金鑰讀取您帳戶之 S3 儲存貯體中的加密日誌。

Example 案例

- 您的 KMS 金鑰、S3 儲存貯體和 IAM 使用者 Bob 都在帳戶 *111111111111* 中。
- 您授予 IAM 使用者 Bob 權限，以解密 S3 儲存貯體中的 CloudTrail 日誌。

在金鑰政策中，您可以為 IAM 使用者 Bob 啟用 CloudTrail 記錄解密許可。

KMS 金鑰政策聲明：

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

允許其他帳戶中的使用者使用您的 KMS 金鑰解密追蹤日誌

您可以允許其他帳戶中的使用者使用您的 KMS 金鑰解密追蹤日誌，而非事件資料存放區日誌。您金鑰政策所需的變更，取決於 S3 儲存貯體在您的帳戶中或另一個帳戶中。

允許其他帳戶中的儲存貯體使用者解密日誌

範例

此政策陳述式示範如何允許其他帳戶中的 IAM 使用者或角色，使用您的金鑰從另一個帳戶中的 S3 儲存貯體讀取加密日誌。

案例

- 您的 KMS 金鑰在帳戶 *111111111111* 中。
- IAM 使用者 Alice 和 S3 儲存貯體都在帳戶 *222222222222* 中。

在這種情況下，您 CloudTrail 授予解密帳戶下的日誌的權限*222222222222*，並授予 Alice 的 IAM 用戶政策許可*KeyA*，以使用您的密鑰（在帳戶中）*111111111111*。

KMS 金鑰政策聲明：

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
```

```
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Alice 的 IAM 使用者政策陳述式：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

允許其他帳戶中的使用者從您的儲存貯體解密追蹤日誌

Example

此政策示範另一個帳戶如何使用您的金鑰從您的 S3 儲存貯體讀取加密日誌。

Example 案例

- 您的 KMS 金鑰和 S3 儲存貯體都在帳戶 *111111111111* 中。
- 要從您儲存貯體讀取日誌的使用者位於帳戶 *222222222222* 中。

若要啟用此案例，請為帳戶CloudTrailReadRole中的 IAM 角色啟用解密許可，然後授予其他帳戶擔任該角色的權限。

KMS 金鑰政策聲明：

```
{
```

```
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRole信託實體政策聲明：

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

如需有關編輯與搭配使用的 KMS 金鑰原則的詳細資訊 CloudTrail，請參閱AWS Key Management Service 開發人員指南中的編輯金鑰原則。

啟用 CloudTrail 以說明 KMS 金鑰屬性

CloudTrail 需要能夠描述 KMS 金鑰的屬性。若要啟用此功能，請將下列必要陳述式依原內容新增至您的 KMS 金鑰政策。除了您指定的其他 CloudTrail 權限之外，此陳述式不會授與任何權限。

安全最佳實務是將 `aws:SourceArn` 條件金鑰新增至 KMS 金鑰政策。IAM 全域條件金鑰`aws:SourceArn`有助於確保僅針對特定追蹤或追蹤 CloudTrail 使用 KMS 金鑰。

```
{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

如需使用 KMS 金鑰政策的更多資訊，請參閱《AWS Key Management Service 開發人員指南》中的編輯金鑰政策。

在 CloudTrail 主控台中建立預設 KMS 金鑰原則

如果您在 CloudTrail 主控台 AWS KMS key 中建立，則會自動為您建立下列原則。此政策允許這些許可：

- 允許 KMS 金鑰的 AWS 帳戶 (根) 權限。
- 允許 CloudTrail 加密 KMS 金鑰下的記錄檔並描述 KMS 金鑰。
- 允許指定帳戶中的所有使用者解密日誌檔案。
- 允許指定帳戶中的所有使用者建立 KMS 金鑰的 KMS 別名。
- 已建立追蹤的帳戶能夠用於帳戶 ID 跨帳戶日誌解密。

主題

- CloudTrail Lake 事件資料存放區的預設 KMS 金鑰原則
- 適用於追蹤的預設 KMS 金鑰政策

CloudTrail Lake 事件資料存放區的預設 KMS 金鑰原則

以下是針對與 CloudTrail Lake 中的事件資料存放區搭配使用 AWS KMS key 而建立的預設原則。

```
{
```

```
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores. Created
${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

適用於追蹤的預設 KMS 金鑰政策

以下是針對您與追蹤搭配使用的預設原則 AWS KMS key 所建立。

> **Note**
>
> 此政策包括允許使用 KMS 金鑰跨帳戶解密日誌檔案的陳述式。

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:root",
                    "arn:aws:iam::account-id:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
        {
```

```
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        }
    ]
}
```

更新資源以使用您的 KMS 金鑰

在 AWS CloudTrail 主控台中，更新追蹤或事件資料存放區以使用 AWS Key Management Service 金鑰。請注意，使用您自己的 KMS 金鑰會產生加密和解密的 AWS KMS 成本。如需詳細資訊，請參閱 AWS Key Management Service 定價。

主題

- 更新追蹤以使用 KMS 金鑰
- 更新事件資料存放區以使用 KMS 金鑰

更新追蹤以使用 KMS 金鑰

若要更新追蹤以使用您修改 AWS KMS key 的項目 CloudTrail，請在 CloudTrail 主控台中完成下列步驟。

> **Note**
>
> 透過下列程序來更新追蹤會使用 SSE-KMS 加密日誌檔案，而不是摘要檔案。摘要檔案是使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。
> 如果您將現有的 S3 儲存貯體搭配 S3 儲存貯體使用 S3 儲存貯體，則 CloudTrail 必須獲得金鑰政策中的許可，才能使用 AWS KMS 動作`GenerateDataKey`和`DescribeKey`。如果 `cloudtrail.amazonaws.com` 未授與金鑰政策中的這些許可，則無法建立或更新追蹤。

若要使用更新系統線 AWS CLI，請參閱啟用和停用 CloudTrail 記錄檔加密 AWS CLI。

更新追蹤以使用您的 KMS 金鑰

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。
2. 選擇 Trails (追蹤)，然後選擇追蹤名稱。
3. 在 General details (一般詳細資訊) 中，選擇 Edit (編輯)。
4. 針對 Log file SSE-KMS encryption (日誌檔案 SSE-KMS 加密)，如果您想要使用 SSE-KMS 而非 SSE-S3 來加密日誌檔案，請選擇 Enabled (啟用)。預設為啟用。如果您未啟用 SSE-KMS 加密，則會使用 SSE-S3 加密來加密您的日誌。如需 SSE-KMS 加密的詳細資訊，請參閱使用伺服器端加密搭配 AWS Key Management Service (SS E-KMS)。如需 SSE-S3 加密的詳細資訊，請參閱搭配使用伺服器端加密與 Amazon S3 受管加密金鑰 (SSE-S3)。

   選擇 Existing (現有) 來使用 AWS KMS key更新您的追蹤。選擇與接收您日誌檔案之 S3 儲存貯體位在相同區域中的 KMS 金鑰。若要驗證 S3 儲存貯體的區域，請在 S3 主控台中檢視其屬性。

   > **Note**
   >
   > 您也可以從另一個帳戶輸入金鑰的 ARN。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。金鑰原則必須允許 CloudTrail 使用金鑰來加密記錄檔，並允許您指定的使用者以未加密的形式讀取記錄檔。如需手動編輯金鑰政策的資訊，請參閱「設定 AWS KMS 金鑰原則 CloudTrail」。

   在AWS KMS 別名中，以格式指定您變更原則以搭配 CloudTrail使用的別名`alias/`*`MyAliasName`*。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。

您可以輸入別名、ARN 或全域唯一金鑰 ID。如果 KMS 金鑰屬於其他帳戶，請驗證金鑰政策具備許可，可讓您使用它。此值的格式可為下列其中之一：

- 別名：`alias/MyAliasName`
- 別名 ARN：`arn:aws:kms:region:123456789012:alias/MyAliasName`
- 金鑰 ARN：`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- 全域唯一金鑰 ID：`12345678-1234-1234-1234-123456789012`

5. 選擇 Update trail (更新追蹤)。

> **Note**
>
> 如果您選擇的 KMS 金鑰已停用或待刪除，您將無法使用該 KMS 金鑰來儲存追蹤。您可以啟用 KMS 金鑰或選擇另一個。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的金鑰狀態：對 KMS 金鑰的影響。

更新事件資料存放區以使用 KMS 金鑰

若要更新事件資料倉庫以使用您為其修改 AWS KMS key 的事件資料倉庫 CloudTrail，請在 CloudTrail 主控台中完成以下步驟。

若要使用更新事件資料倉庫 AWS CLI，請參閱使用更新事件資料倉庫 AWS CLI。

> **Important**
>
> 停用或刪除 KMS 金鑰，或移除金鑰的 CloudTrail 權限，可防 CloudTrail 止將事件擷取到事件資料存放區，並防止使用者查詢使用金鑰加密的事件資料存放區中的資料。將事件資料存放區與 KMS 金鑰建立關聯後，就無法移除或變更 KMS 金鑰。停用或刪除您搭配事件資料存放區使用的 KMS 金鑰之前，請先刪除或備份您的事件資料存放區。

若要更新事件資料存放區以使用您的 KMS 金鑰

1. 請登入 AWS Management Console 並開啟 CloudTrail 主控台，網址為 https://console.aws.amazon.com/cloudtrail/。

2. 在導覽窗格中，選擇 Lake 中的 Event data stores (事件資料存放區)。選擇事件資料存放區以進行更新。
3. 在 General details (一般詳細資訊) 中，選擇 Edit (編輯)。
4. 針對加密，如果未啟用，請選擇使用我自己的 AWS KMS key，以使用您自己的 KMS 金鑰來加密日誌檔案。

   選擇 Existing (現有) 來使用您的 KMS 金鑰更新您的事件資料存放區。選擇與事件資料存放區位在相同區域中的 KMS 金鑰。不支援來自另一個帳戶的金鑰。

   在輸入 AWS KMS 別名中，以格式指定變更原則以搭配 CloudTrail使用的別名`alias/`*`MyAliasName`*。如需詳細資訊，請參閱 更新資源以使用您的 KMS 金鑰。

   您可以選擇別名，或使用全域唯一金鑰 ID。此值的格式可為下列其中之一：

   - 別名：`alias/`*`MyAliasName`*
   - 別名 ARN：`arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
   - 金鑰 ARN：`arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-123456789`0
   - 全域唯一金鑰 ID：`12345678-1234-1234-1234-123456789012`
5. 選擇儲存變更。

> **Note**
>
> 如果您選擇的 KMS 金鑰已停用或待刪除，您將無法使用該 KMS 金鑰來儲存事件資料存放區組態。您可以啟用 KMS 金鑰，或選擇不同的金鑰。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的金鑰狀態：對 KMS 金鑰的影響。

啟用和停用 CloudTrail 記錄檔加密 AWS CLI

本主題說明如何使用啟用和停用 SSE-KMS 記錄檔加密。 CloudTrail AWS CLI如需背景資訊，請參閱使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)。

主題

- 啟用 CloudTrail 記錄檔加密 AWS CLI
- 使用停用 CloudTrail 記錄檔加密 AWS CLI

啟用 CloudTrail 記錄檔加密 AWS CLI

啟用追蹤的日誌檔案加密

1. 使用 AWS CLI建立金鑰。您建立的金鑰必須與接收 CloudTrail 日誌檔的 S3 儲存貯體位於相同的區域。對於此步驟，您可以使用 AWS KMS create-key命令。
2. 取得現有的金鑰原則，以便您可以修改它以配合使用 CloudTrail。您可以使用 AWS KMS get-key-policy命令擷取金鑰原則。
3. 將必要的區段新增至金鑰原則， CloudTrail 以便加密，使用者可以解密您的記錄檔。確定將解密許可授予所有讀取日誌檔案的使用者。請不要變更任何政策的現有區段。如需要包含之政策區段的詳細資訊，請參閱 設定 AWS KMS 金鑰原則 CloudTrail。
4. 使用 AWS KMS put-key-policy命令將修改的 JSON 政策檔案附加至金鑰。
5. 使用`--kms-key-id`參數執行 CloudTrail `create-trail`或`update-trail`命令。此命令會啟用日誌加密。

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

此`--kms-key-id`參數會指定您修改其原則的金鑰 CloudTrail。它可以是下列格式中的任何一種：

- 別名。範例：`alias/MyAliasName`
- 別名 ARN。範例：`arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- 金鑰 ARN。範例：`arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- 全域唯一金鑰 ID。範例：`12345678-1234-1234-1234-123456789012`

以下是回應範例：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
```

```
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "my-bucket-name"
}
```

KmsKeyId 元素的存在指出已啟用日誌檔案加密。加密日誌檔案應該會在大約 5 分鐘內出現在您的儲存貯體中。

啟用事件資料存放區的日誌檔案加密

1. 使用 AWS CLI建立金鑰。您建立的金鑰必須與事件資料存放區位於相同區域中。對於此步驟，請運行 AWS KMS create-key命令。
2. 取得要編輯的現有金鑰原則，以便搭配使用 CloudTrail。您可以透過執行 AWS KMS get-key-policy命令來取得金鑰原則。
3. 將必要的區段新增至金鑰原則， CloudTrail 以便加密，使用者可以解密您的記錄檔。確定將解密許可授予所有讀取日誌檔案的使用者。請不要變更任何政策的現有區段。如需要包含之政策區段的詳細資訊，請參閱 設定 AWS KMS 金鑰原則 CloudTrail。
4. 透過執行 AWS KMS put-key-policy命令，將編輯的 JSON 政策檔案附加至金鑰。
5. 執行 CloudTrail `create-event-data-store`或`update-event-data-store`命令，然後加入`--kms-key-id`參數。此命令會啟用日誌加密。

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

此`--kms-key-id`參數會指定您修改其原則的金鑰 CloudTrail。它可以是下列四種格式中的任何一種：

- 別名。範例：`alias/MyAliasName`
- 別名 ARN。範例：`arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- 金鑰 ARN。範例：`arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- 全域唯一金鑰 ID。範例：`12345678-1234-1234-1234-123456789012`

以下是回應範例：

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

KmsKeyId 元素的存在指出已啟用日誌檔案加密。加密日誌檔案應該會在大約 5 分鐘內出現在您的事件資料存放區中。

使用停用 CloudTrail 記錄檔加密 AWS CLI

若要停止加密追蹤中的日誌，請執行 update-trail 並將空白字串傳送至 kms-key-id 參數：

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

以下是回應範例：

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

沒有 `KmsKeyId` 值指出不再啟用日誌檔案加密。

> **Important**
>
> 您無法停止事件資料存放區上的日誌檔案加密。

文件歷史紀錄

下表說明的文件的重要變更 AWS CloudTrail。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

- API 版本：2013 年 11 月 1 日
- 最新的文件更新

變更	描述	日期
已更新的文件	已新增區段，說明如何使用進階事件選取器篩選資料事件。如需詳細資訊，請參閱使用進階事件選取器篩選資料事件。	2024年5月29 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon Kinesis 資料串流和串流取用者上記 CloudTrail 錄資料事件。如需詳細資訊，請參閱資料事件。	2024年5月21 日
已更新的文件	已更新「CloudTrail 湖泊支援區域」頁面，以新增亞太區域 (海德拉巴) 區域 (距離 ap-south-2)、歐洲 (蘇黎世) 區域 (歐 eu-central-2) 和以色列 (特拉維夫) 區域 (il-central-1)。	2024年5月16日
已新增的功能	您現在可以使用進階事件選取器，在 AWS Step Functions 狀態機器上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。	2024年5月16日
已更新的文件	已新增關於使用檢視 CloudTrail 成本和使用量的章節 AWS Cost Explorer。如需詳細資訊，請參閱以下方式檢視	2024 年 5 月 14 日

	CloudTrail 成本和用量 AWS Cost Explorer。	
已新增的功能	您現在可以使用進階事件選取器，在 Amazon Q 應用程式上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。	2024年5月1日
已更新的文件	使用者指南區段和頁面標題的一般組織改良功能，其中包括下列項目：將 CloudTrail 記錄事件參考頁面的標題變更為了解 CloudTrail 事件，並新增管理事件、資料事件和 Insights 事件的描述。將「設定」頁面的標題變更為 CloudTrail「設定」。將 [記錄資料事件]、[記錄管理事件] 和 [記錄見解] 事件頁面移至了解 CloudTrail 事件區段。將CloudTrail記錄檔範例頁面移至記CloudTrail 錄檔區段。新增個別頁面以列出 CloudTrail Lake 事件資料存放區、查詢和整合的 AWS CLI 指令。	2024年4月10日
已更新的文件	已更新CloudTrail 湖泊支援的區域頁面，以新增歐洲 (西班牙) 區域 (eu-south-2)。	2024年4月10日
已新增的服務支援	此版本支援 AWS 控制目錄。如需詳細資訊，請參AWS 服務 閱記錄 AWS 控制目錄 API 呼叫使用的主題 CloudTrail和 AWS CloudTrail.	2024年4月8日

已新增的服務支援	此版本支援 AWS 期限雲端。如需詳細資訊，請參閱的AWS 服務 主題 CloudTrail。	2024年4月2日
已新增的功能	AWS CloudTrail 事件版本現在是 1.10。如需詳細資訊，請參閱CloudTrail 記錄內容。	2024年3月26日
已新增的服務支援	此版本支援 AWS Billing Conductor。如需詳細資訊，請參AWS 服務 閱使用 AWS CloudTrail. CloudTrail AWS Billing Conductor	2024年3月12日
已新增的功能	您現在可以使用進階事件選取器，在 AWS X-Ray 追蹤和 AWS Systems Manager 受管理節點上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。	2024年3月7日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon Simple Workflow Service (Amazon SWF) 網域上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。	2024年2月14日
已新增的功能	CloudTrail 添加了 `ListInsightsMetricData` API。`ListInsightsMetricData` API 會針對已啟用深入解析的追蹤傳回見解指標資料。如需詳細資訊，請參閱 AWS CloudTrail API 參考ListInsightsMetricData中的。	2024年2月6日

已新增的功能	您現在可以使用進階事件選取器 AWS AppConfig 來記錄 AWS IoT AWS IoT SiteWise、和的 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。	2024 年 1 月 4 日
已新增的功能	您現在可以使用進階事件選取器 AWS IoT Greengrass 來記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。	2023 年 12 月 22 日
新區域支援	CloudTrail 擴大對加拿大西部（卡爾加里）地區的新地區的支持。如需詳細資訊，請參閱CloudTrail 支援的區域。	2023 年 12 月 20 日
已新增的功能	現在，您可以記錄 CloudTrail Amazon Keyspaces（對於 Apache 卡桑德拉） AWS IoT TwinMaker，Amazon RDS 和使用高級事件選擇器的數 AWS Supply Chain 據事件。如需詳細資訊，請參閱資料事件。	2023 年 12 月 20 日
更新的 AWS 受管政策	已更新 CloudTrailServiceRolePolicy 受管政策，允許在停用聯合時於組織事件資料存放區中執行以下動作：`glue:DeleteTable` 和 `lakeformation:DeregisterResource` 。	2023 年 11 月 26 日

已新增的功能	您現在可以聯合 CloudTrail Lake 事件資料存放區，在資料目錄中查看與事件資料存放區相關聯的中繼 AWS Glue 資料，並使用 Amazon Athena 對事件資料執行 SQL 查詢。儲存在 AWS Glue 資料目錄中的表格中繼資料可讓 Athena 查詢引擎瞭解如何尋找、讀取和處理您要查詢的資料。如需詳細資訊，請參閱聯合事件資料存放區。	2023 年 11 月 26 日
已新增的功能	您現在可以使用進階事件選取器 AWS Cloud Map 來記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 11 月 16 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon SQS 訊息上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 11 月 16 日

已新增的功能	CloudTrail Lake 現在為活動資料存放區提供兩種定價選項：一年可延長保留定價和七年保留定價。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。在此版本之前，所有事件資料存放區都使用七年保留定價選項。您可以使用CloudTrail 主控台或 API 作業，AWS CLI將事件資料存放區從使用七年保留定價選項切換為使用一年可延長保留定UpdateEventDataStore價。如需有關定價選項的詳細資訊，請參閱 AWS CloudTrail 定價和事件資料存放區定價選項。	2023 年 11 月 15 日
已新增的功能	您現在可以在 CloudTrail 湖泊中收集「見解」事件。AWS CloudTrail 透過持續分析 CloudTrail 管理事件，深入解析可協助 AWS 使用者識別並回應與 API 呼叫和 API 錯誤率相關的異常活動。若要收集 CloudTrail Lake 中的 Insights 事件，您需要一個來源事件資料存放區來記錄管理事件，並啟用 Insights，以及根據來源事件資料存放區中的異常管理事件活動來收集 Insights 事件的目標事件資料存放區。如需詳細資訊，請參閱為 CloudTrail Insights 事件建立事件資料存放區和記錄見解事件。	2023 年 11 月 9 日

已新增的服務支援	此版本支援 AWS Launch Wizard。如需詳細資訊，請參AWS 服務 閱使用 AWS CloudTrail. CloudTrail AWS Launch Wizard	2023 年 11 月 8 日
已新增的服務支援	此版本支援 Amazon Bedrock。如需詳細資訊，請參閱使用的AWS 服務 主題 CloudTrail和記錄 Amazon 基岩 API 呼叫。 AWS CloudTrail	2023 年 10 月 23 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon CodeWhisperer 自訂上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 10 月 18 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon Timestream CloudTrail 資料庫和表格上記錄資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 9 月 28 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon SNS 主題和平台端點上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 9 月 28 日
已更新的文件	已新增表格，以顯示 AWS Organizations 組織內的管理帳戶、委派管理員帳戶和成員帳戶可以在其中執行的工作 CloudTrail。如需詳細資訊，請參閱組織委派的管理員。	2023 年 9 月 25 日

已新增的服務支援	此版本支援 AWS Marketplace 合約。如需詳細資訊，請參AWS 服務 閱使用的記錄協定 API 呼叫 CloudTrail和記錄主題 AWS CloudTrail。	2023 年 9 月 1 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon Kinesis 影片串流和 Amazon SageMaker 端點上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 8 月 31 日
已新增的服務支援	此版本支援 AWS 應用程式轉換服務。 AWS 應用程序轉換服務是由像 .NET 的 AWS 微服務提取器服務使用的後端服務。如需詳細資訊，請參閱CloudTrail支援的服務和整合。	2023 年 8 月 26 日
已新增的功能	您現在可以使用進階事件選取 AWS Private CA 器，在 Active Directory 的連接器上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 8 月 24 日
已更新的文件	新增 CloudTrail Lake 案例，以示範如何建立事件資料存放區、檢視 CloudTrail Lake 儀表板、將追蹤事件複製到事件資料存放區、檢視和執行範例查詢，以及如何使用 AWS Management Console. 如需詳細資訊，請參閱 CloudTrailLake 的案例	2023 年 8 月 16 日

新區域支援	CloudTrail 擴大對以色列（特拉維夫）地區的新地區的支持。如需詳細資訊，請參閱CloudTrail 支援的區域。	2023 年 8 月 1 日
已新增的服務支援	此版本支援 AWS HealthImaging。如需詳細資訊，請參閱CloudTrail支援的服務和整合和記錄 AWS HealthImaging API 呼叫 AWS CloudTrail。	2023 年 7 月 26 日
已新增的功能	您現在可以使用進階事件選取器，在 AWS HealthImaging 資料存放區上記 CloudTrail 錄資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 7 月 26 日
已新增的功能	您現在可以使用進階事件選取器，在 AWS Systems Manager 控制通道和 Amazon Managed Blockchain 網路上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 6 月 21 日
已新增的功能	您現在可以使用aws cloudtrail verify-query-results指令驗證 CloudTrail Lake 儲存的查詢結果。如需詳細資訊，請參閱使用 AWS CLI確認已儲存查詢結果。	2023 年 6 月 21 日

已新增的服務支援	此版本支援 Amazon Verified Permissions。如需詳細資訊，請參閱CloudTrail支援的服務和整合和記錄使用的 Amazon 驗證許可 API 呼叫 AWS CloudTrail。	2023 年 6 月 13 日
已新增的功能	您現在可以使用 CloudTrail Lake 儀表板來視覺化事件資料存放區中的事件。如需詳細資訊，請參閱檢視 Lake 儀表板。	2023 年 6 月 13 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon 驗證許可政策存放區記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 6 月 13 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon CodeWhisperer 設定檔上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 6 月 6 日
已新增的功能	您現在可以開始和停止事件資料存放區的 CloudTrail 事件擷取。如需有關使用主控台停止事件擷取的資訊，請參閱使事件資料存放區停止擷取事件。如需使用停止事件擷取的相關資訊 AWS CLI，請參閱停止事件資料存放區的擷取。	2023 年 6 月 2 日

已新增的功能	您現在可以使用進階事件選取器，在 Amazon EMR 預寫日誌工作區上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 5 月 31 日
已新增的服務支援	此版本支援 Amazon Security Lake。如需詳細資訊，請參閱CloudTrail支援的服務和整合和記錄使用的 Amazon 安全湖 API 呼叫 AWS CloudTrail。	2023 年 5 月 30 日
已更新的文件	已更新 CloudTrail userIdentity 元素主題，為代表 IAM 身分中心使用者提出的請求加入範例和欄位說明。如需詳細資訊，請參閱 CloudTrail userIdentity 元素。	2023 年 5 月 23 日
已更新的文件	此更新支援下列 CloudTrail處理程式庫的修補程式版本：aws-cloudtrail-processing-library-1.6.1.jar。如需詳細資訊，請參閱上的使用 CloudTrail 處理程式庫和CloudTrail 處理程式庫 GitHub。	2023 年 5 月 23 日
已新增的功能	CloudTrail 湖現在支持所有普雷斯托功能和運營商。如需詳細資訊，請參閱CloudTrail 湖泊 SQL 條件約束。	2023 年 5 月 9 日

已新增的功能	您現在可以使用進階事件選取器，在 Amazon GuardDuty 偵測器上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱使用記錄資料事件和記錄 Amazon GuardDuty API 呼叫 AWS CloudTrail。	2023 年 3 月 30 日
已更新的文件	新增章節關於為事件資料存放區建立使用者定義的成本分配標籤。如需詳細資訊，請參閱為 CloudTrail Lake 事件資料倉庫建立使用者定義的成本配置標籤	2023 年 3 月 24 日
已新增的服務支援	此版本支持 AWS 電信網絡生成器（AWS TNB）。AWS 有關更多信息，請參閱CloudTrail支持的服務和集成和記錄電信網絡生成器 API 調用使用 AWS CloudTrail.	2023 年 2 月 21 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon Cognito 身分識別集區上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 2 月 15 日
已更新的文件	已新增有關 CloudTrail Lake 可用學習資源的新章節。如需詳細資訊，請參閱學習資源。	2023 年 2 月 9 日

已新增的功能	您現在可以使用以外的事件來源建立 CloudTrail Lake 整合 AWS。您可以記錄和儲存來自混合環境中任何來源 (例如在內部部署或雲端、虛擬機器或容器中託管的內部或 SaaS 應用程式) 的使用者活動資料。如需詳細資訊，請參閱與 AWS外部事件來源建立整合。	2023 年 1 月 31 日
已新增的功能	您現在可以使用進階事件選取器，記錄 CloudTrail Lake 頻道上 CloudTrail `PutAuditEvents` 活動的 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2023 年 1 月 31 日
新區域支援	CloudTrail 擴大對亞太區域（墨爾本）區域的支持。如需詳細資訊，請參閱CloudTrail 支援的區域。	2023 年 1 月 24 日
已更新的文件	已新增有關管理資料一致性的新章節 CloudTrail，請參閱中的管理資料一致性 CloudTrail。	2023 年 1 月 18 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon SageMaker 功能商店記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2022 年 12 月 27 日
已新增的服務支援	此版本支援 AWS Marketplace 探索。請參閱 AWS CloudTrail 支援的服務和整合。	2022 年 12 月 15 日

已新增的功能	您現在可以使用進階事件選取器，在 Amazon SageMaker 指標實驗試用元件上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2022 年 12 月 15 日
已新增的功能	您現在可以建立事件資料存放區以包含 AWS Config 組態項目，並使用事件資料存放區來調查生產環境的不合規變更。如需詳細資訊，請參閱建立 AWS Config 組態項目的事件資料存放區。	2022 年 11 月 28 日
新區域支援	CloudTrail 擴大對亞太區域 (海德拉巴) 區域的支援。如需詳細資訊，請參閱CloudTrail 支援的區域。	2022 年 11 月 22 日
已新增的功能	您現在可以使用進階事件選取器，在 Amazon FinSpace 環境上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2022 年 11 月 18 日
新區域支援	CloudTrail 擴大對歐洲（西班牙）區域的新區域的支持。如需詳細資訊，請參閱CloudTrail 支援的區域。	2022 年 11 月 16 日
新區域支援	CloudTrail 將支援擴展至新地區 — 歐洲 (蘇黎世) 區域。如需詳細資訊，請參閱CloudTrail 支援的區域。	2022 年 11 月 9 日

已新增的功能	AWS Organizations 組織的管理帳戶現在可以新增委派的管理員，以管理組織的 CloudTrail 追蹤和事件資料存放區。如需詳細資訊，請參閱組織委派的管理員。	2022 年 11 月 7 日
已新增的功能	您現在可以為 CloudTrail Lake 事件資料存放區啟用 AWS Key Management Service 加密。如需詳細資訊，請參閱建立事件資料存放區。	2022 年 11 月 7 日
已新增的功能	您現在可以在執行查詢時，將 CloudTrail 湖泊查詢結果儲存到 Amazon S3 儲存貯體。如需有關執行查詢的詳細資訊，請參閱執行查詢並儲存查詢結果。如需有關下載查詢結果的詳細資訊，請參閱取得並下載已儲存的查詢結果。	2022 年 10 月 21 日
已新增的功能	您現在可以將 CloudTrail 追蹤事件複製到 CloudTrail Lake 事件資料存放區。如需詳細資訊，請參閱將路徑事件複製到 CloudTrail 湖泊。	2022 年 9 月 19 日
已更新的文件	添加了 CloudTrail 湖泊支持的 Amazon CloudWatch 指標列表。如需詳細資訊，請參閱支援的 CloudWatch 量度。	2022 年 9 月 16 日
已新增的功能	您現在 CloudTrail 可以使用. AWS CLI如需詳細資訊，請參閱 CloudTrail 使用 AWS CLI.	2022 年 9 月 9 日

新區域支援	CloudTrail 擴大對中東 (阿拉伯聯合大公國) 新區域的支援。如需詳細資訊，請參閱CloudTrail 支援的區域。	2022 年 8 月 30 日
已變更的功能	CloudTrail 已將受管理策略的名稱變更AWSCloudTrailReadOnlyAccess 為AWSCloudTrail_ReadOnlyAccess 。此政策中的許可範圍已有所縮減。依預設，該政策不再授予列出所有 Amazon S3 儲存貯體、 AWS Lambda 函數或 AWS KMS 別名的權限。如需詳細資訊，請參閱唯讀存取。	2022 年 6 月 6 日
已變更的功能	作為安全最佳實務，您現在可將 aws:SourceArn 或 aws:SourceAccount 條件金鑰新增至 Amazon S3 儲存貯體政策中的 s3:GetBucketAcl ACL 檢查區塊。如需詳細資訊，請參閱的設定的 Amazon S3 儲存貯體政策 CloudTrail。	2022 年 5 月 11 日

已變更的功能	自 2022 年 2 月 24 日 AWS CloudTrail 起，在源自使用 Proxy 用戶端的 AWS Management Console 工作階段的任何事件中，開始變更`userAgent` 和`sourceIPAddress` 欄位值。對於這些事件，請使用 CloudTrail取代`userAgent` 和`sourceIPAddress` 欄位的值`AWS Internal`。 CloudTrail進行此變更，以標準化其在所 AWS 有服務中記錄服務動作資訊的方式。如需詳細資訊，請參閱CloudTrail 記錄內容。	2022 年 4 月 12 日
已新增的服務支援	此版本支持 Amazon GameSparks。請參閱 AWS CloudTrail 支援的服務和整合。	2022 年 3 月 24 日
已新增的服務支援	此版本支持 AWS App Mesh 特使管理服務。請參閱 AWS CloudTrail 支援的服務和整合。	2022 年 3 月 18 日
已更新的文件	CloudTrail Lake 已新增新查詢範例，這項新功能可讓您針對事件執行精細的多欄位 SQL 查詢。此外，已將新欄位 `BytesScanned` 新增至 `DescribeQuery` 和 `GetQueryResults` 操作的查詢中繼資料結果中。如需詳細資訊，請參閱使用 CloudTrail Lake。	2022 年 3 月 4 日

已變更的功能	CloudTrail 現在，如果滿足以下兩個條件，則會移除資料事件`resources` 區塊中 Amazon S3 儲存貯體擁有者的帳戶 ID：資料事件 API 呼叫來自與 Amazon S3 儲存貯體擁有者不同的 AWS 帳戶，而 API 呼叫者收到僅針對呼叫者帳戶的`AccessDenied` 錯誤訊息。如需詳細資訊，請參閱《編輯其他帳戶呼叫之資料事件的儲存貯體擁有者帳戶 ID》。	2022 年 3 月 3 日
已更新的文件	此更新支援 CloudTrail 處理程式庫的下列版本：已新增對實作自訂 S3 管理員的支援、事件記錄以記錄檔案剖析相關例外狀況、支援剖析中的選用`errorCode` 欄位`insightDetails` ，以及更新帳戶 ID 剖析正則運算式以接受非數值。如需詳細資訊，請參閱上的使用 CloudTrail 處理程式庫和CloudTrail處理程式庫 GitHub。	2022 年 1 月 28 日

已新增的功能	CloudTrail 介紹 CloudTrail Lake，這項新功能可讓您針對事件執行精細的多欄位 SQL 查詢。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。如需詳細資訊，請參閱使用 CloudTrail Lake。	2022 年 1 月 5 日
新區域支援	CloudTrail 擴大對亞太區域 (雅加達) 新區域的支援。如需詳細資訊，請參閱CloudTrail 支援的區域。	2021 年 12 月 13 日
已新增的服務支援	此版本支持 Amazon WorkSpaces 網絡。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 12 月 3 日
已新增的功能	您現在可以使用進階事件選取器，在 Lake Formation 建立的 CloudTrail 資料 AWS Glue 表上記錄資料事件。如需詳細資訊，請參閱記錄資料事件。	2021 年 11 月 30 日
已變更的功能	作為安全最佳實務，您現在可以在關鍵政策和 Amazon S3 儲存貯體政策中新增`aws:SourceArn` 或`aws:SourceAccount` 條件 AWS KMS 金鑰。如需詳細資訊，請參閱設定 AWS KMS 的 Amazon S3 儲存貯體政策 CloudTrail和設定 CloudTrail.	2021 年 11 月 15 日

已新增的服務支援	此版本支援 AWS 彈性中樞。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 11 月 10 日
已新增的功能	新的 CloudTrail 見解事件類型可用：錯誤率見解事件。錯誤率 Insights 事件會擷取在您帳戶中 API 呼叫上發生錯誤的異常活動。如需詳細資訊，請參閱記錄追蹤的 Insights 事件。	2021 年 11 月 10 日
已新增的功能	您現在可以使用進階事件選取器，在 DynamoDB 串流上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。	2021 年 9 月 22 日
已新增的功能	您現在可以在 Amazon S3 存取點上記錄資料事件。使用進階事件選取器記錄 Amazon S3 存取點資料事件 如需詳細資訊，請參閱記錄資料事件。	2021 年 8 月 24 日
已變更的功能	當您設定追蹤以傳送通知至 Amazon SNS 時，會將政策聲明 CloudTrail 新增至 SNS 主題存取政策，以 CloudTrail 便將內容傳送至 SNS 主題。為了安全性最佳做法，我們建議在 CloudTrail 政策陳述式中新增`aws:SourceArn` 或`aws:SourceAccount` 條件金鑰。如需詳細資訊，請參閱的 Amazon SNS 主題政策 CloudTrail。	2021 年 8 月 16 日

已新增的服務支援	此版本支援 Amazon Route 53 應用程式復原控制器。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 7 月 27 日
已新增的功能	您現在可以在 EBS 快照上執行的 Amazon EBS Direct API 上記錄資料事件。使用進階事件選取器記錄 Amazon EBS Direct API 資料事件 如需詳細資訊，請參閱記錄資料事件。	2021 年 7 月 27 日
已變更的功能	CloudTrail 處理資料事件時，它會以原始格式保留數字，無論是整數 (`int`) 還是`float`. 在資料事件欄位中具有整數的事件中， CloudTrail 歷史上會將這些數字當作浮點數處理。現在，在數據事件中 CloudTrail 保留整數的原始格式。如需詳細資訊，請參閱使用 CloudTrail 處理程式庫。	2021 年 7 月 13 日
已新增的功能	您現在可以從追蹤中排除 Amazon RDS Data API 管理事件。如需詳細資訊，請參閱記錄追蹤的管理事件。	2021 年 7 月 1 日
已新增的服務支援	此版本支援 AWS BugBust。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 6 月 24 日
已新增的服務支援	此版本支援 Amazon Managed Grafana 和 Amazon Managed Service (適用於 Prometheus)。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 6 月 2 日

已新增的服務支援	此版本支持 AWS 應用程序運行器。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 5 月 18 日
已新增的服務支援	此版本支援 AWS Systems Manager 事件管理員。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 5 月 10 日
已更新的文件	此更新說明 AWS Config 符合性套件的資料事件記錄需求，特別是針對 HIPAA 或 FedRAMP 等合規性架構。如需詳細資訊，請參閱記錄資料事件。	2021 年 5 月 7 日
已新增的服務支援	此版本支援 Service Quotas 和 Amazon EBS Direct API。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 4 月 13 日
已新增的功能	IAM 管理員設定完成後 AWS STS，當使用者擔任 IAM 角色時，在事件中 CloudTrail 記錄`sourceIdentity` 資訊，或使用假定角色執行任何動作。如需詳細資訊，請參閱 CloudTrail userIdentity 元素。	2021 年 4 月 13 日
已更新的文件	此更新文件會限制某些CloudTrail事件記錄欄位中的內容 (以 KB 為單位)。如需詳細資訊，請參閱CloudTrail 記錄內容。	2021 年 4 月 8 日

已新增的功能	IAM 管理員設定完成後 AWS STS，當使用者擔任 IAM 角色時，在事件中 CloudTrail 記錄`sourceIdentity` 資訊，或使用假定角色執行任何動作。如需詳細資訊，請參閱 CloudTrail userIdentity 元素。	2021 年 4 月 6 日
已新增的功能	您現在可以在 Amazon DynamoDB 資料表上記錄資料事件。您可以使用事件選取器或進階事件選取器來記錄 DynamoDB 資料事件。如需詳細資訊，請參閱記錄資料事件。	2021 年 3 月 23 日
已新增的服務支援	此版本支援 Amazon Managed Workflows for Apache Airflow。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 3 月 22 日
已新增的功能	如果您已選擇使用進階事件選取器，您現在可以在 S3 物件 Lambda 存取點上記錄資料事件。如需詳細資訊，請參閱記錄資料事件。	2021 年 3 月 18 日
已新增的服務支援	此版本支援 AWS 故障注入模擬器。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 3 月 15 日

已新增的功能	如果您選擇使用進階事件選取器，您現在可以在 Amazon Managed Blockchain 中的 Ethereum 節點上記錄資料事件。如需詳細資訊，請參閱記錄資料事件。	2021 年 3 月 1 日
已新增的服務支援	此版本支援 Amazon Managed Blockchain 和 適用於 Managed Blockchain 的 Ethereum 的預覽 請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 2 月 4 日
已新增的服務支援	此版本支援 AWS Amplify。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 2 月 3 日
已新增的服務支援	此版本支援 Amazon Lookout for Metrics。請參閱 AWS CloudTrail 支援的服務和整合。	2021 年 2 月 1 日
已更新的文件	此更新支援下列 CloudTrail 處理程式庫的修補程式版本：更新使用指南中的 .jar 檔案參考，以使用最新版本 aws-cloudtrail-processing-library -1.4.0.jar。如需詳細資訊，請參閱上的使用 CloudTrail 處理程式庫和CloudTrail處理程式庫 GitHub。	2021 年 1 月 12 日
已新增的功能	您現在可以在 AWS Outposts 上的 Amazon S3 存取點上記錄資料事件。如需詳細資訊，請參閱記錄資料事件。	2020 年 12 月 21 日

已新增的服務支援	此版本支援 Amazon Lookout for Equipment 和 Amazon 定 Location Service。 AWS Well-Architected Tool請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 12 月 16 日
已新增的服務支援	此版本支持 AWS IoT Greengrass V2。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 12 月 15 日
已新增的服務支援	此版本支援 EKS 上的 Amazon EMR。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 12 月 10 日
已新增的服務支援	此版本支援 AWS Audit Manager 和 Amazon HealthLake。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 12 月 8 日
已新增的服務支援	此版本支援 Amazon Lookout for Vision。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 12 月 1 日
已新增的功能	AWS CloudTrail 事件版本現在是 1.08。版本 1.08 引入了新的 CloudTrail字段。如需詳細資訊，請參閱CloudTrail 記錄內容。	2020 年 11 月 24 日

已新增的功能	AWS CloudTrail 引入資料事件的進階事件選取器。進階事件選取器可對您登入追蹤的資料事件進行更精細的控制。您可以包含或排除特定 AWS 資源的資料事件，並在這些資源上選取特定 API 以記錄追蹤。如需詳細資訊，請參閱記錄資料事件。	2020 年 11 月 24 日
已新增的服務支援	此版本支援 AWS Network Firewall。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 11 月 17 日
已新增的服務支援	此版本支援 AWS Trusted Advisor。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 10 月 22 日
已更新的文件	新增兩個根使用者登入事件的事件記錄範例。如需詳細資訊，請參閱 AWS 主控台登入事件。	2020 年 10 月 13 日
已變更的功能	`AWSCloudTrail_FullAccess` 政策中的許可已被縮小。此政策不再允許您刪除 Amazon SNS 主題或 Amazon S3 儲存貯體，且 `getObject` 動作已移除。如需詳細資訊，請參閱授與 CloudTrail 使用者自訂權限。	2020 年 9 月 29 日

已更新的文件	此更新支援下列 CloudTrail 處理程式庫的修補程式版本：更新使用指南中的 .jar 檔案參考，以使用最新版本 aws-cloudtrail-processing-library -1.3.0.jar。如需詳細資訊，請參閱上的使用 CloudTrail 處理程式庫和CloudTrail處理程式庫 GitHub。	2020 年 8 月 28 日
已新增的服務支援	此版本支援 AWS Outposts。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 8 月 28 日
已新增的功能	AWS CloudTrail 深入解析介紹見 CloudTrail 解事件的歸因欄位。歸因欄位會顯示與觸發 Insights 事件的異常活動相關聯的主要使用者身分識別、使用者代理程式和錯誤碼。為了比較，歸因欄位也會顯示主要使用者身分識別、使用者代理程式以及與一般或基準活動相關聯的錯誤碼。如需詳細資訊，請參閱記錄追蹤的 Insights 事件。	2020 年 8 月 13 日
已新增的功能	AWS CloudTrail 主機具有新的外觀，旨在使其更易於使用。《 AWS CloudTrail 使用者指南》已更新為如何在主控台中執行工作的程序變更，例如建立追蹤、更新追蹤和下載事件歷程記錄。	2020 年 8 月 13 日

已新增的服務支援	此版本支援 Amazon Interactive Video Service。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 7 月 15 日
已新增的服務支援	此版本支援 Amazon Honeycode。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 6 月 24 日
已新增的服務支援	此版本支援 Amazon Macie。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 5 月 19 日
已新增的服務支援	此版本支援 Amazon Kendra。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 5 月 13 日
已新增的服務支援	此版本支援 AWS IoT SiteWise。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 4 月 29 日
已新增的區域支援	此版本支援額外區域：歐洲 (米蘭)。請參閱 AWS CloudTrail 支援的區域。	2020 年 4 月 28 日
已新增服務和區域支援	此版本支持 Amazon AppFlow。請參閱 AWS CloudTrail 支援的服務和整合。非洲 (開普敦) 區域也新增支援。請參閱 AWS CloudTrail 支援的區域。	2020 年 4 月 22 日

已新增的功能	高容量 AWS KMS 動作 (例如`Encrypt`、`Decrypt`和`GenerateDataKey`) 現在會記錄為「讀取」事件。如果您選擇記錄追蹤上的所有 AWS KMS 事件，並選擇記錄寫入管理事件，則您的追蹤記錄相關 AWS KMS 動作`Disable`，例如、`Delete`和`ScheduleKey` 。	2020 年 4 月 7 日
已新增的服務支援	此版本支援 Amazon CodeGuru 審閱者。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 2 月 7 日
已新增的服務支援	此版本支援 Amazon Managed Apache Cassandra Service。請參閱 AWS CloudTrail 支援的服務和整合。	2020 年 1 月 17 日
已新增的服務支援	此版本支援 Amazon Connect。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 12 月 13 日
已更新的文件	此更新支援下列 CloudTrail 處理程式庫的修補程式版本：更新使用指南中的 .jar 檔案參考，以使用最新版本 aws-cloudtrail-processing-library-1.2.0.jar。如需詳細資訊，請參閱上的使用 CloudTrail 處理程式庫和CloudTrail處理程式庫 GitHub。	2019 年 11 月 21 日

已新增的功能	此版本支援「 AWS CloudTrail 深入解析」，協助您偵測帳戶中的異常活動。請參閱記錄追蹤的 Insights 事件。	2019 年 11 月 20 日
已新增的功能	此版本新增用於從追蹤篩選 AWS Key Management Service 事件的選項。請參閱建立追蹤。	2019 年 11 月 20 日
已新增的服務支援	此版本支持 AWS CodeStar 通知。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 11 月 7 日
已新增的功能	無論您使用 CloudTrail 控制台還是 API CloudTrail，此版本都支持在中創建跟踪時添加標籤。此版本新增了兩個新的 API，`GetTrail` 和 `ListTrails` 。	2019 年 11 月 1 日
已新增的服務支援	此版本支援 AWS App Mesh。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 10 月 17 日
已新增的服務支援	此版本支援 Amazon Translate 。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 10 月 17 日
文件更新	「不支援的服務」主題已還原並更新，只包含目前未記錄事件的那些 AWS 服務 CloudTrail。請參閱 CloudTrail 不支援的服務。	2019 年 10 月 7 日

文件更新	文件已隨 AWSCloudTrailFullAccess 政策的變更而更新。顯示與 AWSCloudTrailFullAccess 許可對等的政策範例已更新，以限制可對符合下列條件陳述式的資源採取何種 iam:PassRole 動作："iam:PassedToService": "cloudtrail.amazonaws.com" 。請參閱 AWS CloudTrail 身分類型政策範例。	2019 年 9 月 24 日
文件更新	文件已更新為新主題「管理 CloudTrail 成本」，可協助您在預算範圍內取得所需的 CloudTrail 記錄資料。	2019 年 9 月 3 日
已新增的服務支援	此版本支援 AWS Control Tower。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 8 月 13 日
已新增的區域支援	此版本支援額外區域：中東 (巴林)。請參閱 AWS CloudTrail 支援的區域。	2019 年 7 月 29 日
文件更新	文件已更新，其中包含的安全性相關資訊 CloudTrail。請參閱 AWS CloudTrail的安全性。	2019 年 7 月 3 日
已新增的服務支援	此版本支援 AWS Ground Station。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 6 月 6 日

已新增的服務支援	此版本支援 AWS IoT Things Graph。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 6 月 4 日
已新增的服務支援	此版本支援 Amazon AppStream 2.0。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 4 月 25 日
已新增的區域支援	此版本支援額外的區域：亞太區域 (香港)。請參閱 AWS CloudTrail 支援的區域。	2019 年 4 月 24 日
已新增的服務支援	此版本支援 Amazon Managed Service for Apache Flink。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 3 月 22 日
已新增的服務支援	此版本支援 AWS Backup。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 2 月 4 日
已新增的服務支援	此版本支持 Amazon WorkLink。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 1 月 23 日
已新增的服務支援	此版本支援 AWS Cloud9。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 1 月 21 日
已新增的服務支援	此版本支援 AWS Elemental MediaLive。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 1 月 19 日

已新增的服務支援	此版本支援 Amazon Comprehend。請參閱 AWS CloudTrail 支援的服務和整合。	2019 年 1 月 18 日
已新增的服務支援	此版本支援 AWS Elemental MediaPackage。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 12 月 21 日
已新增的區域支援	此版本支援額外區域：歐洲 (斯德哥爾摩)。請參閱 AWS CloudTrail 支援的區域。	2018 年 12 月 11 日
文件更新	文件已經更新關於可支援和不支援服務的資訊。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 12 月 3 日
已新增的服務支援	此版本支援 AWS Resource Access Manager (AWS RAM)。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 11 月 20 日
已更新的功能	此版本支援在中建立追蹤 CloudTrail ，以記錄中組織中所有 AWS 帳戶的事件 AWS Organizations。請參閱建立組織追蹤。	2018 年 11 月 19 日
已新增的服務支援	此版本支援 Amazon Pinpoint 簡訊與語音 API。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 11 月 16 日

已新增的服務支援	此版本支援 AWS IoT Greengrass。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 10 月 29 日
已更新的文件	此更新支援下列 CloudTrail 處理程式庫的修補程式版本：更新使用指南中的 .jar 檔案參考，以使用最新版本 aws-cloudtrail-processing-library -1.1.3.jar。如需詳細資訊，請參閱上的使用 CloudTrail 處理程式庫和CloudTrail處理程式庫 GitHub。	2018 年 10 月 18 日
已新增的功能	此版本支援在 Event history (事件歷史記錄) 使用額外篩選條件。請參閱在 CloudTrail 主控台中檢視 CloudTrail 事件。	2018 年 10 月 18 日
已新增的功能	此版本支援 Amazon Virtual Private Cloud (Amazon VPC) 在您的 VPC 與 AWS CloudTrail之間建立私有連線。請參閱搭 AWS CloudTrail 配介面 VPC 端點使用。	2018 年 8 月 9 日
已新增的服務支援	此版本支援 Amazon Data Lifecycle Manager。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 7 月 24 日
已新增的服務支援	此版本支援 Amazon MQ。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 7 月 19 日

已新增的服務支援	此版本支援 AWS 行動 CLI。請參閱 AWS CloudTrail 支援的服務和整合。	2018 年 6 月 29 日
AWS CloudTrail 文檔歷史記錄通知可通過 RSS 提要	您現在可以透過訂閱 RSS 摘要來接收有關 AWS CloudTrail 文件更新的通知。	2018 年 6 月 29 日

舊版更新

下表說明 2018 年 6 月 29 日 AWS CloudTrail 之前的文件發行歷史記錄。

變更	描述	版本日期
已新增的服務支援	此版本支援 Amazon RDS Performance Insights。如需詳細資訊，請參閱CloudTrail 支援的服務和整合。	2018 年 6 月 21 日
已新增的功能	此版本支援記錄事件歷史記錄中的所有 CloudTrail 管理事件。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。	2018 年 6 月 14 日
已新增的服務支援	此版本支援 AWS Billing and Cost Management。請參閱CloudTrail 支援的服務與整合。	2018 年 6 月 7 日
已新增的服務支援	此版本支援 Amazon Elastic Container Service for Kubernetes (Amazon EKS)。請參閱CloudTrail 支援的服務與整合。	2018 年 6 月 5 日
已更新的文件	此更新支援 CloudTrail處理程式庫的下列修補程式版本： • 更新使用指南中的 .jar 檔案參考，以使用最新版本 aws-cloudtrail-processing-library -1.1.2.jar。 如需詳細資訊，請參閱（詳見）使用 CloudTrail 處理程式庫和〈CloudTrail 處理程式庫〉 GitHub。	2018 年 5 月 16 日

變更	描述	版本日期
已新增的服務支援	此版本支援 AWS Billing and Cost Management。請參閱CloudTrail 支援的服務與整合。	2018 年 6 月 7 日
已新增的服務支援	此版本支援 Amazon Elastic Container Service for Kubernetes (Amazon EKS)。請參閱CloudTrail 支援的服務與整合。	2018 年 6 月 5 日
已更新的文件	此更新支援 CloudTrail處理程式庫的下列修補程式版本： • 更新使用指南中的 .jar 檔案參考，以使用最新版本 aws-cloudtrail-processing-library -1.1.2.jar。 如需詳細資訊，請參閱（詳見）使用 CloudTrail 處理程式庫和〈CloudTrail 處理程式庫〉 GitHub。	2018 年 5 月 16 日
已新增的服務支援	此版本支援 AWS X-Ray。請參閱CloudTrail 支援的服務與整合。	2018 年 4 月 25 日
已新增的服務支援	此版本支援 AWS IoT 分析。請參閱CloudTrail 支援的服務與整合。	2018 年 4 月 23 日
已新增的服務支援	此版本支援 Secrets Manager。請參閱CloudTrail 支援的服務與整合。	2018 年 4 月 10 日
已新增的服務支援	此版本支援 Amazon Rekognition。請參閱CloudTrail 支援的服務與整合。	2018 年 4 月 6 日
已新增的服務支援	此版本支援 AWS 私有憑證授權單位 (PCA)。請參閱 CloudTrail 支援的服務與整合。	2018 年 4 月 4 日
已新增的功能	此版本支援讓您更輕鬆地使用 Amazon Athena 搜尋 CloudTrail 日誌檔。您可以直接從 CloudTrail 主控台自動建立用於查詢記錄的資料表，並使用這些資料表在 Athena 中執行查詢。如需詳細資訊，請參閱CloudTrail 支援的服務與整合和在 CloudTrail主控台中建立 CloudTrail 記錄檔資料表。	2018 年 3 月 15 日

變更	描述	版本日期
已新增的服務支援	此版本支援 AWS AppSync。請參閱CloudTrail 支援的服務與整合。	2018 年 2 月 13 日
新增了區域支援	此版本支援額外區域：亞太區域 (大阪) (ap-northeast-3)。請參閱CloudTrail 支援的地區。	2018 年 2 月 12 日
已新增的服務支援	此版本支援 AWS Shield。請參閱CloudTrail 支援的服務與整合。	2018 年 2 月 12 日
已新增的服務支援	此版本支持 Amazon SageMaker。請參閱CloudTrail 支援的服務與整合。	2018 年 1 月 11 日
已新增的服務支援	此版本支援 AWS Batch。請參閱CloudTrail 支援的服務與整合。	2018 年 1 月 10 日
已新增的功能	此版本支持將 CloudTrail 事件歷史記錄中可用的帳戶活動量擴展到 90 天。您還可以自定義列的顯示以改善 CloudTrail 事件的視圖。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。	2017 年 12 月 12 日
已新增的服務支援	此版本支持 Amazon WorkMail。請參閱CloudTrail 支援的服務與整合。	2017 年 12 月 12 日
已新增的服務支援	此版本支 Alexa for Business AWS Elemental MediaConvert、和 AWS Elemental MediaStore。請參閱CloudTrail 支援的服務與整合。	2017 年 12 月 1 日
新增功能與文件	此版本支援記錄 AWS Lambda 函數的資料事件。 如需詳細資訊，請參閱 記錄資料事件。	2017 年 11 月 30 日
新增功能與文件	此版本支援記錄 AWS Lambda 函數的資料事件。 如需詳細資訊，請參閱 記錄資料事件。	2017 年 11 月 30 日

變更	描述	版本日期
新增功能與文件	此版本支援 CloudTrail 處理程式庫的下列更新： • 新增管理事件之布林值識別的支援。 • 將 CloudTrail 事件版本更新為 1.06。 如需詳細資訊，請參閱（詳見）使用 CloudTrail 處理程式庫和〈CloudTrail 處理程式庫〉 GitHub。	2017 年 11 月 30 日
已新增的服務支援	此版本支援 AWS Glue。請參閱CloudTrail 支援的服務與整合。	2017 年 11 月 7 日
新增文件	此版本會新增主題：配額 AWS CloudTrail。	2017 年 10 月 19 日
已更新的文件	此版本更新了 Amazon Athena AWS CodeBuild 、Amazon 彈性容器登錄和 AWS Migration Hub. CloudTrail	2017 年 10 月 13 日
已新增的服務支援	此版本支援 Amazon Chime。請參閱CloudTrail 支援的服務與整合。	2017 年 9 月 27 日
新增功能與文件	此版本支援為 AWS 帳戶中的所有 Amazon S3 儲存貯體設定資料事件記錄。請參閱記錄資料事件。	2017 年 9 月 20 日
已新增的服務支援	此版本支援 Amazon Lex。請參閱CloudTrail 支援的服務與整合。	2017 年 8 月 15 日
已新增的服務支援	此版本支援 AWS Migration Hub。請參閱CloudTrail 支援的服務與整合。	2017 年 8 月 14 日
新增功能與文件	此版本支援 CloudTrail 預設為所有 AWS 帳戶啟用。過去 7 天的帳戶活動可在 CloudTrail事件歷史記錄中找到，最近的事件會顯示在控制台儀表板上。此功能先前稱為 API 活動歷史記錄，已取代為 事件歷史記錄。	2017 年 8 月 14 日

變更	描述	版本日期
新增功能與文件	此版本支援從 API 活動歷史記錄頁面上的 CloudTrail 主控台下載事件。您可以下載 JSON 或 CSV 格式的事件。 如需詳細資訊，請參閱 下載事件。	2017 年 7 月 27 日
已新增的功能	此版本支援記錄兩個額外區域 (歐洲 (倫敦) 和 加拿大 (中部)) 中的 Amazon S3 物件層級 API 操作。 如需詳細資訊，請參閱 使用 CloudTrail 記錄檔。	2017 年 7 月 19 日
已新增的服務支援	此版本支援在 CloudTrail API 活動歷史記錄功能中查找 Amazon CloudWatch 事件的 API。	2017 年 6 月 27 日
新增功能與文件	此版本支援下列服務的 CloudTrail API 活動歷程記錄功能中的其他 API： • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	2017 年 6 月 27 日
已新增的服務支援	此版本支援 AWS CodeStar。請參閱CloudTrail 支援的服務與整合。	2017 年 6 月 14 日

變更	描述	版本日期

新增功能與文件	此版本支援 CloudTrail 處理程式庫的下列更新：
	• 新增對來自相同 SQS 佇列之 SQS 訊息的不同格式的支援，以識別 CloudTrail 記錄檔。下列是支援的格式：
	  • CloudTrail 傳送至 SNS 主題的通知
	  • Amazon S3 傳送至 SNS 主題的通知
	  • Amazon S3 直接傳送至 SQS 佇列的通知
	• 新增 `deleteMessageUponFailure` 屬性的支援，而您可以使用此屬性刪除無法處理的訊息。
	
	如需詳細資訊，請參閱（詳見）使用 CloudTrail 處理程式庫和〈CloudTrail 處理程式庫〉 GitHub。
		2017 年 6 月 1 日

已新增的服務支援	此版本支援 Amazon Athena。請參閱CloudTrail 支援的服務與整合。	2017 年 5 月 19 日
已新增的功能	此版本支援將資料事件傳送至 Amazon CloudWatch 日誌。 如需設定追蹤記錄來記錄資料事件日誌的詳細資訊，請參閱「資料事件」。 如需將事件傳送至 CloudWatch 記錄檔的詳細資訊，請參閱使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。	2017 年 5 月 9 日
已新增的服務支援	此版本支援計 AWS Marketplace 量服務。請參閱CloudTrail 支援的服務與整合。	2017 年 5 月 2 日
已新增的服務支援	此版本支持 Amazon QuickSight。請參閱CloudTrail 支援的服務與整合。	2017 年 4 月 28 日

變更	描述	版本日期
新增功能與文件	此版本支援建立新追蹤記錄的已更新主控台體驗。您現在可以設定新追蹤記錄，記錄管理和資料事件的日誌。如需詳細資訊，請參閱 建立追蹤。	2017 年 4 月 11 日
已新增的文件	如果 CloudTrail 未將日誌傳遞到 S3 儲存貯體，或從帳戶中的某些區域傳送 SNS 通知，您可能需要更新政策。 若要進一步了解如何更新 S3 儲存貯體政策，請參閱「常見的 Amazon S3 政策設定錯誤」。 若要進一步了解如何更新 SNS 主題政策，請參閱「CloudTrail 沒有傳送區域的通知」。	2017 年 3 月 31 日
已新增的服務支援	此版本支援 AWS Organizations。請參閱CloudTrail 支援的服務與整合。	2017 年 2 月 27 日
新增功能與文件	此版本支援設定記錄管理和資料事件日誌之追蹤記錄的已更新主控台體驗。如需詳細資訊，請參閱 使用 CloudTrail 記錄檔。	2017 年 2 月 10 日
已新增的服務支援	此版本支援 Amazon Cloud Directory。請參閱CloudTrail 支援的服務與整合。	2017 年 1 月 26 日
新增功能與文件	此版本支援在 API 活動歷史記錄中查找 Amazon GameLift 和 AWS Managed Services 的 CloudTrail API。 AWS CodeCommit	2017 年 1 月 26 日
已新增的功能	此版本支援與 AWS Health Dashboard整合。 您可以使用 AWS Health Dashboard 來識別追蹤是否無法將日誌傳遞至 SNS 主題或 S3 儲存貯體。當 S3 儲存貯體或 SNS 主題的政策發生問題時，可能會發生這種情況。 AWS Health Dashboard 通知您有關受影響的追蹤，並建議修正原則的方法。 如需詳細資訊，請參閱《AWS Health 使用者指南》。	2017 年 1 月 24 日

變更	描述	版本日期
新增功能與文件	此版本支援在 CloudTrail 主控台中依事件來源篩選。事件來源會顯示提出要求的 AWS 服務。 如需詳細資訊，請參閱 使用主控台檢視最近的管理事件。	2017 年 1 月 12 日
已新增的服務支援	此版本支援 AWS CodeCommit。請參閱CloudTrail 支援的服務與整合。	2017 年 1 月 11 日
已新增的服務支援	此版本支援 Amazon Lightsail。請參閱CloudTrail 支援的服務與整合。	2016 年 12 月 23 日
已新增的服務支援	此版本支援 AWS Managed Services。請參閱CloudTrail 支援的服務與整合。	2016 年 12 月 21 日
新增了區域支援	此版本支援歐洲 (倫敦) 區域。請參閱CloudTrail 支援的地區。	2016 年 12 月 13 日
新增了區域支援	此版本支援加拿大 (中部) 區域。請參閱CloudTrail 支援的地區。	2016 年 12 月 8 日
已新增的服務支援	此版本支援「 AWS CodeBuild 請參閱CloudTrail 支援的服務與整合」。 此版本支援 AWS Health。請參閱CloudTrail 支援的服務與整合。 此版本支援 AWS Step Functions。請參閱CloudTrail 支援的服務與整合。	2016 年 12 月 1 日
已新增的服務支援	此版本支援 Amazon Polly。請參閱CloudTrail 支援的服務與整合。	2016 年 11 月 30 日
已新增的服務支援	此版本支援 AWS OpsWorks for Chef Automate。請參閱CloudTrail 支援的服務與整合。	2016 年 11 月 23 日

變更	描述	版本日期
新增功能與文件	此版本支援設定您的追蹤記錄唯讀、唯寫或所有事件。 CloudTrail 支援記錄 Amazon S3 物件層級 API 操作`GetObject` ，例如`PutObject` 、和`DeleteObject` 。您可以設定追蹤記錄來記錄物件層級 API 操作的日誌。 如需詳細資訊，請參閱 使用 CloudTrail 記錄檔。	2016 年 11 月 21 日
新增功能與文件	此版本支援 `userIdentity` 元素中的其他 `type` 欄位值：`AWSAccount` 和 `AWSService` 。如需更多詳細資訊，請參閱 欄位 for `userIdentity` 。	2016 年 11 月 16 日
已新增的服務支援	此版本支援 Application Auto Scaling。請參閱CloudTrail 支援的服務與整合。	2016 年 10 月 31 日
新增了區域支援	此版本支援美國東部 (俄亥俄) 區域。請參閱CloudTrail 支援的地區。	2016 年 10 月 17 日
新增功能與文件	此版本支援記錄非 API AWS 服務事件。如需詳細資訊，請參閱 AWS 服務事件。	2016 年 9 月 23 日
新增功能與文件	此版本支援使用 CloudTrail 主控台來檢視受支援的資源類型 AWS Config。如需詳細資訊，請參閱 使用 AWS Config檢視所參考的資源。	2016 年 7 月 7 日
已新增的服務支援	此版本支援 AWS Service Catalog。請參閱CloudTrail 支援的服務與整合。	2016 年 7 月 6 日
已新增的服務支援	此版本支援 Amazon Elastic File System (Amazon EFS)。請參閱CloudTrail 支援的服務與整合。	2016 年 6 月 28 日
新增了區域支援	此版本支援一個額外區域：ap-south-1 (亞太區域 (孟買))。請參閱CloudTrail 支援的地區。	2016 年 6 月 27 日
已新增的服務支援	此版本支援 AWS Application Discovery Service。請參閱CloudTrail 支援的服務與整合。	2016 年 5 月 12 日

變更	描述	版本日期
已新增的服務支援	此版本支援南美洲 (聖保羅) 地區的 CloudWatch Logs。如需詳細資訊，請參閱 使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。	2016 年 5 月 6 日
已新增的服務支援	此版本支援 AWS WAF。請參閱CloudTrail 支援的服務與整合。	2016 年 4 月 28 日
已新增的服務支援	此版本支援 AWS Support。請參閱CloudTrail 支援的服務與整合。	2016 年 4 月 21 日
已新增的服務支援	此版本支援 Amazon Inspector。請參閱CloudTrail 支援的服務與整合。	2016 年 4 月 20 日
已新增的服務支援	此版本支援 AWS IoT。請參閱CloudTrail 支援的服務與整合。	2016 年 4 月 11 日
新增功能與文件	此版本支援使用安全性宣告標記語言 AWS Security Token Service (SAML AWS STS) 和 Web 身分聯合進行的 log () API 呼叫。如需詳細資訊，請參閱 具有 SAML 和網路身分聯盟的 AWS STS API 的值。	2016 年 3 月 28 日
已新增的服務支援	此版本支援 AWS Certificate Manager。請參閱CloudTrail 支援的服務與整合。	2016 年 3 月 25 日
已新增的服務支援	此版本支援 Amazon 資料 Firehose。請參閱CloudTrail 支援的服務與整合。	2016 年 3 月 17 日
已新增的服務支援	此版本支援 Amazon CloudWatch 日誌。請參閱CloudTrail 支援的服務與整合。	2016 年 3 月 10 日
已新增的服務支援	此版本支援 Amazon Cognito。請參閱CloudTrail 支援的服務與整合。	2016 年 2 月 18 日
已新增的服務支援	此版本支援 AWS Database Migration Service。請參閱CloudTrail 支援的服務與整合。	2016 年 2 月 4 日

變更	描述	版本日期
已新增的服務支援	此版本支持 Amazon GameLift （ Amazon GameLift ）。請參閱CloudTrail 支援的服務與整合。	2016 年 1 月 27 日
已新增的服務支援	此版本支援 Amazon CloudWatch 活動。請參閱CloudTrail 支援的服務與整合。	2016 年 1 月 16 日
新增了區域支援	此版本支援一個額外區域：ap-northeast-2 (亞太區域 (首爾))。請參閱CloudTrail 支援的地區。	2016 年 1 月 6 日
已新增的服務支援	此版本支援 Amazon Elastic Container Registry (Amazon ECR)。請參閱CloudTrail 支援的服務與整合。	2015 年 12 月 21 日
新增功能與文件	此版本支援 CloudTrail 跨所有區域開啟，並支援每個區域的多個追蹤。如需詳細資訊，請參閱 使用 CloudTrail 軌跡。	2015 年 12 月 17 日
已新增的服務支援	此版本支援 Amazon Machine Learning。請參閱CloudTrail 支援的服務與整合。	2015 年 12 月 10 日
新增功能與文件	此版本支援日誌檔案加密、日誌檔案完整性驗證和標記。如需詳細資訊，請參閱使用 AWS KMS 金鑰加密 CloudTrail 記錄檔 (SSE-KMS)、驗證 CloudTrail 記錄檔完整性 及 更新追蹤。	2015 年 10 月 1 日
已新增的服務支援	此版本支持 Amazon OpenSearch 服務。請參閱CloudTrail 支援的服務與整合。	2015 年 10 月 1 日
已新增的服務支援	此版本支援 Amazon S3 儲存貯體層級事件。請參閱CloudTrail 支援的服務與整合。	2015 年 9 月 1 日
已新增的服務支援	此版本支援 AWS Device Farm。請參閱CloudTrail 支援的服務與整合。	2015 年 7 月 13 日
已新增的服務支援	此版本支援 Amazon API Gateway。請參閱CloudTrail 支援的服務與整合。	2015 年 7 月 9 日

變更	描述	版本日期
已新增的服務支援	此版本支援 CodePipeline。請參閱CloudTrail 支援的服務與整合。	2015 年 7 月 9 日
已新增的服務支援	此版本支援 Amazon DynamoDB。請參閱CloudTrail 支援的服務與整合。	2015 年 5 月 28 日
已新增的服務支援	此版本支援美國西部 (加利佛尼亞北部) 區域的 CloudWatch Logs。如需有關 CloudWatch 記錄監控 CloudTrail 支援的詳細資訊，請參閱使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔。	2015 年 5 月 19 日
已新增的服務支援	此版本支援 AWS Directory Service。請參閱CloudTrail 支援的服務與整合。	2015 年 5 月 14 日
已新增的服務支援	此版本支援 Amazon Simple Email Service (Amazon SES)。請參閱CloudTrail 支援的服務與整合。	2015 年 5 月 7 日
已新增的服務支援	此版本支援 Amazon Elastic Container Service，請參閱 CloudTrail 支援的服務與整合。	2015 年 4 月 9 日
已新增的服務支援	此版本支援 AWS Lambda。請參閱CloudTrail 支援的服務與整合。	2015 年 4 月 9 日
已新增的服務支援	此版本支持 Amazon WorkSpaces。請參閱CloudTrail 支援的服務與整合。	2015 年 4 月 9 日
	此版本支援查閱 CloudTrail (CloudTrail 事件) 擷取的 AWS 活動。您可以查詢和篩選您帳戶中與建立、修改或刪除有關的事件。若要查詢這些事件，您可以使用 CloudTrail 主控台、 AWS Command Line Interface (AWS CLI) 或 AWS SDK。如需詳細資訊，請參閱 使用 CloudTrail 事件歷史記錄。	2015 年 3 月 12 日
已新增的服務支援和新文件	此版本支援亞太區域 (新加坡)、亞太區域 (雪梨)、亞太區域 (東京) 和歐洲 (法蘭克福) 區域的 Amazon CloudWatch Logs。如需詳細資訊，請參閱將事件傳送至 CloudWatch 記錄檔。	2015 年 3 月 5 日

變更	描述	版本日期
新增文件	CloudTrail 概念頁面已新增說明 AWS Security Token Service (AWS STS) 地區端點 CloudTrail 支援的新章節。	2015 年 2 月 17 日
已新增的服務支援	此版本支援 Amazon Route 53。請參閱CloudTrail 支援的服務與整合。	2015 年 2 月 11 日
已新增的服務支援	此版本支援 AWS Config。請參閱CloudTrail 支援的服務與整合。	2015 年 2 月 10 日
已新增的服務支援	此版本支援 AWS CloudHSM。請參閱CloudTrail 支援的服務與整合。	2015 年 1 月 8 日
已新增的服務支援	此版本支援 AWS CodeDeploy。請參閱CloudTrail 支援的服務與整合。	2014 年 12 月 17 日
已新增的服務支援	此版本支援 AWS Storage Gateway。請參閱CloudTrail 支援的服務與整合。	2014 年 12 月 16 日
新增了區域支援	此版本支援一個額外的區域： us-gov-west-1（AWS GovCloud （美國西部））。請參閱CloudTrail 支援的地區。	2014 年 12 月 16 日
已新增的服務支援	此版本支援 Amazon S3 Glacier。請參閱CloudTrail 支援的服務與整合。	2014 年 12 月 11 日
已新增的服務支援	此版本支援 AWS Data Pipeline。請參閱CloudTrail 支援的服務與整合。	2014 年 12 月 2 日
已新增的服務支援	此版本支援 AWS Key Management Service。請參閱CloudTrail 支援的服務與整合。	2014 年 11 月 12 日
新增文件	「使用 Amazon CloudWatch 日 CloudTrail 誌監控日誌檔」的新小節已新增至指南》。它說明如何使用 Amazon CloudWatch 日誌來監控日 CloudTrail 誌事件。	2014 年 11 月 10 日

變更	描述	版本日期
新增文件	「使用 CloudTrail 處理程式庫」的新小節已新增至指南》。它提供了有關如何使用 AWS CloudTrail 處理庫在 Java 中編寫 CloudTrail 日誌處理器的信息。	2014 年 11 月 5 日
已新增的服務支援	此版本支援 Amazon Elastic Transcoder。請參閱CloudTrail 支援的服務與整合。	2014 年 10 月 27 日
新增了區域支援	此版本支援一個額外區域：eu-central-1 (歐洲 (法蘭克福))。請參閱CloudTrail 支援的地區。	2014 年 10 月 23 日
已新增的服務支援	此版本支持 Amazon CloudSearch。請參閱CloudTrail 支援的服務與整合。	2014 年 10 月 16 日
已新增的服務支援	此版本支援 Amazon Simple Notification Service。請參閱CloudTrail 支援的服務與整合。	2014 年 10 月 09 日
已新增的服務支援	此版本支持 Amazon ElastiCache。請參閱CloudTrail 支援的服務與整合。	2014 年 9 月 15 日
已新增的服務支援	此版本支持 Amazon WorkDocs。請參閱CloudTrail 支援的服務與整合。	2014 年 8 月 27 日
已新增的內容	此版本包含討論記錄日誌登入事件的主題。請參閱AWS Management Console 登入事件。	2014 年 7 月 24 日
已新增的內容	此版本的 eventVersion 元素已升級至 1.02 版，而且已新增三個新欄位。請參閱CloudTrail 記錄內容。	2014 年 7 月 18 日
已新增的服務支援	此版本支援 Auto Scaling (請參閱 CloudTrail 支援的服務與整合)。	2014 年 7 月 17 日
新增了區域支援	此版本支援三個額外區域：ap-southeast-1 (亞太區域 (新加坡))、ap-wetheast-1 (亞太區域 (東京))、sa-east-1 (南美洲 (聖保羅))。請參閱CloudTrail 支援的地區。	2014 年 6 月 30 日
額外的服務支援	此版本支援 Amazon Redshift。請參閱CloudTrail 支援的服務與整合。	2014 年 6 月 10 日

變更	描述	版本日期
已新增的服務支援	此版本支援 AWS OpsWorks。請參閱CloudTrail 支援的服務與整合。	2014 年 6 月 5 日
已新增的服務支援	此版本支持 Amazon CloudFront。請參閱CloudTrail 支援的服務與整合。	2014 年 5 月 28 日
新增了區域支援	此版本支援三個額外區域：us-west-1 (美國西部 (加利佛尼亞北部))、eu-west-1 (歐洲 (愛爾蘭))、ap-southeast-2 (亞太區域 (雪梨))。請參閱CloudTrail 支援的地區。	2014 年 5 月 13 日
已新增的服務支援	此版本支援 Amazon Simple Workflow Service。請參閱CloudTrail 支援的服務與整合。	2014 年 5 月 9 日
已新增的內容	此版本包含討論在帳戶之間共享日誌檔案的主題。請參閱在 AWS 帳戶之間共用 CloudTrail 記錄檔。	2014 年 5 月 2 日
已新增的服務支援	此版本支持 Amazon CloudWatch。請參閱CloudTrail 支援的服務與整合。	2014 年 4 月 28 日
已新增的服務支援	此版本支援 Amazon Kinesis。請參閱CloudTrail 支援的服務與整合。	2014 年 4 月 22 日
已新增的服務支援	此版本支援 AWS Direct Connect。請參閱CloudTrail 支援的服務與整合。	2014 年 4 月 11 日
已新增的服務支援	此版本支援 Amazon EMR。請參閱CloudTrail 支援的服務與整合。	2014 年 4 月 4 日
已新增的服務支援	此版本支援 Elastic Beanstalk。請參閱CloudTrail 支援的服務與整合。	2014 年 4 月 2 日
額外的服務支援	此版本支援 AWS CloudFormation。請參閱CloudTrail 支援的服務與整合。	2014 年 3 月 7 日
新的指南》	此版本推出 AWS CloudTrail。	2013 年 11 月 13 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

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。